EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios

Supplement 1

FINAL REPORT

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, D.C. 20555-0001

Electric Power Research Institute
3420 Hillview Avenue
Palo Alto, CA 94304-1338

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Washington, DC 20402-0001
   Internet: http://bookstore.gpo.gov
   Telephone: 1-866-512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22161-0002
   http://www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

U.S. Nuclear Regulatory Commission
Office of Administration
Multimedia, Graphics and Storage & Distribution Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
http://www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG-0750).

EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios

NUREG-1921
Supplement 1

EPRI 3002009215

FINAL REPORT

Manuscript Completed: August 2017
Date Published: January 2020

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, D.C. 20555-0001

U.S. NRC-RES Project Manager
S. Cooper

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304-1338

EPRI Project Manager
A. Lindeman

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATIONS NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATIONS BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATIONS PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research

JENSEN HUGHES

John Wreathall & Co., Inc.

Sandia National Laboratories

Scientech, a business unit of Curtiss-Wright Flow Control Company

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ABSTRACT

Fire probabilistic risk assessments analyze a wide variety of fire-induced scenarios, one of which is fire damage rendering the main control room (MCR) either uninhabitable or ineffective. As a result of this fire damage, operators cannot stay in the MCR and the command and control of the plant is transferred from the MCR to another location. This is commonly referred to as main control room abandonment (MCRA).

Main control room abandonment is analyzed as a special case of fire human reliability analysis. While NUREG-1921/EPRI 1023001 – *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines* briefly addressed abandonment, additional guidance and inputs are needed to properly address the unique contexts of abandonment scenarios. Therefore, this effort builds upon previous fire PRA research efforts that developed explicit guidance for estimating human error probabilities for human failures events under fire-related conditions. In particular, this guidance builds upon, rather than replaces, NUREG-1921, which provides, among other items, a process for conducting fire human reliability analysis through several steps including: identification and definition, qualitative analysis, quantification, recovery analysis, dependency analysis, and treatment of uncertainty.

The success of performing shutdown from outside of the MCR is dependent on a number of factors including the plant strategy and procedure, capabilities of the remote shutdown panel, and the number of local operator actions. This report provides additional guidance beyond NUREG-1921 in several areas, including: modeling considerations, feasibility assessment, identification and definition, timing, performance shaping factors (including a preliminary assessment of command and control), and walk-through and talk-through guidance. Overall, this report provides guidance to develop a qualitative foundation for MCRA scenarios that will ultimately support quantification of human failure events related to abandonment.

Keywords
Command and control
Fire human reliability analysis (Fire HRA)
Fire protection
Main control room abandonment (MCRA)
Probabilistic risk assessment (PRA)
Qualitative analysis

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

PRIMARY AUDIENCE: Fire probabilistic risk assessment (PRA) engineers and fire human reliability assessment (HRA) practitioners supporting the development and/or maintenance of fire PRAs.

SECONDARY AUDIENCE: Engineers, utility managers, operators, and other stakeholders who review fire PRAs, and who are interested in learning about the human and plant response during a main control room abandonment (MCRA) event.

KEY RESEARCH QUESTION

Main control room abandonment (MCRA) is defined as those scenarios where command and control of the plant is transferred out of the main control room to another location. For fire scenarios, this may occur due to either loss of habitability or loss of control.

How should fire probabilistic risk assessments model human and plant response for fire scenarios resulting in MCRA?

RESEARCH OVERVIEW

Through a joint research effort between EPRI and the NRC, this report builds upon prior fire methodology reports including *Fire PRA Methodology for Nuclear Power Facilities,* (EPRI 1011989/NUREG/CR-6850) where the fire PRA tasks related to MCRA are not fully addressed or described. Additionally, this report supplements the guidance for MCRA scenarios where *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines* (EPRI 1023001/NUREG-1921) provides preliminary guidance.

Specifically, this report addresses the qualitative HRA and PRA considerations for MCRA including:

- Modeling considerations for MCRA, scenario-specific success criteria, and incorporation of human failure events (HFEs) and equipment failures into the plant response model.
- MCRA scenario development, including consideration of the decision to abandon
- Feasibility assessment and HFE definition and identification
- Timing and timeline guidance
- Qualitative HRA specific to MCRA scenario context, including consideration of performance shaping factors and other influences on operator performance.

In developing this guidance, the fire HRA process in EPRI 1023001/NUREG-1921 was followed, with additional guidance specific to the MCRA context provided for each relevant step. Historical event reviews, cognitive literature searches, and interviews with current and former operator trainers and operators assisted in forming the basis for this guidance. Feedback on the guidance was provided at two key points in the report development process. First, a draft document was prepared in spring 2016 to support a presentation to the Reliability and PRA Subcommittee of the Advisory Committee on Reactor Safeguards (ACRS) in May 2016. Following that meeting, a second draft was developed and was subjected to a peer review including both industry and regulatory stakeholders.

KEY FINDINGS

MCRA is a unique case of fire HRA necessitating the development of a solid qualitative analysis that accounts for fire-related damage criteria leading to abandonment, changes in crew structure and interaction after abandonment, and the coordination of many overlapping timeframes and actions.

The aspects of a good qualitative MCRA analysis include:

- Collection and review of plant specific information and fire PRA insights
- Identification of MCRA scenarios including consideration of the decision to abandon and proper treatment within those scenarios based on different functional requirements
- Review of MCRA procedure steps and assessment of why each step is/is not relevant to the analysis
- Plant-specific walk-throughs and talk-throughs of the MCRA procedure
- Development of timeline based on walk/talk-throughs, simulator exercises, training material and thermal-hydraulic analyses
- Identifying and defining HFEs based on the MCRA procedure and context of MCRA scenarios
- Evaluation of HFE specific timing and performance shaping factors based on the context of MCRA scenarios
- Assessment of command and control in terms of existing plans, training, and communication strategies
- Documentation of analysis, including input parameters

WHY THIS MATTERS

This report provides consensus guidance for analyzing the human and plant response for fires resulting in MCRA. This guidance can be applied to the development or maintenance of fire probabilistic risk assessments. The insights from this process may be fed back into operations, training, or design changes to enhance the feasibility and reliability of the MCRA strategy.

HOW TO APPLY RESULTS

Users will benefit from the introductory material provided in Sections 1 and 2 that discusses the scope of the document and the context differences for MCRA. PRA modeling, scenario-specific success criteria, and the incorporation of HFEs and equipment failures into the plant response model can be found in Section 3. Section 4 provides guidance for developing and performing the qualitative assessment associated with the decision to abandon. Section 5 provides guidance on identification and definition of human failure events for MCRA scenarios. Section 6 provides guidance on feasibility assessment. Sections 7 and 8 provide guidance to develop and assess qualitative inputs including timing, timelines, and performance shaping factors. Guidance on performing walk-throughs and talk-throughs for MCRA is provided in Section 4 and Appendix C.

LEARNING AND ENGAGEMENT OPPORTUNITIES

Users of this report may be interested in fire PRA training, Module IV – Fire Human Reliability Analysis, sponsored jointly between EPRI and the U.S. NRC-RES.

EPRI's HRA Users Group performs research aimed at improving human reliability analysis and provides technology transfer opportunities. The collaboration site for the user group can be accessed at: https://membercenter.epri.com/collaboration/4000000763/Pages/default.aspx

EPRI CONTACT: Ashley Lindeman, Senior Technical Leader, 704.595.2538, alindeman@epri.com

NRC CONTACT: Susan Cooper, Senior Reliability & Risk Engineer, 301.415.0915, susan.cooper@nrc.gov

Program: Risk and Safety Management (41.07.01)

Implementation Category: Plant Optimization

CITATIONS

This report was prepared by:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304

Principal Investigators:
A. Lindeman
M. Presley

Under contract to EPRI:

Jensen Hughes
111 Rockville Pike Suite 550
Rockville, MD 20850-5109

Principal Investigators:
E. Collins
P. Amico
J. Julius

Scientech, a business unit of Curtiss-Wright Flow Control Company
16300 Christensen Road, Suite 300
Tukwila, WA 98188

Principal Investigators:
K. Kohlhepp Gunter

U.S. Nuclear Regulatory Commission (NRC)
Office of Nuclear Regulatory Research (RES)
Washington, DC 20555

Principal Investigators:
S. Cooper
T. Rivera

Under contract to NRC-RES:

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Principal Investigator:
S. Hendrickson

John Wreathall & Co., Inc.
4157 MacDuff Way
Dublin, OH 43106

Principal Investigator:
J. Wreathall

This report describes research sponsored by EPRI and the NRC.

This publication is a corporate document that should be cited in the literature in the following manner:

EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios: Supplement 1, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, D.C., and Electric Power Research Institute (EPRI), Palo Alto, CA. 2017. NUREG-1921 Supplement 1 and EPRI 3002009215. (While the NRC and EPRI reports have different publication dates, they are essentially the same report.)

The report should be cited internally in NRC documents in this way:

U.S. Nuclear Regulatory Commission, NUREG-1921, Supplement 1, "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines - Qualitative Analysis for Main Control Room Abandonment Scenarios," EPRI 3002009215, 2018.

ACKNOWLEDGMENTS

The authors would to thank the organizations and individuals who contributed their time, insights, and experience throughout the development of this report.

In support of this project, NRC-RES led interviews with NRC staff who had previous experience in nuclear power plant operations and/or training. The project team would like to thank: Harry Barrett, Kevin Coyne, Sean Curie (formerly NRC-NRR), Jim Kellum, Michelle Kichline, Mark King, Bernie Litkett, Jack McHale (retired NRC), and Ross Telson for their expertise. The interviews assisted the team in further understanding the context surrounding the MCR abandonment. Also, Kendra Hill-Wright (formerly NRC-RES) provided invaluable assistance in the development of this report in its earlier stages.

The project team provided a draft of the report to the Reliability and PRA Subcommittee of the NRC's Advisory Committee on Reactor Safeguards (ACRS) in April 2016. Feedback was provided to the project team during the May 4, 2016 meeting of the Reliability and PRA Subcommittee. The project team thanks the members of the subcommittee for their valuable feedback on the report.

In July 2016, a revised draft was provided for an independent peer review. The peer review team was composed of stakeholders from the industry, NRC, and members of the human factors and cognitive science community. We thank those who provided comments: Harry Barrett (NRC-NRR), Valerie Barnes (NRC-RES), Fernando Ferrante (formerly NRC-RES), Donnie Harrison (NRC-NRO), Christopher Hunter (NRC-RES), J.S. Hyslop (NRC-NRR), Lynn Kolonauski (Jensen Hughes), Laura Militello (Applied Decision Science), Steve Odell (Westinghouse), Lauren Killian Ning (NRC-RES), Andy Ratchford (Jensen Hughes), Emilie Roth (Roth Cognitive Engineering), Nathan Siu (NRC-RES), Jeff Stone (Exelon), Ricky Summitt (RSC Engineers), and Claire Taylor (OECD Halden Reactor Project).

ACRONYMS

ADV	atmospheric dump valve
AFW	auxiliary feedwater
AIT	augmented inspection team
ANS	American Nuclear Society
AO	auxiliary operator
AOP	abnormal operating procedures
APP	annunciator panel procedures
ARP	annunciator response procedures
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event ANAlysis
ATWS	anticipated transient without scram
BOP	balance of plant
BWR	boiling water reactor
C&C	command and control
CAFTA	Computer Aided Fault Tree Analysis System
CBDTM	cause-based decision tree method
CCDP	conditional core damage probability
CCW	component cooling water
CDF	core damage frequency
CFCU	containment fan cooler unit
CFR	Code of Federal Regulations
CLERP	conditional large early release probability
COP	common operational picture
CRE	control room envelope
CRHS	control room habitability systems

CRS	control room supervisor
CS	core spray
CSR	cable spreading room
CST	condensate storage tank
CVCS	chemical and volume control system
DHR	decay heat removal
ECCS	emergency core cooling system
EDG	emergency diesel generator
EDMG	extensive damage mitigation guidelines
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERO	emergency response organization
ERV	electromatic relief valve
ESF	engineered safety features
ESW	emergency service water
FAQ	frequently asked question
FLEX	flexible and diverse mitigation strategies
FPRA	fire probabilistic risk assessment
FRANX	Fire Risk Analysis Tool
FSS	fire scenario selection
FW	feedwater
GDC	general design criteria
HEP	human error probability
HFE	human failure event
HMI	human-machine interface
HPCI	high pressure coolant injection
HPI	high pressure injection
HRA	human reliability analysis
HVAC	heating, ventilation, and air conditioning
IA	instrument air
IN	information notice

IPEEE	individual plant examination of external events
ISLOCA	interfacing-system loss of coolant accident
JPM	job performance measure
LAR	licensee amendment request
LCS	local control station
LCO	limiting condition for operation
LER	licensee event report
LERF	large early release frequency
LOC	loss of control
LOCA	loss of coolant accident
LOH	loss of habitability
LOOP	loss of offsite power
LPCI	low pressure coolant Injection
LPI	low pressure injection
LWGR	light water cooled graphite moderated reactor
MCB	main control board
MCR	main control room
MCRA	main control room abandonment
MD AFW	motor-driven auxiliary feedwater
MFW	main feedwater
MOV	motor operated valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSO	multiple spurious operation
NATO	North Atlantic Treaty Organization
NEI	Nuclear Energy Institute
NFPA	National Fire Protection Association
NLO	non-licensed operator
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSCA	nuclear safety capability assessment

OCC	outage command center
OMA	operator manual action
PHWR	pressurized heavy water reactor
PORV	power-operated relief valve
PPE	personal protective equipment
PRA	probabilistic risk assessment
PRM	plant response model
PSF	performance shaping factor
PWR	pressurized water reactor
PZR	pressurizer
RAI	request for additional information
RCIC	reactor core isolation cooling
RCP	reactor coolant pump
RCS	reactor coolant system
RHR	residual heat removal
RNO	response not obtained
RO	reactor operator
RPD	recognition-primed decision-making
RPV	reactor pressure vessel
RSDP	remote shutdown panel
RWST	refueling water storage tank
SAMG	severe accident management guidelines
SBO	station blackout
SCBA	self-contained breathing apparatus
SER	safety evaluation report
SF	situational factors
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SISBO	self-induced station blackout
SM	shift manager

SORV	stuck-open relief valve
SPDS	safety parameter display system
SR	supporting requirements
SRM	staff requirements memorandum
SRO	senior reactor operator
SRV	safety relief valve
SS	shift supervisor
SSC	structures, systems, and components
SSD	safe shutdown
STA	shift technical advisor
SW	service water
TAF	top of active fuel
TCOA	time-critical operator actions
T-H	thermal hydraulic
THERP	technique for human error-rate prediction
TMI	Three Mile Island
TSC	technical support center
UAT	unit auxiliary transformer
U.S.	United States
VCT	volume control tank

1
INTRODUCTION

This report provides human reliability analysis (HRA) and probabilistic risk assessment (PRA) guidance on treatment of scenarios that require main control room abandonment (MCRA) in response to a fire event, focusing particularly on qualitative analysis. Follow-on work is planned to address HRA quantification for MCRA scenarios.

This guidance is intended for practitioners of both fire HRA and fire PRA. Good practice for HRA/PRA always consists of close collaboration between HRA and PRA. As discussed in this report, proper treatment of MCRA scenarios requires an even closer cooperation of HRA and PRA analysts, as HRA must provide input *before* MCRA scenarios can be defined and developed for the overall PRA model.

Consequently, this guidance builds upon the fire HRA guidance provided in a previously published joint report, *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines* [1] and augments (and sometimes replaces) that given in the overall fire PRA methodology report, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,* (EPRI 1011989/NUREG/CR-6850) [2].

The fire HRA process steps identified in NUREG-1921 are unchanged for MCRA. Instead, this report expands upon the guidance and discussion given in NUREG-1921 regarding task interfaces and interactions between HRA and other disciplines in a fire PRA to address additional needs for performing HRA for MCRA. In addition, it focuses on the differences between MCRA scenarios and other fire scenarios and how such differences are treated in HRA/PRA.

1.1 Objectives and Scope

The overall objective of this most recent EPRI/NRC-RES collaboration is to provide additional guidance for both HRA and PRA involving MCRA scenarios. MCRA due to both loss of habitability (LOH) and loss of control (LOC) are addressed. In both cases, MCRA is defined to have occurred when command and control (e.g., the decision-making and coordination function performed by the shift supervisor or manager) has left the MCR for a different location. Therefore, this guidance does *not* apply to scenarios where operators are dispatched from the MCR to perform actions elsewhere when the shift supervisor/manager (or equivalent) remains in the MCR.[1]

This document provides updated guidance for:

- Fire HRA for MCRA scenarios, for which NUREG-1921 provides limited guidance
- Fire PRA tasks related to MCRA that NUREG/CR-6850 either does not address or does not clearly describe

This report is intended to supplement the fire HRA guidance provided in NUREG-1921. Thus, this report can be considered additional, rather than replacement, guidance for qualitative HRA tasks. NUREG-1921 remains the guiding document for the scope of fire HRA guidance, in general.

This updated guidance on MCRA scenarios has been developed with both NRC and industry needs for transition to National Fire Protection Association (NFPA) 805 [3] in mind. The examples and insights presented in this report are derived from experience within the United States. In general, this guidance may be applied internationally, but with the understanding that the strategies, capability of remote, or alternate, shutdown panels, staffing, and procedure progression may differ from those found in the United States.

Recognizing the breadth of such a project, EPRI and NRC-RES approached the development of guidance into two phases. This first supplement to NUREG-1921 (i.e., this report) addresses qualitative HRA/PRA for MCRA, including:

- MCRA scenario development, including consideration of the decision to abandon
- Human failure event (HFE) definition and identification
- Qualitative HRA specific to MCRA scenarios, including consideration of performance shaping factors (PSFs) and other influences on operator performance

A second phase of guidance development will address HRA quantification for MCRA. Fire HRA tasks of recovery analysis, dependency evaluation, uncertainty analysis, and documentation will be addressed in both developmental phases, as appropriate.

[1] Such scenarios are sometimes referred to as “partial abandonment.” This terminology should be avoided; there are only abandonment and non-abandonment scenarios. Abandonment occurs when command and control is shifted out of the MCR, even if an operator remains in the MCR to perform actions as part of the abandonment strategy. The guidance in this document applies to such cases. Non-abandonment occurs when command and control is *not* shifted out of the MCR, regardless of how many operators are dispatched to other locations in the plant to perform actions as part of the abandonment strategy. The guidance in this document *does not* apply to such cases.

However, as noted in NUREG-1921, fire HRA tasks are not typically performed in series or independently of one another. Consequently, Supplement 1 may include discussion of qualitative inputs that ultimately support HRA quantification (which will be addressed in a separate report).

Also, because MCRA guidance in this report relates to fire PRA tasks, portions of this report are intended to supplement or replace portions of NUREG/CR-6850 [2]. This report addresses:

- Modeling considerations for MCRA
- MCRA-specific success criteria
- Incorporation of HFEs and equipment failures into the plant response model (PRM)

1.1.1 Expected Usage

The PRA model should reflect the MCRA actions that are required under different sets of circumstances. For example, some MCRA scenarios may involve loss of offsite power (LOOP), while others will not. As always, coordination is required between PRA and HRA analysts to make the best compromise between modeling distinctions to reflect the diversity of the plant and operator response while recognizing which bounding scenarios and HFEs are appropriate to model.

Given the uniqueness and importance of MCRA LOC scenarios, additional guidance is provided to aid the analyst in evaluating the decision to abandon the MCR. While this guidance is primarily contained in Section 4, there are subsections throughout this report that provide clarification on LOC and decision to abandon distinctions for the specific section topics.

One of the most important features of an MCRA HRA is the timing of the individual operator actions within the context of the timing of the MCRA scenario(s). Integration of the various fire timelines (e.g., fire modeling, accident sequence analysis with the operator response timeframes) is discussed. Examples are provided to demonstrate this timeline development and integration process.

Time can also be a key factor in determining the feasibility of MCRA strategies on a scenario basis. As a result, this report expands upon the treatment of feasibility assessment included in NUREG-1921 to discuss MCRA scenario feasibility and go/no-go criteria at the HFE level.

Once MCRA HFEs are assessed as being feasible, this report provides MCRA-related considerations for PSFs, including tables to trigger the analyst to consider the key PSF influences for various aspects of MCRA scenarios, such as those involving rapid response or capability of the RSDP.

Section 10.4, Interface with Operations, discusses the interaction between the PRA/HRA analysts and plant staff. The HRA depends upon interviews with plant personnel to obtain a significant amount of information and insights to support the analysis, but outputs can also help risk-inform the focus of MCRA procedures and training.

Ultimately, the modeling guidance, timelines, and qualitative insights (including PSFs) will be applied to the quantification of HFEs (assessment of HEPs) and, by extension, the MCRA scenarios in the fire PRA model. Quantification will be covered in a subsequent report, but the intent of this report is to supply the crucial qualitative analysis background and context to properly inform the MCRA HRA. Overall, the guidance in this report assists in the development of the following outputs to support the fire PRA including:

- MCRA scenario definition and modeling of abandonment
- Decision to abandon
- Identification of HFEs
- MCRA feasibility assessment
- Inputs to quantification of MCRA HFEs
- Insights on recovery and dependency
- Insights on MCRA feasibility and reliability (that can, for example, be useful information for the NPP operations department)

1.2 Fire HRA Background

Working jointly under a Memorandum of Understanding, the Electric Power Research Institute (EPRI) and the U.S. Nuclear Regulatory Commission's Office of Nuclear Regulatory Research (NRC-RES) published EPRI 1011989/NUREG/CR-6850, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* [2]. While NUREG/CR-6850 developed methods, tools and data for performing at-power fire probabilistic risk analysis, it did not identify or produce a method to develop best-estimate human error probabilities (HEPs) given the PSFs and the fire-related effects.

Following the publication of NUREG/CR-6850, a subsequent joint effort produced EPRI 1023001/NUREG-1921, *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines - Final Report* [1] to fulfill the need for explicit HRA guidance on performing both qualitative and detailed quantitative analysis to support best-estimate human error probabilities in fire PRAs. In particular, NUREG-1921 provided tools for performing fire HRA such as:

- Road maps for better understanding the relationship between fire HRA and other fire PRA tasks with respect to both information flow and treatment of fire-induced cable failures or electrical faults
- Search schemes and screening techniques for identifying HFEs to be included in fire PRAs, including operator response to spurious operations of equipment and indications
- Criteria for assessing the feasibility of operator actions, especially those taken outside of the MCR
- Techniques for obtaining or developing more realistic timing inputs
- Identification of previously little (if at all) discussed factors that can influence ex-control room operator actions (e.g., security and keys for locked doors, communication equipment and its reliability)

As the above list illustrates, many of these tools provided in NUREG-1921 focused on operator actions taken outside of the MCR. This guidance in NUREG-1921 is an advance in the current state-of-the-art. Both NRC and industry have taken advantage of this advance, expanding or extrapolating guidance from NUREG-1921 into other areas requiring additional HRA guidance. In particular, NRC-RES has used NUREG-1921 as the basis for its overall HRA approach in its site-wide, multi-hazard Level 3 PRA [4], as well as a new HRA approach for Level 2 HRA/PRA [5]. Also, EPRI based its approach for seismic HRA guidance [6] on NUREG-1921.

While NUREG-1921 represents an advance in HRA practice, NUREG-1921 (see Section 1.2 of Reference 1) does identify a few areas that would benefit from further research, especially treatment of MCRA and associated shutdown strategies.

This report on qualitative MCRA HRA/PRA guidance is intended to partially address this research need. Development of the quantitative aspects of MCRA HRA will be addressed in a future report. Since the development and publication of guidance for MCRA HRA qualitative and quantitative guidance will not be done in parallel, additional updates and improvements to this report (i.e., Supplement 1) are expected. Other improvements might be identified through separate HRA/PRA research projects (e.g., NRC's project to respond to SRM-M061020 [7] on HRA model differences).

1.3 Report Scope

Following publication of NUREG-1921, the industry proposed fire PRA Frequently Asked Question (FAQ) 13-0002 [8] in response to recurring requests for additional information (RAI) from the NRC to plants transitioning to NFPA 805. Transitioning plants were asked to justify the screening value used to quantify MCRA or provide a detailed analysis for MCRA scenarios. The scope of the FAQ intended to address a long-standing concern regarding the use of “screening” HEPs for modeling failure to successfully abandon the MCR due to fire in the MCR and transfer functions necessary to maintain safe shutdown capability to ex-MCR location(s). After considerable effort by both industry and the NRC, ending with the recognition by both that more research was needed, the NRC documented some interim guidance in a memorandum to the Nuclear Energy Institute (NEI) [9] and NEI provided a response to the interim guidance [10].

As evident throughout the FAQ discussions and highlighted in this report, there are many variations between nuclear power plants (NPPs) with respect to MCRA and associated shutdown strategies. This report represents a sampling of these variations but cannot achieve completeness. The authors of this report aim to provide appropriate HRA guidance that can be adjusted for plant-specific MCRA strategies. However, some gaps might be identified that warrant the development of more explicit guidance.

As stated above, this report provides expanded qualitative guidance for MCRA HRA. This guidance has been developed using the experience of the joint EPRI/NRC-RES fire HRA team, along with other industry and regulatory experience as needed. A follow-on report will offer quantification guidance for MCRA HRA.

1.4 Technical Approach

The technical approach used to develop this supplement to NUREG-1921 on qualitative HRA for MCRA and modeling MCRA in fire PRAs consisted of:

- Technical exchange among team members on common and dissimilar experiences in performing or reviewing the assessment of HRAs for MCRA scenarios in fire events, encompassing experiences, such as:
  - Preparing MCRA HRAs and logic models in support of fire PRA development for NFPA 805 licensee amendment requests (LARs) and subsequent RAIs
  - Reviewing MCRA HRAs for NFPA 805 submittals
  - Preparing MCRA HRAs and logic models for non-NFPA 805 risk-informed applications
  - Conducting interviews and walkdowns of MCRA strategies at different NPPs
  - Performing qualitative HRA tasks, including specific activities and results that were either similar to or different from that discussed in NUREG-1921
- Comparing similar or different approaches to MCRA in team discussions and development of a common approach for qualitative HRA and logic modeling
- Discussions of operational experience (e.g., significant fire events, other significant NPP events) that related to development of qualitative HRA guidance
- Conduct of supplemental interviews of NRC staff with operational experience on MCRA strategies and training
- Development of a shared view on MCRA HRA regarding:
  - The unique challenges of modeling MCRA HRA and scenario logic modeling, including the need for additional qualitative HRA beyond the guidance in NUREG-1921
  - Parallels between MCRA HRA and other relatively novel HRAs (e.g., Level 2 HRA/PRA for NPPs, HRA for non-NPP applications such as Yucca Mountain waste repository and U.S. Army chemical weapons destruction facilities)
  - The importance of capturing the current state of knowledge on performing MCRA HRA for both the HRA and PRA communities
  - The importance of properly evaluating and capturing the fire-induced and random failures that can complicate or defeat successful completion of an MCRA scenario
- Review of psychological literature (e.g., NUREG-2114 [11]) to identify or develop an explanatory model for operator response in MCRA scenarios (which differs from that for internal events, Level 1 HRA/PRA in many important ways)

Ultimately, the guidance provided in this report reflects the collective experience of the team.

Finally, recognizing that additional and different experience with MCRA HRA exists outside of the team, the overall project scope included a peer review. Future testing of the quantification guidance is also planned.

1.5 Report Structure

This report is structured to address what additional guidance, beyond that in NUREG-1921 and NUREG/CR-6850, is needed for qualitative HRA/PRA involving MCRA scenarios. In some cases, this report structure coincides with that used in NUREG-1921. In other cases, new topics are addressed (e.g., modeling abandonment in PRA) or deferred to the next phase of guidance development (e.g., HRA quantification).

NUREG-1921 defines qualitative analysis as Step 2 in the overall fire HRA process (given in Section 2.2 of NUREG-1921). Most of the guidance for qualitative analysis is given in Section 4 of NUREG-1921. However, since qualitative analysis supports all HRA tasks, NUREG-1921 qualitative analysis guidance was sometimes repeated in discussion of other steps in the fire HRA process.

The reader should note that, while this report is arranged sequentially, the topics for MCRA qualitative analysis are not sequential or independent. For example, the timing discussion provided in Section 7 is important to all other sections (except this section and the overview in Section 2). Also, the discussions in Section 3, 4, and 5 are interrelated as they all address the development of MCRA scenarios and modeling of operator actions.

In particular, this report is arranged in the following sections and appendices:

- Section 1 (i.e., this section) identifies the objectives and scope of this report and provides background information on the project tasks.
- Section 2 provides analysts with overview information regarding what is unique about the MCRA context and implications for HRA/PRA. Section 2 also describes the interfaces between tasks for modeling MCRA and other fire PRA tasks.
- Section 3 discusses PRA modeling of MCRA, including important interactions and collaborations between HRA and PRA analysts.
- Section 4 discusses the decision to abandon for both LOH and LOC.
- Section 5 discusses the first step defined in NUREG-1921's fire HRA process, identification and definition of HFEs, specifically for the MCRA context.
- Section 6 discusses key changes to HRA feasibility assessment, as needed for MCRA HRA.
- Section 7 provides guidance on the development of timing information needed for MCRA HRA, especially timelines.
- Section 8 discusses PSFs and the different features of PSF categories already identified in NUREG-1921 that must be addressed in MCRA HRA. The issue of "command and control," which is of key importance in MCRA, is introduced in this section, but is discussed further in Appendix B.

- Section 9 discusses recovery analysis, sources of uncertainty, and dependencies for MCRA, paralleling Steps 4, 5 and 6 in the fire HRA process given in Section 2.2 of NUREG-1921.
- Section 10 provides concluding remarks including: a discussion of the properties of a good qualitative analysis, MCRA modeling and HRA checklists, interface with plant operations (including plant modifications, procedure modifications, and training updates), discussion of PRA standard requirements, documentation, and areas for future development.

The appendices are presented in order of expected usage. Specifically:

- Appendix A Main Control Room Abandonment Regulatory Background, Historical Events, and Remote Shutdown Panel Variations
- Appendix B Command and Control
- Appendix C Guidance and Tips for MCRA-Related Information Collection
- Appendix D Insights from Operator Interviews

1.6 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

   Note: When reference is made in this document to NUREG/CR-6850/EPRI 1011989, it is intended to incorporate the following as well:

   Fire Probabilistic Risk Assessment Methods Enhancements: Supplement 1 to NUREG/CR-6850 and EPRI 1011989. EPRI, Palo Alto, CA and the NRC, Washington DC: September 2010. EPRI 1019259.
3. National Fire Protection Association (NFPA) Standard 805, *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants*, 2001 Edition.
4. Kuritzky, N. Siu, K. Coyne, D. Hudson, and M. Stutzke, “L3PRA: Updating NRC's Level 3 PRA Insights and Capabilities,” *Proceedings of IAEA Technical Meeting on Level 3 Probabilistic Safety Assessment,* Vienna, Austria, July 2-6, 2012. (Available through the NRC Agencywide Documents Access and Management System (ADAMS) Accession Number: ML12173A092.)
5. Cooper, S., Wreathall, J., Hendrickson, S., “How to Explain Post-Core Damage Operator Actions for Human Reliability Analysis (HRA): Insights from a Level 2 HRA/PRA Application, *PSA 2015*, Sun Valley Idaho, April 26-30, 2015. Available through ADAMS Accession Number: ML15113A940.
6. *An Approach to Human Reliability Analysis for External Events with a Focus on Seismic*, EPRI, Palo Alto, CA: December 2016. EPRI 3002008093.

7. U.S. Nuclear Regulatory Commission, *Staff Requirements – Meeting with Advisory Committee on Reactor Safeguards,* SRM M061020, November 8, 2006.
8. Nuclear Energy Institute, Fire PRA Frequently Asked Question (FAQ) 13-0002, "Modeling of Main Control Room (MCR) Abandonment on Loss of Habitability," August 2013. Available through ADAMS Accession Number: ML13249A249.
9. Memorandum from U.S. Nuclear Regulatory Commission, Joseph G. Giitter, to Nuclear Energy Institute, Michael D. Tschiltz, dated July 23, 2013, with Supplemental Interim Technical Guidance, ADAMS Accession Number ML14156A522.
10. "Comments and Recommendations on the NRC's MCR Abandonment ISG to Use a Screening HEP of 0.1," Dated April 2, 2014 ADAMS Accession Number ML14127A464.
11. U.S. Nuclear Regulatory Commission. NUREG-2114, *Cognitive Basis for Human Reliability Analysis.* Washington, D.C.: January 2016.

2
OVERVIEW OF MCRA QUALITATIVE HRA/PRA

2.1 Introduction

This section provides an overview of the qualitative HRA/PRA guidance for MCRA scenarios. As is the case throughout this report, this section builds upon the foundation in the Qualitative Analysis section of NUREG-1921 [1].

In particular, discussion is provided on why separate guidance is needed for MCRA, particularly what is unique about the MCRA context and the associated implications for HRA/PRA (see Section 2.2 and 2.3, respectively). Following this discussion, a high-level description is provided of what different HRA guidance is needed (as well as what is the same as for other fire scenarios), using the guidance in NUREG-1921 as the basis. The HRA/PRA steps or qualitative analysis tasks that require even more detailed discussion are identified, then addressed in later sections in this report.

It must be noted that, even more so than the fire HRA guidance provided in NUREG-1921, it is challenging to provide generic MCRA HRA/PRA guidance due to the very plant-specific nature of MCRA strategies.

2.2 What's Unique About MCRA Context(s)?

The contexts associated with MCRA are unique for many reasons, including:

- Being prepared to abandon the MCR is a regulatory requirement for not only fire events, but also other events (e.g., toxic gas intrusion) that make the MCR uninhabitable. (See Appendix A, Section A.1, for a summary explanation of the regulatory requirements.)
- Events that require MCRA are rare, even compared to other events modeled by HRA/PRA. (See Appendix A, Section A.2, for a summary of the very limited historical experience related to MCRA.)
- Unlike the MCRs (which have been almost standardized following post-Three Mile Island 2 design upgrades), remote shutdown panel (RSDP) design varies greatly from one plant to another. In turn, these design differences can result in operational differences, such as:
  - Some plants have one RSDP. A few plants have two RSDPs, although there can be differences between the two RSDPs so far as electrical independence from the MCR. Also, a few plants do not have a designated RSDP and, instead, perform many operator actions at local plant panels.
  - RSDPs vary in their capabilities with respect to which systems and associated equipment can be controlled, and what indications are provided (see Section A.3). In essentially all cases, the capability provided at the RSDP is less than that found in the MCR.

    - For those plants with highly capable RSDPs, relatively few local operator actions will be required to control needed equipment and obtain necessary information. However, even for these NPPs, it is very likely that the requirements for safe shutdown regarding the number of operators, the number of local actions, and the number of locations for these actions will be greater than what would be required if the MCR were not abandoned.
    - In contrast, those plants that have RSDPs with limited capability are likely to require many local operator actions in multiple locations in order to perform equipment manipulations and monitor and/or check local indications. This case represents an even greater difference as compared to a plant shutdown from the MCR.
  - At many NPPs, operators will need to abandon the MCR because certain equipment can no longer be operated or certain instrumentation can no longer be viewed from the MCR. At other NPPs, operators may not need to abandon the MCR, because control of that specific equipment can be individually transferred to the RSDP.

- Typically, there is no indicator or explicitly defined cue that is used to determine when the MCR must be (or would be) abandoned. (Several sections address this topic, including Section 3 on PRA modeling, Section 4 on the decision to abandon, and Section 8 on performance shaping factors.)
- MCRA scenarios span three different contexts, involving different time frames (see Section 7 on timing) and locations:
  - In the MCR - before, during, and immediately after the decision to abandon
  - At the RSDP - after abandonment
  - At local panels or equipment in the plant - after abandonment

2.3 Implications of MCRA Context(s) for HRA/PRA

Although HRA/PRA guidance has recently evolved to include fire events (and other external hazards, by extension), the guidance needed for MCRA scenarios is different from what has already been developed. Some of the aspects of MCRA, such as distributed response and coordinated actions amongst multiple locations, have been considered in HRA/PRA applications (especially for non-nuclear power PRAs[2]). However, no formal guidance for these similar contexts has been developed prior to this document. (NRC is currently developing generic HRA guidance, IDHEAS-G [3], which could assist HRA analysts in understanding new contexts, developing associated new HRA quantification tools, and performing novel applications.)

[2] Examples of such applications where there is a “distributed” response and the need to coordinate amongst multiple locations include PRAs performed for the Yucca Mountain Repository surface facilities (See Reference 2), the U.S. Army Chemical Demilitarization Facilities, and various petro-chemical facilities in the U.S..

There are many reasons why MCRA HRA/PRA requires different guidance, and some of these are interconnected. High-level reasons for requiring additional guidance for MCRA include:

- MCRA is a special case of fire PRA that does not build directly from internal events HFEs (even though it may contain similar actions). The decision to abandon is typically captured by a unique procedure that is likely to be separate from the fire response procedure set.[3] The potential for involvement of multiple operators performing distinct but correlated tasks outside the MCR makes the abandonment scenario a challenging analysis for both the fire PRA and HRA. (See the bullet below for more on procedures for MCRA versus those typically addressed in HRA.)
- There are many implications for HRA when the control room crew leaves the MCR, going well beyond a simple location change for operator actions. Some of these implications include:
  - For US NPPs, response to the Three Mile Island 2 (TMI-2) event has resulted in standardized requirements for MCR design, emergency operating procedures (EOPs) (in format, content, etc.), and operator training. As a result, HRA analysts can assume (but should verify) that the MCR environment provides a high level of support to MCR operator actions. However, that same level of support cannot be expected for MCRA scenarios. As a matter of fact, the HRA analyst should expect that every NPP's RSDP is unique in its design, capabilities, and limitations.
  - Almost all HRA methods have been based on assumptions related to the fact that decision-making, and most other operator actions, are taken in the MCR. However, one common HRA assumption that cannot be used for MCRA scenarios, is that the MCR crew can be modeled as if it were a single entity. This assumption is justified for almost all other PRA scenarios (except Level 2 PRA) by the way the MCR operating crew works as a team and is supported by, for example:
    - MCR design
    - Frequent operator training
    - Real-time and face-to-face, 3-way communication
    - In many cases, all crew members are working off the same procedure and providing backup to other crew members
  - When command and control resides in the MCR, decision-making (and any operator actions taken) is supported by many alarms, indications, and other instrumentation. In addition, decision-making by the Shift Supervisor (or Shift Manager) is supported by additional management or staff, either required to be present (e.g., the Shift Technical Advisor [STA]) or expected to respond to a serious plant upset. Such support and extra help (as well as multiple phones) also eases the burden of necessary communications, whether it be fire brigade updates, notifications to the NRC, or reports back from field operators or health physics. However, in MCRA scenarios, command and control is likely to lose some of these supports. For example, staffing assignments may change during MCRA due to fire brigade responsibilities (although plants are required to ensure

[3] See Appendix A for a background discussion on the regulatory requirements for MCRA.

that a basic level of staffing is maintained) and procedure assignments. Consequently, command and control in MCRA scenarios typically must rely upon a different level and mode of information acquisition, staffing, and communications. Appendix B provides background on the topic of command and control.

- Treatment of MCRA may not rely on the typical assumption that fire initiation, reactor trip, and the "start of the scenario" (from an operations perspective) are simultaneous. Instead, proper HRA treatment of MCRA needs to include explicit consideration of these scenario milestones since it is possible they may occur at different times.
- The definition of a MCRA scenario for LOC requires significant input from operators and operations personnel who would be making the abandonment decision rather than solely being based on plant conditions, associated engineering calculations, etc. HRA input is crucial for the proper definition of MCRA scenarios, rather than the typical situation in which the PRA analysts have the lead in scenario definition and development.
- The MCRA shutdown strategy will almost certainly involve a greater number of operator actions, with a correspondingly greater number of action locations and need for a greater number of operators to perform those actions. In many cases, this means that assessment of the shutdown strategy requires consideration of the feasibility of the coordinated operator response, as well as the feasibility of individual operator actions. The resulting feasibility assessment requires consideration of multiple timelines that represent each operator/operator action, including important coordination points or other intersections.
- The greater number of local (i.e., "in the field") operator actions, plant-specific differences with respect to shutdown strategy, overall design (including design of the RSDP), plant layout, and equipment are even more important than for those fire scenarios that principally involve operator actions in the MCR.
- NPP operators are familiar with many "rare events" due to their frequent simulator training, but they may consider MCRA scenarios even less credible. To date, no MCRA events have occurred in the U.S, and realistic simulator training of MCRA scenarios (including representative communications with field operators) is uncommon. Such limitations in operational experience are likely to impact what input can be collected in interviews with operations personnel, how such input can be collected, and how to use such information. (Appendix A provides additional background information on MCR abandonment regulatory requirements and near miss events.)

2.4 NUREG-1921: What's the Same and What's Different for MCRA?

This supplement to NUREG-1921 is specifically focused on HRA/PRA for MCRA scenarios. Consequently, NUREG-1921 remains the recommended HRA guidance for supporting non-MCRA scenarios in fire PRA.

In general, the reader can assume that, if this report does not address a certain topic or issue, then the guidance in NUREG-1921 still applies. Specific topics or issues that will be explicitly addressed for MCRA scenarios in the remaining sections include:

1. The fire HRA process,
2. Relationship with other fire PRA tasks, and
3. General assumptions.

In addition, Appendix C provides support material for qualitative analysis for MCRA scenarios, such as addressing plant-specific information collection and managing resources for performing MCRA HRA.

2.4.1 Fire HRA Process

Section 2.2 in NUREG-1921 provides a process for performing fire HRA that is comprised of seven steps and associated sub-steps shown in Figure 2-1. All of these steps are relevant and applicable to performing HRA for MCRA scenarios.

However, treatment of MCRA often requires that the HRA task provide input to the overall fire PRA for the appropriate development of MCRA scenarios. In other words, the HRA analyst may be tasked with performing tasks traditionally assigned to the accident sequence analyst, for example.

For simplicity, this supplement to NUREG-1921 treats the HRA process as unchanged,[4] but recognizes that greater HRA input and interaction with the larger fire PRA is required (which also implies some alteration of the fire PRA guidance given in NUREG/CR-6850 [6]).

This report is particularly focused on supplementing NUREG-1921 with MCRA-specific guidance related to Steps 1 and 2 (and associated sub-steps), HFE Identification and Definition (Step 3) and Qualitative Analysis (Step 4). Figure 2-2 pictorially represents the flow of information between the various report sections for the MCRA process. This process diagram indicates the progression between the various tasks described in the report as well as any additional guidance provided in NUREG-1921 [1].

[4] By making this choice, the fire HRA and fire PRA process diagrams remain the same, but guidance for how various tasks are performed is changed to address MCRA. However there are HRA methods (such as ATHEANA [4,5], specifically Step 3, that is titled ‘describe the base case scenario’) that include steps that overlap with PRA scenario development.

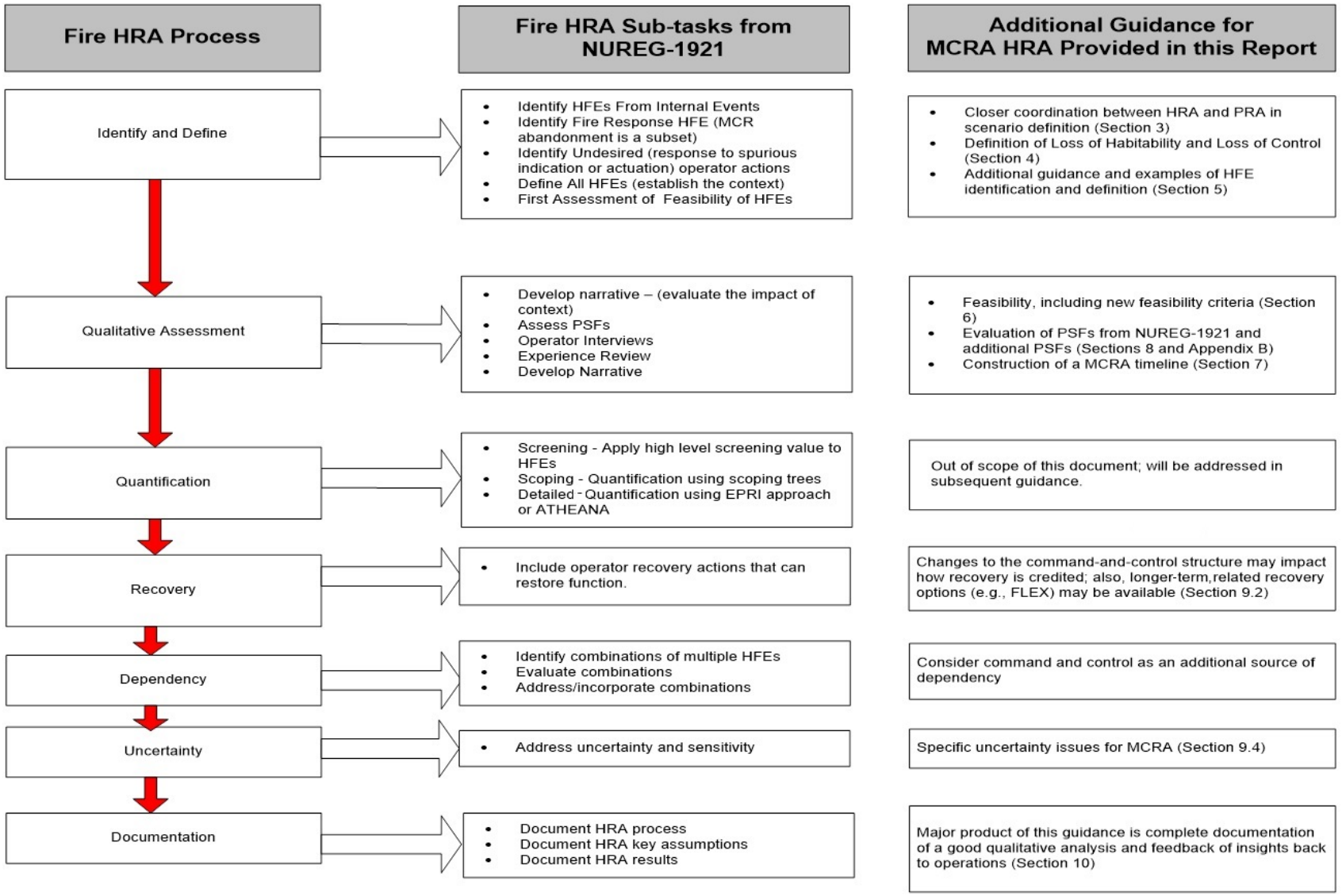


Figure 2-1
NUREG-1921's fire HRA process steps and sub-steps

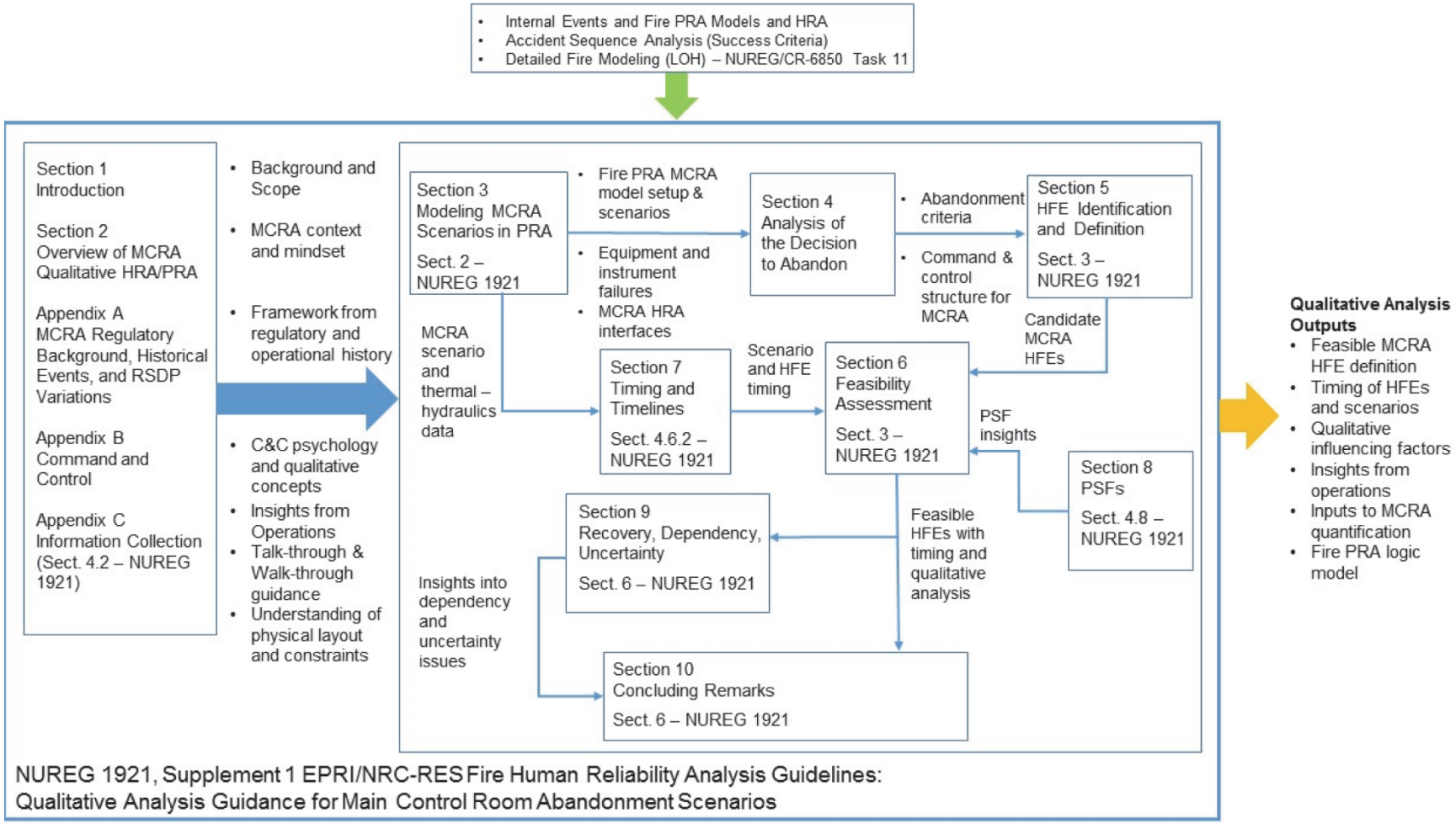


Figure 2-2
MCRA inputs and outputs roadmap

2.4.2 Relationship with Other Fire PRA Tasks

Section 2.3 in NUREG-1921 discusses the relationship between fire HRA and other fire PRA tasks. As part of this discussion, Figure 2-2 and Table 2-1 in NUREG-1921 [1] illustrate where fire HRA fits into the overall fire PRA development and how information (e.g., inputs and outputs of various tasks) flows between fire HRA and fire PRA. Table 2-1 below is an abridged version of Table 2-1 in NUREG-1921, showing only the specific aspects of that table that have additional guidance addressed in this document.

Table 2-1
Fire PRA/fire HRA task interfaces addressed in this report

NUREG/CR-6850 [6] Fire PRA Task	Combined ASME/ANS Fire PRA Standard [7] Element (Category II)	Additional MCRA PRA/HRA Guidance
3. Cable Selection	Cable Selection	Ensure that the cables associated with the RSDP and any credited local instrumentation are evaluated in accordance with requirements of the standard.
5. Fire-Induced Risk Model	Plant Response Model	Integrate HFEs for MCRA-specific fire scenarios, depending upon binning strategy. Define the needs for thermal-hydraulic calculations to support the development of MCRA-specific timelines. Proper inclusion and integration of MCRA-specific equipment failures into the logic model.
12. Fire HRA	Human Reliability Analysis	Substantial new guidance is addressed in this document.

2.4.3 General Assumptions

Section 2.4 of NUREG-1921 provides five general assumptions applicable to performing fire HRA. All of these assumptions are also applicable to MCRA HRA/PRA.

One other important assumption used in NUREG-1921, carried over from NUREG/CR-6850 [1, 6] is that the start of the scenario (i.e., t=0) occurs simultaneously with the start of the fire. This assumption is a common simplification in PRA (including for other initiating events that do not necessarily result in an immediate reactor trip). For MCRA HRA/PRA, this assumption may not be applicable in all cases as noted in Section 4.6.2 of NUREG-1921 [1] and further reinforced in Section 7.3.2.

2.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. U.S. Department of Energy, *Yucca Mountain Repository License Application: Safety Analysis Report.* DOE/RW-0573, Revision 0. June 2008.
3. U.S. Nuclear Regulatory Commission. *The General Methodology of An Integrated Human Event Analysis System (IDHEAS),* ADAMS Accession Number ML16074A389, February 2016. NUREG-2198 (draft).
4. U.S. Nuclear Regulatory Commission. *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA),* Rockville, MD, May 2000. NUREG-1624, Revision 1.
5. U.S. Nuclear Regulatory Commission., *ATHEANA User's Guide,* Washington, D.C., June 2007. NUREG-1880.
6. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

   Note: When reference is made in this document to NUREG/CR-6850/EPRI 1011989, it is intended to incorporate the following as well:

   Fire Probabilistic Risk Assessment Methods Enhancements: Supplement 1 to NUREG/CR-6850 and EPRI 1011989. EPRI, Palo Alto, CA and the U.S. NRC, Washington DC: September 2010. EPRI 1019259.
7. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008*, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,* The American Society of Mechanical Engineers, New York, NY, February 2009.

3
MODELING MCRA SCENARIOS IN FIRE PRA

This section describes the modeling of MCRA scenarios in a fire PRA. Although the primary focus of the section is on the PRA modeling, there is an important discussion about the interface between the PRA modeling and HRA. While this need exists in all aspects of PRA, it is perhaps much more acute for MCRA than for other aspects. Therefore, the HRA analyst should become familiar with and understand the content of this section. Conversely, the fire PRA analysts[5] should not assume that limiting themselves to this section will suffice to understanding all the needs and limitations faced by the HRA analysts. While it is not necessary to understand the details of all of the HRA modeling issues addressed in Sections 4 through 10 of this report, the analysts performing the fire PRA modeling should have a general understanding of the contents of those sections because there are certain aspects that affect the development of the model.

3.1 Introduction

The objective of this section is to provide a better understanding of how to address the aspects of the various MCRA requirements in sections of the ASME/ANS PRA Standard [1] that, by their very nature, apply to MCRA. In particular, this section provides guidance on: 1) the fire scenario selection (FSS), which includes the identification, definition, and fire modeling of fire scenarios, and 2) the plant response model (PRM), which includes the fire PRA logic model development and quantification. Meeting this objective is accomplished by expanding on the MCRA procedure and guidance in NUREG/CR-6850 [2]. The need for this additional guidance results from experience gained through fire PRA peer reviews and RAIs from NRC to licensees on their NFPA 805 LARs. This experience has made clear that, although the HRA associated with MCRA is not the most significant issue, there are important PRA modeling issues that affect the results of the analysis that are often missed or modeled improperly. This section provides insights on the current state-of-practice for these MCRA PRA modeling issues. In order to develop the qualitative analysis for any given MCRA scenario, the modeling starts with the PRA. Fire modeling identifies equipment damaged by the fire. For each postulated fire scenario, the impact on the plant equipment is derived based on the cables and/or components lost in the fire. This provides inputs to the HRA to establish the context for the actions to be taken, which is required to perform the qualitative and quantitative analyses.

[5] In the context of this report, fire PRA analysts include both those individuals who build and quantify the logic model and those who conduct the fire scenario modeling calculations.

For fires that progress to the point of requiring MCRA, the design basis plant response is to shut down at a RSDP or Local Control Stations (LCS) outside of the MCR. The procedure used to accomplish safe shutdown is designed to mitigate most, if not all, of the effects of fire including spurious component operations and to provide sustained decay heat removal. The overall process of abandoning the MCR and re-establishing decay heat removal mitigates the effects of the fire (except for fire-damaged components that cannot be recovered).

The modeling guidance considerations that need to be addressed for MCRA are:

1. The plant conditions that would constitute a LOC or LOH for the specific plant are defined based on HRA operator interviews and procedure review. Appropriate logic is then included in the model to capture when those conditions occur.
2. Based on the fire modeling for the MCR, the scenarios that would result in a LOH are determined. Generally, abandonment actions are credited only for these scenarios. In other words, analysts should not credit actions in the MCR that are absent from the abandonment procedure(s), even if they appear in other procedures, unless those procedures are directly entered from the abandonment procedure(s). The exceptions to this guidance are “immediate actions” that are typically performed from memory.
3. Random failures of equipment required for remote shutdown (including the controls located at the RSDP) should be included in the model.
4. Mitigatable fire-induced failures of equipment required for remote shutdown (including the controls located at the RSDP) should be included in the model. This requires analyzing the circuits[6] of the RSDP to determine if any abandonment scenarios can cause failure.
5. Non-mitigatable fire-induced failures of equipment required for remote shutdown should be included in the model. These would include spurious operations that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed).
6. For scenarios modeled with detailed fire modeling, detection and suppression should be accounted for in the model to the extent that they are required to ensure realism in the dominant scenarios.

This section considers three approaches to appropriately address the MCRA modeling considerations noted above. The primary approach, which is addressed in Sections 3.2 through 3.6, is integration of the MCRA modeling into the plant logic model for the fire PRA. This approach is typically consistent with the other fire PRA scenarios and improves traceability and documentation. The two other approaches, discussed in Section 3.7, use scenario bins or a single bounding MCRA failure probability for all recoverable MCRA scenarios.

[6] Circuit analysis should be performed in manner that meets the requirements of the ASME/ANS PRA Standard.

This section is organized as follows:

- Section 3.2 - Modeling Considerations for Crediting Abandonment
- Section 3.3 - Success Criteria Development
- Section 3.4 - Incorporating the HFEs into the model
  - Decision to Abandon
    - LOH
    - LOC
  - Actions to transfer command and control to the remote shutdown location(s)
  - Actions that take place following abandonment
    - Discussion of interface between the logic model development and HRA to determine HFEs
    - Identification of actions in procedures, including distinctions between risk-significant steps and those that are not required to reach a safe-and-stable end state
- Section 3.5 – Incorporating Equipment Failures into the Model
  - Conditions beyond the capability of the RSDP equipment and procedures
  - Random and fire-induced failure of RSDP and/or local stations
  - Random and fire-induced failure of required equipment
    - Recoverable (generally only fire-induced failures may be recoverable)
    - Non-recoverable (random failures or fire-induced damage such as due to spurious operations)
- Section 3.6 – An Example of a Detailed Integrated Logic Model
- Section 3.7 – Alternate Approaches
  - Use of a single value for all abandonment scenarios
  - Use of scenario bins

3.2 Modeling Considerations for Crediting Abandonment

The first part of the modeling effort is to identify those scenarios that create conditions that may result in the need for MCRA. There are two types of scenarios where such credit for MCRA can be taken: 1) those that result in the MCR becoming environmentally uninhabitable due to heat or smoke (referred to LOH scenarios), and 2) those that result in a loss of ability to successfully prevent core damage from the MCR (referred to as LOC scenarios).[7] Section 4 discusses the decision to abandon for both cases.

Fires that occur in the MCR can lead to both types of scenarios (LOH and LOC), depending on the location and severity of the fire. Generally, fires that occur in electrical cabinets ancillary to the primary safety systems (e.g., "back panels") will only lead to LOH scenarios since, absent the LOH, the MCR will remain functional (even if the cabinets are damaged by the fire). Fires on key panels containing circuits interfacing with important front line systems (e.g., main control board panels containing reactor systems or support system circuits) can lead to LOC or to LOH. In some cases, a fire causing LOC could grow large enough to also result in LOH. In such a case, the scenario would be modeled as LOH, with the LOC failures being treated as consequential failures. This is because the LOH would be the overriding reason for leaving the MCR. (Such cases are discussed later in this section.)

Fires in other plant locations (e.g., relay room, cable spreading room (CSR), and cable tunnel/chase/corridor) typically only result in LOC scenarios. If adequate smoke and fire barriers exist, it is unusual for a fire in one of these areas to result in LOH in the MCR. However, it is worth noting that historical events [3] show that smoke can migrate to the MCR from fires outside the MCR. Therefore, while this usually does not result in sufficient smoke to reach LOH conditions, it should be confirmed that the plant does not have migration pathways for smoke or fire that could result in a LOH for fires that start in other areas (and that these areas can support a large enough fire) before dismissing the possibility. This assessment would be part of the fire modeling activities for MCRA, as discussed in Section 3.2.1.

3.2.1 General Considerations for Detailed Fire Modeling (NUREG/CR-6850 Task 11)

Regardless of the type of MCRA scenario (LOH or LOC), detailed fire modeling plays a key role. Task 11 of NUREG/CR-6850 provides separate procedures for the detailed fire modeling within individual plant areas, for MCR fires, and for the multi-compartment analysis. The goal of Task 11 is to provide detailed modeling of risk significant scenarios, including detailed analysis of fires, and those scenarios that can result in MCRA whether they occur in the MCR or in other plant areas. The results of Task 11 are estimates for the frequency of fire scenarios involving a specific ignition source failing a target set[8] before fire protection can prevent damage to the

[7] The LOC may occur from fire-induced failures or from fire-induced failures plus one or more random failures. The operators would have no way to make the distinction – they only know that they have lost control and are unable to re-establish control from the MCR. Therefore, their decision to abandon the MCR is unaffected by why the LOC occurs. As a practical matter, however, the LOC scenarios that include additional random failures will tend to be lower frequency and thus not significantly impact the overall risk from MCRA scenarios.

[8] A target set as defined in the ASME/ANS RA-Sa-2009 [1] *is a group of damage targets that will be assumed to suffer fire-induced damage based on the same damage criteria and damage threshold in any given fire scenario.*

target set. This result is combined in the PRA quantification steps to determine the conditional core damage probability (CCDP) or conditional large early release probability (CLERP) given failure of the target set. Multiplying the fire scenario frequency by the CCDP or CLERP provides an estimate of the CDF or LERF contribution for each fire scenario.

The detailed fire modeling task has been divided into sub-categories in NUREG/CR-6850 [2]:

1. Single compartment fire scenarios (Section 11.5.1),
2. MCR fire scenarios (Section 11.5.2),
3. Subsets of 1 and 2 that result in LOC (Section 11.5.3), and
4. Multi-compartment fire scenarios (Section 11.5.4).

Of these, items 2 and 3 are the most relevant to MCRA. For item 2 (i.e., fires in the MCR), the existing discussion in NUREG/CR-6850 for LOH provides guidance that requires minimal clarification. Item 3 (i.e., fires that result in LOC) is treated very briefly in NUREG/CR-6850 and has a lack of clear guidance. Experience has shown that this lack of adequate guidance is the biggest problem leading to misrepresentation of LOC in MCRA analyses. Therefore, this report provides that needed guidance.

Fire HRA guidance is addressed in NUREG-1921 [4]. The NUREG-1921 guidance is quite clear in the case of scenarios that do not result in MCRA. For those that do result in MCRA, the experience has been that the guidance is not as clear. In other words, for fires that do not require abandonment, use of the FSS and PRM guidance in NUREG/CR-6850 and the HRA guidance in NUREG-1921 is applicable and sufficient. For MCRA scenarios, this guidance is not sufficient and Section 1.2 of NUREG-1921 identifies MCRA HRA as an area requiring additional research.

Figure 3-1 shows where the guidance for the MCRA FSS/PRM and HRA fits within NUREG/CR-6850 Task 11, NUREG-1921, and this report. Of particular note is that Section 11.5.3 of NUREG/CR-6850 provides no guidance on MCRA for LOC from an FSS perspective, and that Task 5 of NUREG/CR-6850 provides no guidance for building the model for abandonment scenarios.

Note that some in the industry refer to certain scenarios as “partial abandonment.” This phrase has been used to denote scenarios where procedures call for dispatching certain operators from the MCR to the RSDP or to other stations to perform local actions to compensate for degraded instrumentation or controls in the MCR. However, command and control for these scenarios resides in the MCR. Consequently, the guidance in this report does not acknowledge “partial abandonment;” there are only abandonment and non-abandonment scenarios. Abandonment occurs when command and control passes from the MCR to the RSDP (or its equivalent), so the scenario presented above is simply a non-abandonment scenario, albeit a complex one. The guidance in this document does not cover such scenarios, since dispatching people to the RSDP (or other location) while staying in the MCR is similar to sending people from the MCR to perform other local actions in other situations (even internal events). So, additional guidance for this situation was not needed (i.e., NUREG-1921 provides sufficient guidance for these scenarios).

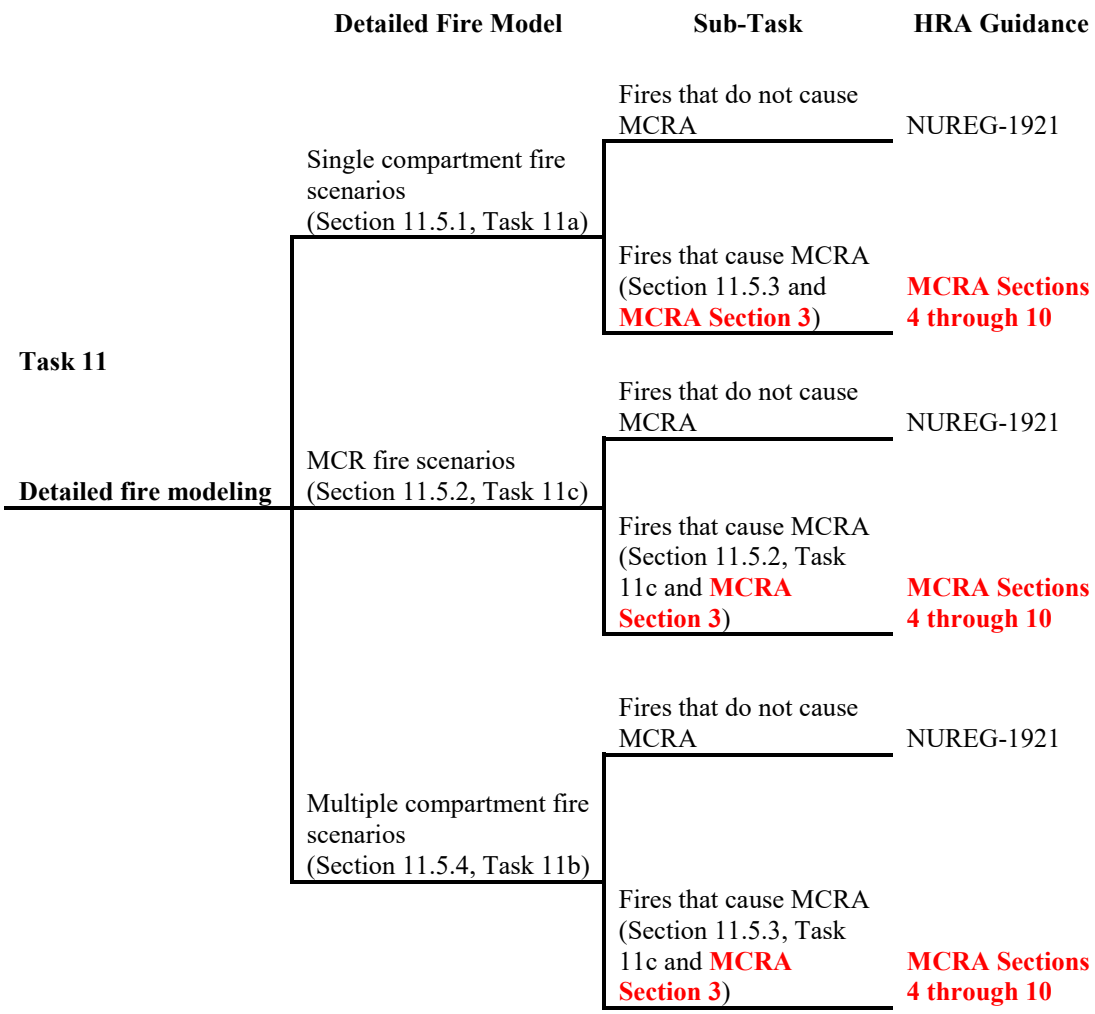


Figure 3-1
Relationship between NUREG/CR-6850 Task 11 and applicable MCRA guidance

3.2.2 Fire Scenario Development for MCRA (NUREG/CR-6850 Task 11)

For fires leading to MCRA, NUREG/CR-6850 follows the same eleven step process used to perform the detailed fire modeling for individual areas. This process is depicted in Figure 3-2.

When following this process, fire compartment details are collected in Step 1, then detailed fire modeling occurs in Steps 2 through 9. The plant response model, specifically the failure probability for using alternate shutdown features, is developed in Step 10. Step 11 concludes the process with documentation.

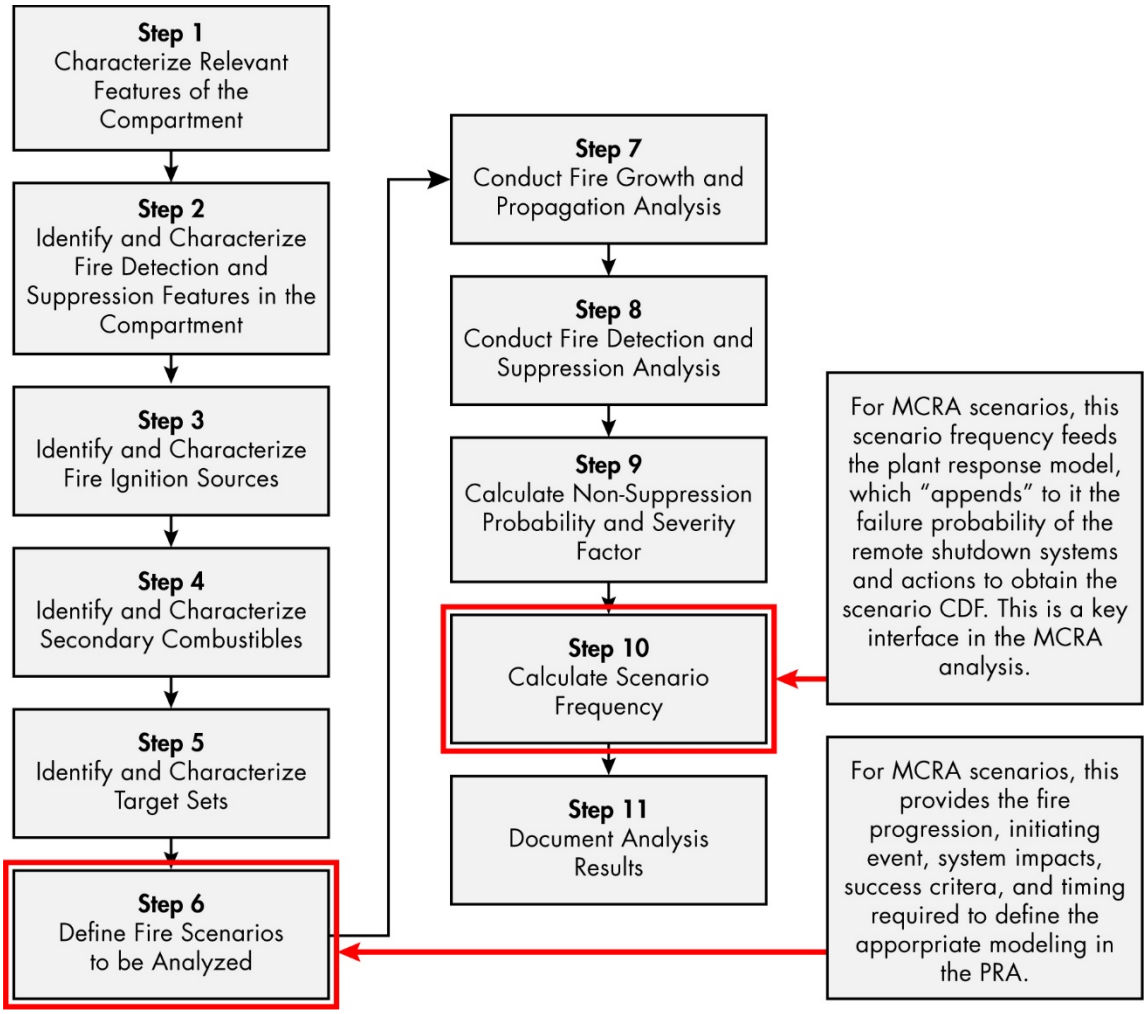


Figure 3-2
NUREG/CR-6850 Task 11 flow chart

Step 6 in Figure 3-2 is the point where the distinction is made between an abandonment and a non-abandonment scenario. Both types of scenarios start with the same initiator (i.e., a fire occurring at a specific ignition source). Abandonment scenarios can be of two different types based on the location of the ignition source: 1) in the MCR, or 2) in one of the designated plant areas that are recognized as triggering conditions that might require MCRA. These fires can follow either the upper or lower branch in the third column of Figure 3-1. All other fires only follow the upper branch. Fire modeling will determine how long it takes for a fire to reach the point where a LOH or LOC condition exists. Fires that are suppressed before that time are non-abandonment scenarios (upper branch) and fires that are not suppressed in time are designated to be abandonment scenarios (lower branch).

As noted in Figure 3-2, Step 10 is the point at which the fire scenario development for MCRA interfaces with the plant response model (PRM) and the HRA. This step, described in Section 11.5.2.10 of NUREG/CR-6850 [2], provides a basic understanding of how MCRA fits within the overall fire PRA. The guidance in this section is intended to expand on the NUREG/CR-6850 discussion to assist the analysts in implementing the process shown in Figure 3-2. NUREG/CR-6850, Section 11.5.2.10 states [2]:

Estimate Failure Probability of Using Alternate Shutdown Features

To eventually quantify main control room fire risk, the possibility of safe shutdown using the alternate shutdown means (i.e., safe shutdown from outside the control room) should be included in the analysis. Two different approaches may be followed.

1. An overall failure probability is estimated representing the failure of the alternate shutdown means.
2. The alternate shutdown procedure is integrated in the plant response model (i.e., the fault - trees and event trees). The core damage sequences are adjusted to include failures associated with alternate shutdown means, and the human error probabilities are reevaluated based on the alternate shutdown procedures.

The first approach (that is, the use of an overall probability value) can be used if the probability value is evaluated conservatively and a proper basis is provided. This approach was used in several IPEEE submittals. For example, in many cases, 0.1 was used as a point value estimate for the probability from reference [11.3] *Perspective Gained from the Individual Plant Examination of External Events (IPEEE), 2002.*

For the second approach (i.e., integrating the alternate shutdown procedures in the plant response model), the following steps are suggested. The first step is to review the applicable procedures and associated documentation. This review should identify the preferred equipment for safe shutdown, and the operator actions necessary to actuate and control them. (If the procedure identifies backup equipment, the corresponding shutdown method should also be evaluated.) If a timeline is not provided in the procedure or other associated documents, a general timeline of key operator actions should be developed. The operator actions performed in the control room and automatic system actuations upon which the timeline is based should also be identified. This step, in effect, establishes the "design basis" or capability of alternate shutdown features.

The second step is to verify that alternate shutdown capabilities satisfy the potential accident sequences associated with the postulated target set damage. Both the available equipment and the timeline for planned actuation should be evaluated.

To evaluate the planned timeline, accident sequence timing modeled in the plant model (i.e., fault trees and event trees) should be compared with the alternate shutdown procedure timeline. The comparison should ensure that the planned operator action times upon which alternate shutdown procedures are based will be less than the operator actuation or recovery times postulated for the applicable fire-induced accident sequences.

Consideration should also be given to how the timeline might change under various failure conditions. For example, if the procedure assumes that auxiliary feedwater is available and actuated from the control room, the analyst may need to consider the possibility of a stuck-open safety relief valve, thus significantly changing the time available to recover failed auxiliary feedwater system. As another example, a fire in a portion of the main control board may cause a RCP seal LOCA in excess of normal

> makeup capability. Complicated operator actions are generally necessary to safely shut down the plant under such conditions. This is further complicated if the alternate shutdown procedure has to be implemented.
>
> Clearly, the timelines and especially comparison of the timelines between those in the fault tree and event tree models and the alternate shutdown procedures should be used to establish the human error probabilities. Furthermore, if needed, those times can be used to quantify dynamic human actions or evaluate the feasibility of recovery actions, should random equipment failures occur.

The second approach mentioned in the quote above is the preferred approach and, therefore, is the primary focus of this section. The first approach may be used in situations where MCRA scenarios are not dominant risk contributors since it is conservative for most scenarios. However, as stated in Section 5.1.3 of NUREG-1921, a feasibility assessment of the operator actions in the scenarios must also be performed.

3.2.3 Crediting MCRA for Loss of Habitability Scenarios

MCRA due to LOH refers to the scenario(s) in which operators may be forced to leave the MCR due to fire-generated conditions. Section 4, which addresses the decision to abandon the MCR, also briefly discusses this type of MCRA scenario.

The determination of which scenarios to credit MCRA for LOH situations is a direct result of fire modeling calculations. The FSS process discussed in Section 3.2.1 is followed to determine how long a fire would need to burn in order to reach those conditions. This is performed for each ignition source in the MCR.[9] The LOH scenario frequency is determined by applying the non-suppression probability associated with the amount of time it takes to reach LOH criteria (i.e., if the fire is suppressed before that time is reached, then the LOH condition is assumed to not exist). In some cases, a given ignition source cannot result in LOH, in which case there is no LOH scenario associated with that ignition source.

The LOH threshold criteria and basis are discussed in detail in Section 4.1, “Loss of Habitability.” The fire PRA assumes that the operator will stay in the MCR as long as possible, even if the use of a breathing apparatus is necessary, until conditions related to smoke and heat levels are met. Because of the conservative nature of these conditions (i.e., the criteria have the underlying assumptions that the operators will remain in the MCR until they are in pain or until they cannot see annunciators, even when leaning very close to the panels to read instruments, gauges, and signs), the amount of time that remains available to perform the required post-abandonment actions is minimized. The likelihood of abandonment is then governed by the probability of a fire that can generate such conditions. Consequently, the conditional probability of abandonment upon reaching the habitability criteria is set to 1.0.

The PRA logic model needs to be set up so that the failure of the operators or equipment to mitigate the LOH MCRA scenario is only applied to those scenarios that are determined by the fire modeling to result in exceeding the LOH criteria. The time of abandonment (as calculated by the FSS process) for each scenario is a key input to the HRA. This time is scenario-specific based on the specific characteristics of the ignition source, available combustibles, and location

[9] In rare cases, it may be possible for a fire that is not in the MCR to result in a LOH in the MCR. Detailed fire modeling is used to determine the time until those conditions are reached.

of the fire within the MCR. This time will impact the HRA because it changes the amount of time operations can be performed in the MCR as well as the remaining time to affect a successful remote shutdown after the MCR is abandoned. How this information is used in the development to the MCRA timeline(s) is discussed in Section 7.

3.2.4 Crediting MCRA for Loss of Control Scenarios

The plant model logic needs to determine scenarios where LOC may occur, and then allow consideration of the actions and equipment required to accomplish remote shutdown under these conditions. For example, in internal events PRA for a pressurized water reactor (PWR) that has a once-through cooling (i.e., bleed-and-feed) procedure, the model is structured such that this cooling procedure is only credited when there is a non-recovered, total loss of secondary cooling that results in certain parameters being exceeded. Modeling of a fire-induced LOC should follow a similar approach, but the situations are less clear since LOC is not a consistently defined scenario from plant-to-plant in the same way that loss of secondary cooling scenarios are. What is important from the modeling perspective is that the conditions that are considered to represent a LOC for the specific plant need to be determined, and model logic implemented such that it only credits MCRA for LOC when the cues associated with those conditions are present. Typical PRA modeling assumes that all fire-induced failures for any given scenario occur concurrently,[10] including the fire-induced plant trip. In addition, the time of abandonment does not change with LOC scenario, as it is the time it takes the operators to confirm the LOC and make the decision to abandon (which should be same for all scenarios if consistent cues for LOC are identified). This timing will come from the HRA, not from the fire modeling.

For LOC, fire modeling only provides fire-induced failures and provides inputs to the thermal-hydraulic analysis that determines when the LOC conditions are reached given those failures. However, the HRA determines: 1) how long it takes the operators to react to these conditions, 2) how long it takes the operators to determine that the conditions correspond with an LOC scenario, and 3) how long it takes the operators to decide to abandon. All three of these HRA determinations are independent of fire modeling.

These cues for LOC do not usually come directly from the abandonment procedure in the same way as they come from AOPs and EOPs. The abandonment procedure does not generally provide unambiguous cues for abandonment (i.e., when parameter x reaches value y and alarm z occurs that are typical for most accident conditions). Some guidance along these lines may appear in the procedure, but in the end there is always a certain amount of discretion given to the final decision maker (e.g., shift manager) to declare when it is no longer possible to successfully reach a safe-and-stable condition from the MCR. For this reason, the determination of the cues for LOC requires significant interaction between the PRA analyst, fire modelers, and HRA analysts, since (as noted above and confirmed by operator interviews) the MCRA procedures generally do not contain the same specificity of cue-response as other AOPs and EOPs. It will be necessary for the logic modeling and fire modeling analysts to provide insights into the expected

[10] This is standard PRA practice, not just for fire, but for all hazards assessed in a PRA. The fault tree model is not dynamic as regards time. Just as failure to run basic events are assumed to occur at T=0 even though they could actually occur at any time during the mission time, so are fire-induced failures. This assumption is conservative because it results in the highest core heat levels that need to be dissipated following plant trip (no credit for systems running for some time period after the trip) and thus the shortest amount of time available to take mitigating actions.

fire-induced failures that will dominate the LOC scenarios. LOC scenarios are those that will lead directly to core damage if the operators remain in the MCR (i.e., in the absence of operator actions taken following abandonment). For each LOC scenario (or group of scenarios that share the same characteristics) that would lead to core damage in the absence of abandonment actions, the HRA analysts will need to conduct operator interviews to determine if the abandonment procedures and equipment cover these situations and also whether the operators would interpret the conditions as a LOC. The HRA team would then define the specific cues/ conditions that the operators would interpret as LOC, and the PRA analyst would implement logic in the model that would allow MCRA credit when (and only when) those cues/conditions exist. The details of the interview process and how it is used to determine the cues that may lead operators to abandon are contained in Section 4.3.3.

3.3 Success Criteria Development

There are two aspects of success criteria that are important for MCRA scenarios.

The first is determining if there is a relationship between the success criteria for the internal events PRA initiating events and the characteristics of the MCRA scenarios. In general, the following three guidelines apply:

1. If the characteristics of the MCRA scenario maps to an internal events PRA initiating event, use the success criteria from the internal events PRA.
2. If the characteristics of the MCRA scenario maps to multiple internal events PRA initiating events, either use the limiting success criteria from the internal events PRA or split the fire into multiple scenarios and apply the appropriate criteria to each.
3. If the characteristics of the MCRA scenario do not map to the internal events PRA (e.g., spurious operation leads to an initiating event not explicitly modeled in the internal events PRA), then either develop success criteria specifically for that particular scenario or choose bounding success criteria from the internal events PRA.

The appropriate success criteria needs to be selected so that each scenario is appropriately addressed. It may be that a combination of all three of these options will be used, depending on the MCRA scenarios.

The second important aspect of success criteria is that, even if MCRA scenarios map to success criteria from the internal events PRA, these scenarios may need special consideration when it comes to the success criteria for achieving successful remote shutdown because: 1) the impacts of the fire may be unique compared to the internal events PRA model, and 2) only limited equipment is available from the RSDP. In particular, bounding success criteria used for the internal events PRA or non-MCRA scenarios in the fire PRA may be too conservative with regard to timing for MCRA scenarios. In many cases, the success criteria timing for a scenario may, for the sake of simplicity, be based on a bounding case. For example, the time to recover feedwater may have been based on plant trip at low water level and used for all cases of loss of feedwater because the additional time available given trip at nominal water level has no significant impact on the HEP for recovering feedwater in the MCR. However, MCRA actions required to restore feedwater from the RSDP take longer than in-MCR actions to restore feedwater. The need for additional time could be significant, and could, in some cases, make

the difference between the action being feasible versus infeasible. Therefore, it is important when evaluating the use of previously-calculated success criteria for MCRA scenarios to determine whether they are overly conservative with respect to the specifics of the MCRA scenarios being evaluated. This information is fed into the development of the timelines, which are addressed in detail in Section 7.

3.4 Incorporating the HFEs into the Model

A key aspect of developing the fire PRA model is to incorporate the HFEs into the model logic. This requires defining the appropriate HFEs, which, in turn, requires significant interaction between the PRA and HRA analysts. There are two different types of HFEs that need to be addressed: 1) the decision to abandon the MCR, and 2) the performance of the necessary actions to avoid core damage within an abandonment scenario.

3.4.1 Incorporating the Decision to Abandon the MCR

Section 3.2 discusses how to identify MCRA scenarios. Once abandonment occurs, the model needs to account for whether the decision to abandon is made in time to avoid core damage. The cases of LOH and LOC are fundamentally different, and so they are discussed separately.

Abandonment for Loss of Habitability. The PRA model does not need to incorporate an HFE for the failure to abandon the MCR in the case of LOH. As discussed in Section 3.2.3 (see also Section 4), the occurrence of the conditions associated with a LOH are specified in NUREG/CR-6850 and their onset for any given fire scenario is a direct result of a fire modeling calculation. This criterion is most frequently encountered when a fire located in a panel, cable bundle, or transient source burns sufficiently to generate smoke and heat that would necessitate evacuation. For MCRA on LOH, it is not necessary to consider the possibility that the MCR is not abandoned. The conditions established in Step 11c of NUREG/CR-6850 will result in scenarios where it is physically very difficult for the operators to remain in the MCR without risking serious physical harm. In general, plant procedures and training provide specific cues to indicate an abandonment condition. The fire PRA and MCRA HRA assume that it is not credible that the operators will remain in the MCR under these harsh environmental conditions. Therefore, the probability of abandonment due to LOH is not based on HRA; rather, it is developed by establishing and justifying the fire conditions that would force abandonment (e.g., smoke, heat). This probability that the fire grows to the point of requiring evacuation is developed using a zone model or computational fluid dynamics fire model calculation. Therefore, the plant logic model does not need to include an HFE for failure to abandon on a LOH.

Abandonment for Loss of Control. Abandoning the MCR due to a LOC is only successful when the operators interpret the available cues correctly and make the decision to transition to the procedure for abandonment. The modeling considerations for LOC are discussed in Section 3.2.4, which allow credit for the MCRA on LOC only when: 1) the appropriate cues exist and 2) the operators equate these cues with an LOC condition, leading them to enter the MCRA procedure. The model construct would then incorporate an HFE for the failure of decision to abandon. Failure of this decision would result in the failure of all actions associated with the abandonment procedure.

3.4.2 Incorporating Actions to Transfer Command and Control

Regardless of the type of abandonment (LOH or LOC) or the extent of fire-induced damage, a base set of actions are always required in order to transfer command and control to the remote shutdown location(s). Some of these actions are performed in the MCR before it is physically abandoned, and some are performed at the RSDP or other locations. In some cases, actions are taken while in transit to the RSDP (or other local plant panels). These actions typically include isolating MCR control circuits, de-energizing control circuits to prevent spurious operations, and energizing the RSDP. From the perspective of the logic modeling, all of these actions are assumed to be required in order for the abandonment scenario to be successful. Therefore, the model should include an HFE to represent these actions, and should be applied to both LOH and LOC scenarios.

The set of actions associated with the transfer of control from the MCR to the RSDP are commonly referred to as the “enabling” actions. Examples of such actions include isolating the control circuits in the MCR and activating (or permitting) the local control circuits to allow operation of the required equipment locally at the panels/stations. These common actions can be assumed to be required in order for the MCRA to be successful and, therefore, should be incorporated into the model as failing all systems/functions required for the specific MCRA scenario. For this reason, these actions are incorporated into a single HFE in the model. For the LOC case, they could be considered as the execution part of the cognitive failure to abandon. However, these actions need to be defined as a separate HFE for LOH scenarios since there is no cognitive failure to abandon is modeled in these scenarios (see Section 3.4.1).

3.4.3 Incorporating Actions After Abandonment

Typically, a number of operator actions are required to implement the MCRA procedure(s). In order for these actions to be fully integrated into the model, they should be organized by each system and/or function required for safe shutdown. This approach is similar to the way non-MCRA actions are generally organized in a PRA. However, fire scenarios that result in MCRA do not always cause a loss of all of the systems that the MCRA procedure(s) include as part of the shutdown strategy. In those scenarios, the systems that operate properly despite the fire can be credited as functional without crediting success of the operator actions associated with those systems. Therefore, the MCRA safe shutdown actions associated with each system/function should be incorporated into the model in an AND relationship with the failure of the system/function to operate automatically.

In general, it is expected that reliability concerns for these operator actions will likely be dominated by execution, rather than decision-making. This topic will be discussed in later guidance that addresses HRA quantification for MCRA scenarios. For the purposes of the discussion in this section, the phrase “execution HFEs” is used to describe failure of operator actions taken while following the MCRA procedure(s) as opposed to a “cognitive HFE” used to describe the failure of operators to decide to enter the MCRA procedure.

Defining the execution HFEs requires significant interaction between the PRM and HRA analysts in order to address both the needs of the model and the structure of the procedures. This definition is relatively straightforward for those aspects of the procedures that are written functionally. For example, if the procedure has an attachment where the sole purpose of the attachment is to restore power to one or both emergency AC busses, then all the required execution actions in that attachment would be associated with that system/function and would fit into the associated HFE.

Defining execution HFEs is more complex when an attachment to the MCRA procedure is written for each operator by location (i.e., an operator is instructed to perform all the actions that are required for the same area of the plant, which may involve multiple systems/functions). For example, there may be two attachments, one for each operator, where they work in tandem to: 1) first, restore AC power, and 2) then start the charging system. It would be natural from an HRA perspective to put the entire set of actions in a single HFE, where failure of the operator actions represented by the HFE would fail the MCRA shutdown strategy. However, this modeling approach would not serve the purposes of the plant model if, in some MCRA scenarios, AC power is not lost, but charging is lost. For those scenarios, the performance of the actions associated with the AC power recovery are not required, and their failure does not impact success. Combining these two actions into a single HFE would incorrectly represent the response to the scenario in the model, when only the failures associated with starting the charging system matter.

3.5 Incorporating Equipment Failures into the Model

In evaluating the failure probability for remote shutdown following MCRA, some analyses have assumed that the HFE contribution will dominate, making the assigned HEP(s) an adequate surrogate for the overall failure probability. However, other plants have performed more detailed assessments and have shown that this is not always (or even not often) the case for some scenarios. For example, if offsite power is failed and the RSDP relies on an emergency diesel generator (EDG), then the probability that the EDG fails to run for its mission time could be comparable to the HEP for such MCRA scenarios.

This section addresses how to incorporate equipment failures into the model such that their impact on the MCRA failure probability is correctly captured, such as:

- Do not credit MCRA in scenarios that represent conditions beyond the capability of the RSDP equipment and procedures, i.e., reflect that these conditions lead to core damage
- Include random and fire-induced failure of the RSDP and/or local stations
- Include random and fire-induced failure of required equipment:
  - Mitigatable failures (Generally, only fire-induced failures may be mitigatable failures. For example, a fire-induced failure of control circuit could be mitigated by using an alternate control circuit or manually operating the affected component.)

- Non-mitigatable failures (i.e., random equipment failures and fire-induced damage, such as multiple spurious operations [MSOs]);[11] include dedicated systems that are used only under MCRA situations
- Do not credit systems that are intentionally disabled under MCRA situations

3.5.1 Conditions Beyond the Capability of the Remote Shutdown Equipment and Procedures

Usually, the plant's remote shutdown capability is designed to allow a shutdown under specific initial conditions that are defined using deterministic rules. Examples of such initial conditions, using the single failure criterion, are:

- Assuming reactor trip
- Assuming the absence (or mitigation) of spurious operations
- Assuming turbine trip/main steam isolation valve (MSIV) closure

In PRA, there may be risk-significant scenarios that exceed the initial conditions that are assumed in the design of the remote shutdown capability. That is, there may be scenarios where failures occur such that, even if every operator action is successful and none of the equipment called for in the MCRA procedure fails, core damage still occurs. It is essential that: 1) an assessment be performed to identify scenarios where such conditions exist, and 2) the model does not credit MCRA credit in those cases. Most remote shutdown strategies are designed to be capable of successful shutdown only under general transient conditions and this design may not have considered the impact of MSOs. In such situations (i.e., the strategy is not capable of mitigating these events), no credit for remote shutdown should be applied for conditions such as anticipated transient without SCRAM (ATWS), loss of coolant accidents (LOCAs), interfacing-systems LOCA (ISLOCA), or main steam line break (MSLB) (e.g., un-isolated stuck-open atmospheric relief valves for PWRs). Due to the variability in strategies, this assessment must be conducted on a plant-specific basis. Given the plant-specific nature of RSDP design (or alternative strategy), it is not possible to provide a comprehensive list of situations to consider. However, the following list should be considered at a minimum when performing the remote shutdown capability assessment:

- ***LOCAs.*** Fire-induced or random LOCAs (e.g., spurious power-operated relief valve (PORV) opening or failure of a PORV to re-close, reactor coolant pump (RCP) seal LOCAs, spurious opening of reactor coolant system (RCS) interface valves) are often situations that cannot be mitigated in an MCRA situation. For PWRs, the RSDP or procedures may not provide for RCS make-up and, if they do, they may not provide for recirculation or containment cooling.
- ***ATWS.*** Some plants have identified fire-induced failures that can prevent RCS trip long enough that the limited functionality provided under MCRA conditions will not mitigate the event.

[11] In certain cases it may be possible to repair a randomly failed piece of equipment, so this is an exception to the general expectation that random failures are non-mitigatable. Such cases can be treated in the same manner as they are treated elsewhere in the PRA, taking into account the availability of resources under the context of an abandonment scenario.

- ***MSLB.*** Spurious valve opening or failure to close MSIVs on the non-credited train has minimal effect on safe shutdown. The non-credited steam generator will blow dry and then the credited steam generator (SG) is used for cooldown. A spuriously opened MSIV or atmospheric steam dump valve on the credited SG often must be isolated locally in order to provide an intact SG for decay heat removal. In the case where no MSIVs close, all SGs will blow down through the common steam supply to the condenser, which typically is an unanalyzed condition that cannot be mitigated using remote shutdown procedures.
- ***ISLOCA.*** Spurious valve operations may result in ISLOCA. Most plant MCRA procedures and equipment will be unable to mitigate an ISLOCA.

The equipment failures that can lead to these conditions should be incorporated in the model as a direct failure of successful shutdown when MCRA would otherwise be credited. Circuit analysis provides insights on where these fire-induced failures may occur.

3.5.2 Random and Fire-Induced Failure of RSDP and/or Local Stations

Implementation of a MCRA shutdown strategy requires operator actions to: 1) isolate the primary control circuits that go to the MCR and 2) enable controls at the RSDP, local control stations, or some combination of the two. One of the common issues found in fire PRA modeling of MCRA scenarios is inadequate representation of these aspects of MCRA strategy implementation.

First, the analyst should investigate if fire damage could defeat the ability to either isolate the MCR or enable the RSDP/local station functions. The functionality of the RSDP, as well as the potential need for cues and indications from other local panels, should be considered. Since the purpose of the RSDP/local station(s) is to allow for a controlled shutdown of the plant when the MCR must be abandoned, the analyst may be tempted to assume, if a fire occurred requiring MCRA, that these functions are free from fire damage. However, experience gained from multiple NPPs is that this is not always the case. In other words, the design (e.g., MCR panels, RSDP, panels used for MCR isolation or RSDP/local station enabling) is not always free from fire damage for scenarios when such actions are required. Therefore, circuit analysis (in accordance with the requirements of the ASME/ANS PRA Standard [1]) of the local functions at the RSDP/local stations is needed. The scope should include any adverse impacts to the MCR isolation function, and the cables that could cause these functions to fail.

In addition to addressing the fire-induced failures, the second area for consideration is random circuit failures. The primary concern is the failure of the isolation, enabling, and/or activation switches. While individual switches are generally reliable, the combined failure of all required switches could be a meaningful risk contributor, especially for those plants where: 1) only a single train is used in the MCRA design (i.e., all the switches must work so the individual failure probabilities must be summed), and 2) not much fire damage is represented in the MCRA scenario (which often has the highest frequency among MCRA scenarios). Therefore, in addition to mapping the cables to the basic events for failures of the RSDP/local stations, a random (i.e., non-fire) failure probability should be assigned to each switch. Overall, this concern could be addressed by assigning a random failure basic event to each switch or a single random failure basic event for the sum of all switches.

These circuits are crucial to the success of the MCRA shutdown strategy, because MCRA procedures generally do not provide for "work-arounds" to recover from such failures in time to avoid core damage. In other words, abandonment procedures generally assume that the required circuits are designed to work when abandonment is required and, therefore, will always work; abandonment procedures do not include "response not obtained" alternatives.[12] If these alternative do exist in the MCRA procedures, then the steps to recover from a failure can still be credited as long as there is sufficient time available to mitigate the event.

3.5.3 Random and Fire-Induced Failure of Required Equipment

The final equipment consideration for MCRA is the front-line and support system components that need to operate in order to reach a safe, stable state. Even if the scenario is within the capabilities of the MCRA equipment and procedures, the operators perform all the correct actions, and all of the control circuits are free from fire damage and operate successfully, it is still possible that some equipment will fail. For example, if the turbine-driven auxiliary feedwater (AFW) pump is needed to provide flow to the steam generators, and if it has suffered a random mechanical failure of the shaft, it will not start even if the RSDP control circuit sends the appropriate signal. On the other hand, if it only failed because of fire damage to the control circuit from the MCR, and that is now isolated and the RSDP control circuit is enabled, it may now start, if demanded. There are two types of failures that need to be considered – mitigatable and non-mitigatable.

Non-mitigatable failures can be either fire-induced or random. These failures appear in both the non-MCRA and MCRA parts of the model (i.e., the component is failed whether or not a MCRA event has occurred). If the failure is modeled in both the non-MCRA and the MCRA logic, the same basic event name must be used in both parts of the model in order for the Boolean reduction to work properly. Fire-induced failures become non-mitigatable only when the affected component is directly damaged by the effects of the fire. For MCRA scenarios, this usually applies to fires in the control complex (e.g., MCR, CSR, relay room) where there is a potential for a fire to either: 1) do substantial damage to the cables required to supply both control and indication to the MCR, or 2) render the MCR uninhabitable. These areas typically do not physically contain any of the front line and support system components used in the MCRA shutdown strategy. The fire-induced non-mitigatable failures of concern are those that result from control system faults that cause a component to damage itself. Examples of such non-mitigatable failures include control system failures that cause:

- a diesel to start and overload while disabling the protective trips
- components to run without cooling
- valves to over torque so they cannot be operated

These failures are typically modeled as part of the MSO evaluation process. Where such MSOs could cause failure of a component credited in the MCRA, the same MSO logic should appear in both the non-MCRA and MCRA parts of the model.

[12] There may be exceptions, or such alternative might be added as the result of procedure update, in which case they could be credited if there is sufficient time available.

Mitigatable failures of the required equipment are a subset of the fire-induced failures. This is not to be confused with repair. Mitigatable failures are fire-induced failures that fail the normal means of operating equipment, but do not render the equipment unusable. The classic case is fire damage that prevents the operation of equipment using remote switches or fails the automatic operation of the equipment, but it is still possible to operate the equipment locally. The local manual operation can be credited if it is proceduralized. Examples include:

- Starting and loading of an EDG from the diesel room
- Using a handwheel to operate a valve

3.5.4 Modeling Dedicated Systems

Some plants have dedicated shutdown equipment (i.e., equipment that is solely installed for either station blackout (SBO) or fires) that can only be controlled at either the RSDP or a local control station. To credit such equipment, the equipment and any control circuits need to be free of fire damage. These systems may not be modeled in the PRA prior to the consideration of MCRA, and would, therefore, need to be added to the model. Even though they should, by design, be free from fire damage (i.e., unaffected by any fire in a remote shutdown area), this should be confirmed by cable selection and circuit analysis. The model would need to include all other random and fire-induced equipment failures as well as relevant HFEs that could lead to failure of the systems.

3.5.5 Accounting for Intentionally Disabled Systems

The fire model accounts for systems that are disabled by the fire, but systems also may be intentionally disabled as part of the fire response. Consequently, even if these systems are not damaged by the fire, they should not be credited as potential mitigating systems in MCRA scenarios. This is generally associated with actions that disable systems in order to prevent spurious operations, but there is no provision in the procedures to restore the system after abandonment. The model needs to account for this and not credit the intentionally-disabled systems whenever an abandonment scenario has occurred. In some cases, it may only be a specific train of a system that will be disabled (e.g., when the procedure calls for disabling all but the “credited” train). For example, the logic could account for this by placing an OR gate above the existing gate for failure of the system or train, with the second input being either a house event or other logic that will be set to 1.0 for any scenario where the MCR is abandoned.

3.5.6 Self-induced Station Blackout (SISBO) and Other Recoverable Pre-Emptive Action

Section 3.5.5 discusses the treatment of systems that are intentionally disabled and not utilized following abandonment. This section discusses a variation on that situation – systems that are intentionally disabled, specifically to protect them from fire damage. After the MCR is abandoned, certain (maybe not all) systems are selectively restored to service after abandonment. This type of strategy is commonly called “self-induced station blackout,” or SISBO.

The SISBO approach is a strategy that, in order to meet deterministic requirements, purposefully isolates offsite power and de-energizes non-safety switchgear and a train of engineered safety feature equipment to reduce the likelihood of spurious operation. A SISBO

approach is associated with the plant fire procedures (rather than the MCRA procedure). For non-abandonment cases, the SISBO procedure refers the operator to a list of equipment that could be impacted by a fire in specific areas and instructs the operator to de-energize that equipment from the MCR. Later, when the fire location is better understood and the fire is under control, operators re-energize sufficient equipment to bring the plant to a safe, stable state from the MCR.

For MCRA scenarios involving SISBO, the key difference is that the fire results in abandonment of the MCR prior to re-energizing (and aligning, if necessary) the equipment. This assumption is made regardless of when the abandonment is expected to occur in the scenario's timeline.

From the standpoint of modeling and the HFE definition, the non-MCRA model should already represent the assumption that the system needs to be re-energized and aligned from the MCR. For MCRA scenarios, the only modification to the model required for the affected systems is that the HFE associated with these actions from the MCR is failed. In other words, the only way the system can be returned to operation is through the success of operator actions to recover the system remotely as specified in the abandonment procedure (which is modeled with a different HFE).

3.6 An Example of a Detailed Integrated Logic Model

Putting all the modeling aspects together, this section provides an example of integrated model logic for MCRA. The logical construct for developing the integrated model is shown in Figure 3-3.[13] This figure illustrates the Boolean logic to account for the aspects discussed in Section 3.5. This logic is a key aspect of the process and is intended to be implemented individually for each system/function required for abandonment scenarios. Note that this section only applies to systems credited under MCRA conditions. For systems that are intentionally disabled as part of the abandonment strategy, see the discussion in Section 3.5.5.

The example fault tree shown in Figure 3-3 models the failure of System X in either a MCRA or a non-MCRA scenario. This logic does not have to be implemented in the model in the form of a fault tree. Because of the capabilities of the various software codes used for PRA, some aspects of the logic could better be implemented as boundary conditions, rules files, flag files, exchange sets, or other post-processing techniques. In addition, alternative fault tree modeling to that in Figure 3-3 could be used to model the failure of System X.

The following is the description of the key gates/events in the fault tree shown in Figure 3-3.

- SYS-X-FAIL-ALL: This is the top gate for crediting System X in the PRA model. This logic ensures that System X will only fail if: 1) it fails automatically (due to fire or random events), and 2) it fails to be restored following MCRA.
- SYS-X-FAIL: This gate represents the system tree as it is used for fire and internal events scenarios. It is the internal events system fault tree with the addition of the fire PRA impacts. This part of the tree will include the mapping of the fire-induced circuit failures to the component failures, and include any operator actions that are credited for non-abandonment

[13] Double diamond is the computer aided fault tree analysis system (CAFTA) symbol denoting a developed event (a more detailed fault tree). The symbol shaped like a hand denotes a human failure basic event in CAFTA.

scenarios.[14] Note that this gate would not exist in the case of dedicated shutdown systems, discussed in Section 3.5.4, since these systems are not credited in the internal events PRA or in non-abandonment scenarios in the fire PRA. This gate would also not exist for the case where the plant utilizes a SISBO strategy, as no credit would be taken for the system automatically starting and functioning since the operators would de-energize the system prior to abandoning the MCR and would need to re-energize it remotely. Success of this gate (that is, SYS-X-FAIL is not TRUE) implies that System X was never lost in the scenario.

- SYS-X-FAIL-MCRA. This gate provides the credit for the system restoration actions called for in the abandonment procedure. The logic is set up such that it will automatically fail in a non-abandonment scenario, and thus is only actuated if the scenario being evaluated can take credit for abandonment.
- NOT-MCRA. This house event controls whether an abandonment scenario is taking place, and is set to allow credit for abandonment restoration when warranted. The default value for this flag is TRUE, which means that gate SYS-X-FAIL-MCRA is failed and no abandonment credit is added.
  - When using CAFTA, the general approach would be that FRANX is used to set the flag to FALSE for abandonment cases. These are MCRA scenarios that are determined to be a LOH and scenarios that cause failures that would result in meeting the cues for LOC (e.g., fire in control complex and failure to be able to start any injection from the MCR).
  - It is also possible to build a fault tree structure that models the LOC conditions (i.e., system failures) that provides the cues for LOC and includes the logic of the LOH scenarios.
- SYS-X-NONMIT-MCRA. This is the top gate for the logic to credit System X in a MCRA scenario. This portion of the tree in LOC or LOH conditions determines the probability that System X does not perform its required function for shutdown from outside the MCR given that it failed to perform its function automatically.
- SYS-X-NONMITFAIL. As discussed previously, the model must take into account failures of equipment that cannot be mitigated by shutdown outside of the MCR. This logic will fail System X if failures have occurred that would not allow successful restoration of the system even if the operator actions are performed successfully.
- SYS-X-RANDOM. This gate is a link to the logic that contains random, mechanical failure of System X that cannot be overcome by the RSDP actions, even if they work properly. This is to ensure that random failures to start, run, etc., that represent mechanical failures, are not restored, while still allowing restoration for those cases where a fire-induced failure would be bypassed by the function at the RSDP. Again, this logic would also appear under gate SYS-X-FAIL, but in this case fire-induced effects would not be mapped to these events because it has been determined that the fire-induced failures are not fatal (i.e., the equipment can be recovered by following the abandonment procedure). The modeling here

[14] It would also be necessary to consider whether these operator actions can still be credited for abandonment scenarios. It may be necessary to map them to failure (set to true) for abandonment scenarios if they are not included in the abandonment procedure.

can be complicated, because these basic events need to be properly linked to the equivalent failures under SYS-X-FAIL, but without the fire-induced impacts. It is important to carefully review the basic events and failure mechanisms to make sure they are properly apportioned to SYS-X-LOCAL, SYS-X-DAMAGE, and SYS-X-RANDOM.

- SYS-X-NONMIT-FIRE. This gate gathers failures that are non-mitigatable, which can be either random or fire-induced.
- SYS-X-LOCAL. This gate is a link to the logic that contains failures associated with the operability of the RSDP to restore and operate System X. This would include failure to transfer control to the panel or failure of the RSDP function itself. Both random and fire-induced failures are included, so they would need to have random failure probabilities assigned and also be mapped to cables. Failures of the transfer switches that activate the RSDP, any isolation switches that clear hot shorts, and any controls located on local panels not at the RSDP would be included in this logic.
- SYS-X-DAMAGE. This gate is a link to the logic that contains fire-induced failures that would cause unrecoverable damage to needed equipment for System X. This is mostly related to MSO induced failures, such as fire-induced failures that would overload diesels, cause NRC Information Notice (IN) 92-18 valves to jam, etc. Note that this logic would likely also appear under gate SYS-X-FAIL, since it would also fail the system in non-abandonment scenarios. It would be repeated here to ensure that its recovery is not credited during abandonment. Note that this gate would include logic for any conditions that cannot be successfully mitigated by the capabilities of the RSDP or that are not covered by the remote shutdown procedures. For example, the remote shutdown capabilities of many PWRs are such that they cannot successfully respond to a LOCA condition. In this case, this logic would include the occurrence of an RCP seal LOCA as a condition that would defeat the remote shutdown function following abandonment.
- H-SYS-X-MCRA. The structure under gate SYS-X-NONMITFAIL addressed the equipment failures that will fail the abandonment shutdown. This gate addresses the human failures that will fail abandonment shutdown, and inputs to this gate include the HFEs that will fail system restoration. There are three errors considered; (1) failure to properly execute the actions to transfer command and control, which will appear for every system and fails MCRA for all LOH or LOC scenarios; (2) failure to abandon the MCR, which applies only to LOC, will appear for every system, and fails MCRA for all LOC scenarios; and (3) failure to properly execute the abandonment actions for the specific system, which will appear only under that system and fails MCRA for all LOH and LOC scenarios where the fire impacts that system.
- H-SYS-X-MCRA-AFTER. This gate includes the operator actions that take place after abandonment that will fail the restoration of System X under abandonment conditions, regardless of the cause of the abandonment. The approach shown provides a structure that allows for variations of this HFE to address different failure conditions. Although this could significantly complicate the modeling, the distinction between certain actions based on relevance to the scenario (e.g., diesel start and load shedding actions for AC power recovery cases) may be functionally warranted, in particular if the risk associated with abandonment scenarios is significant. Note that an alternative approach could be that all

required, individual operator actions are modeled a single HFE that represents a bounding case for failing to successfully reach a safe, stable condition (i.e., it would bound all actions required to recover all systems). This alternative and other variations are discussed in Section 3.7.

- G-H-MCRA-COG. This gate represents the failure of the operators to decide to abandon the MCR. It is generally accepted that the operators will abandon the control room if the conditions are such that they cannot function and that their safety is threatened, so there is no cognitive decision about whether to abandon for LOH. However, the decision on whether to abandon due to LOC is usually at the discretion of the shift manager. For this case, there is a decision process involved and a cognitive HFE is modeled. This gate decides if the cognitive HFE for failure to abandon should be applied.
- H-MCRA-COG. This basic event is the cognitive HFE for failure to abandon in time. If this failure occurs, it will fail abandonment for LOC. This same basic event appears under every abandonment tree for all the systems modeled, so it is a common failure mechanism that will fail all functional recoveries covered by the abandonment procedure.
- LOC-CONDITION. This gate is a link to the logic that determines whether the LOC condition exists. It will be a model of the conditions that result in a LOC from the MCR, as defined in the plant procedures or through operator interviews and/or simulator training.
- H-MCRA-EXE. This basic event is the execution HFE for failure of the operator actions that take place between the time the decision is made to abandon and the time at which command and control has been transferred from the MCR. These actions are common to all abandonment scenarios, and generally include such things as isolating the MCR circuits, depowering circuits to prevent spurious operations, and powering up the remote shutdown locations. These actions are common to all MCRA scenarios, and so this basic event will appear under every abandonment tree for all systems modeled.

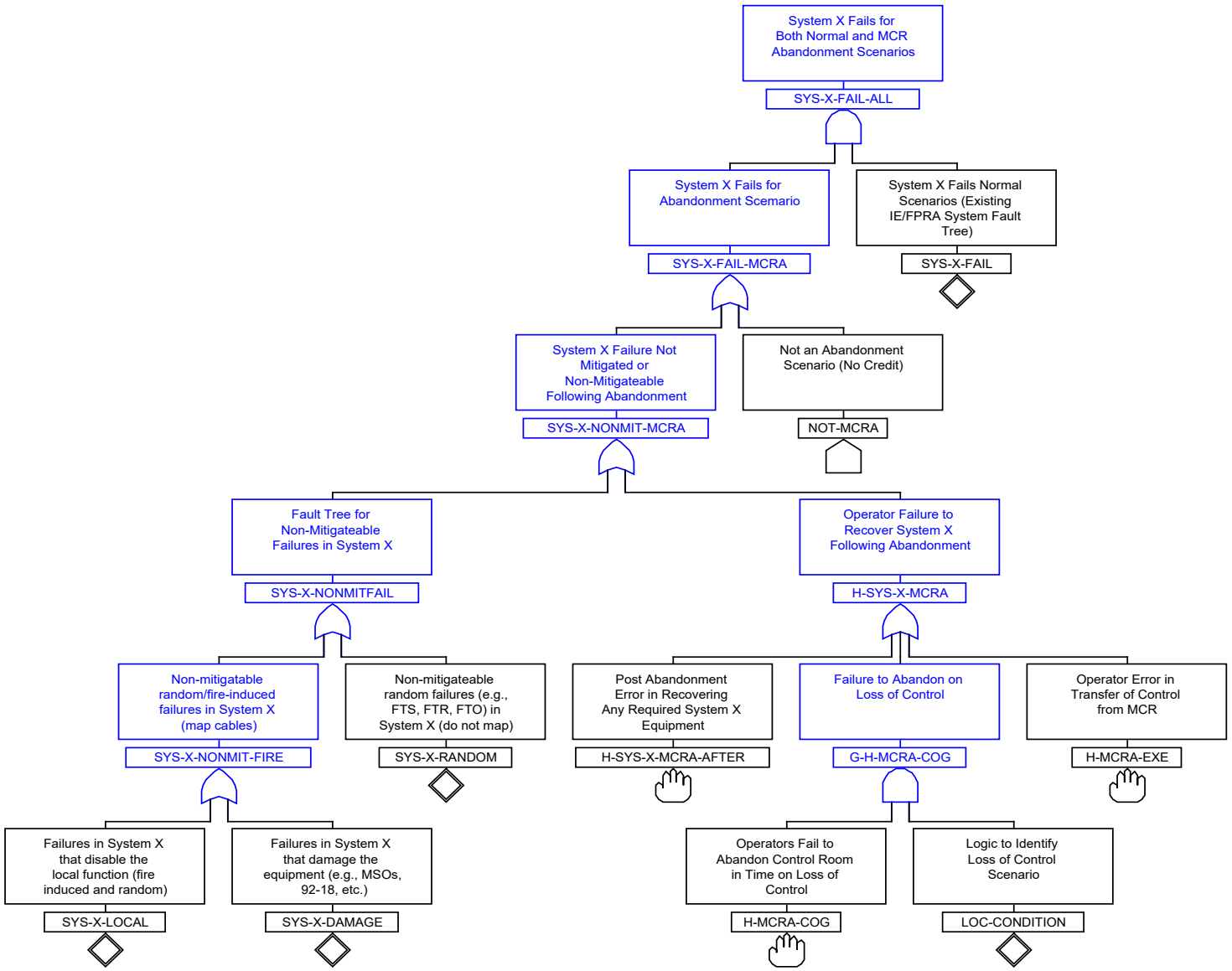


Figure 3-3
Example logic for integrating MCRA into the PRA model

3.7 Alternate Approaches

While the approach discussed above will provide the most realistic assessment of MCRA, there are simplified approaches that may provide a sufficient answer. Such approaches might be implemented for MCRA scenarios that are not significant risk contributors.

One alternative approach comes directly from NUREG/CR-6850, which is to use a single overall value for the probability of failure to achieve a successful alternate shutdown. However, it does not provide sufficient guidance on how to implement this approach, what the considerations are, and what constituent pieces of this single value need to include. To address this gap, the guidance for using this approach is discussed in Section 3.7.1. The key problem with the single value approach is that the value must be bounding for all abandonment scenarios. Because the most severe scenarios also tend to be the ones with the lowest frequency, the use of a bounding value based on the most severe scenarios will be quite conservative for the more frequent, less severe scenarios. If the use of a single value results in the elimination of MCRA scenarios as dominant contributors, it would be an acceptable modeling choice.

Many PRAs produce unacceptable results using this approach, but analysts do not elect to perform the more detailed approach in Section 3.6. This has resulted in the development of a "middle ground" approach that was not mentioned in NUREG/CR-6850 that removes some, but not all, of the conservatism from the use of a single value. This approach uses severity bins for the MCRA scenarios, with a value for the probability of failure to achieve a successful alternate shutdown tailored to each bin. The guidance for this approach is provided in Section 3.7.2.

3.7.1 Single Overall Probability for Alternate Shutdown

NUREG/CR-6850 Section 11.5.2.10 clearly identifies that the failure probability for MCRA should be identified and addressed as part of the analysis and provides two suggestions for how to incorporate in the fire PRA model. As discussed in Section 3.2.2, one of those approaches is a simplified model consisting of estimation of a single probability. The applicable text from that section of NUREG/CR-6850 [2] states:

> The first approach (that is, the use of an overall probability value) can be used if the probability value is evaluated conservatively and a proper basis is provided. This approach was used in several IPEEE submittals. For example, in many cases, 0.1 was used as a point value estimate for the probability" from reference [11.3] *Perspective Gained from the Individual Plant Examination of External Events (IPEEE), 2002*.

So, it can be seen that there are only two requirements to this approach in NUREG/CR-6850:

1. That the overall probability for shutdown be evaluated conservatively, and
2. That the basis be provided.

The benefits of this approach from a modeling perspective is that it is not necessary to add a number of different HFEs and equipment failures into the model structure at various locations – it becomes a single basic event appended to cutsets where MCRA can be credited.

It is effectively a CCDP given the frequency of a recoverable MCRA scenario. This allows the abandonment model structure to be placed high up in the logic structure and triggered when needed. It is even possible, depending on the software used, to treat this as a recovery rule that is applied following quantification of the cutsets.

However, NUREG/CR-6850 does not state what should, or should not, be included in this overall probability, which has led to inconsistency in how it has been applied. For example, should this overall probability include both operator actions and hardware failure probabilities or does it represent only operator actions?

As a result of this open question, the fire PRAs performed to date have modeled MCRA scenarios using different quantification approaches and different levels of detail. For example, some fire PRA models consist of a single, overall HEP,[15] which in many cases has been based on judgment, to represent the collective set of operator actions needed to safely shutdown the plant following a fire in the MCR or cable spreading room requiring MCRA. This single HEP may have been applied to all MCR fire scenarios that led to evacuation due to LOH. Several peer reviews have questioned the validity of applying a single representative HEP (or CCDP) to the range of scenarios modeled in the PRA based on the principle value may not be bounding, such as when time-critical actions are involved, if hardware failures are not included, or if the HEP is applied to scenarios where recovery actions are not feasible.

Because the guidance in NUREG/CR-6850 is ambiguous, this report recommends that if the fire PRA follows this approach it should not be applied to scenarios with the following characteristics:

1. Scenarios where operator actions required for success are not feasible (i.e., MCRA should not be credited).
2. Scenarios including operator actions that are time-critical. The determination of what constitutes time-critical in this context (i.e., whether a detailed analysis is needed) will require the exercise of some judgment. It will depend not only on the relationship between the time required and the time available (the estimated time margin), but also needs to take into consideration the complexity of the action and when in the overall timeline it occurs. Each action should be evaluated as to the available time margin and a justification provided as to why it is not time-critical. If for any of the actions this justification cannot be provided, then that action should be considered to be a time-critical action, and a detailed analysis is needed.

If this approach is followed, the first consideration is which situations represent cases where success is not possible (and this needs to be taken into account). That is, the CCDP is only applied to cases where success of MCRA is possible.[16] So, the assessment discussed in Section 3.5.1 still needs to be performed and the model should be developed such that no credit is given for MCRA for those scenarios. In addition, some of the accident sequences or cutsets in

[15] Past practice sometimes use a single point value of 0.1 for this HEP. However, NUREG-1921 recommends against the use of the 0.1 point value estimate for the single HFE. In addition, this report is not intended to provide quantification guidance.

[16] So, while we refer to a single CCDP for MCRA, there are in fact in reality two – 1.0 for cases where MCRA cannot succeed and the single, bounding value where it can.

otherwise recoverable scenarios may include failures of equipment required for MCRA that themselves are not recoverable. These are discussed in Section 3.5.3, and the model must be constructed such that the occurrence of *any* non-recoverable failure of equipment utilized in the MCRA strategy should preclude credit for MCRA for that accident sequence or cutset. Finally, any fire-induced failures of required equipment at the RSDP and/or local stations also should be assumed to preclude credit for MCRA. (Random failures of this equipment are addressed in the single value; see below.) When using the single basic event approach to MCRA, this basic event should be placed near the logic that excludes credit for MCRA.

For the scenarios that can credit MCRA, the following elements should be incorporated into the single probability:

1. All of the execution actions required for safe shutdown can be individually analyzed and integrated into a single, overall HFE.[17] This means that the HEP for this HFE is the failure of *any* required action, regardless of the status of the systems in the scenario (e.g., it is assumed that AC power *always* has to be recovered for MCRA). So, a single overall HEP is acceptable since it would be developed from detailed HRA that assumes all the actions required for shutdown are always needed for all scenarios.
2. If credit is to be taken for LOC situations, the decision to abandon must be taken into account as described previously, and the subsequent HEP added to the (overall) single failure probability.[18]
3. All of the *random* failures discussed in Section 3.5.2 covering failure of required equipment for the RSDP and/or local stations are added to the single probability.
4. All of the *random* failures of required equipment discussed in Section 3.5.3 that address failure of required equipment are added to the single failure probability. It is understood that this may result in some double counting, since any accident sequences or cutsets that already include random failure of this equipment will be excluded from MCRA credit. However, this is necessary in order to ensure that the single probability is bounding in all cases where it is applied.

An example of the logic that would need to be implemented is shown in Figure 3-4. While shown in fault tree structure, this logic could be implemented in any number of ways, such as using recovery rules. The gate H-MCRA represents the single HFE used, which in reality is two different HFEs, one for LOH (two elements) and one for LOC (three elements). In actual implementation, the gate H-MCRA could be a HFE that is assigned one of two HEP values through an “exchange table” based on whether abandonment is due to LOC or LOH.

[17] Note that this is unlikely to be all actions taken during abandonment. It is expected that some actions that are taken are to protect equipment, and failure to perform those actions would not result in core damage. Therefore, these would not need to be considered in the analysis.

[18] One approach would be to give no credit for LOC, in which case these scenarios are assigned a CCDP of 1.0. If LOC is credited, either the LOC decision to abandon HEP could be incorporated into the single probability or two probabilities could be used; one for LOC and one for LOH. The model would become a little more complicated, as the logic would need to differentiate between the two.

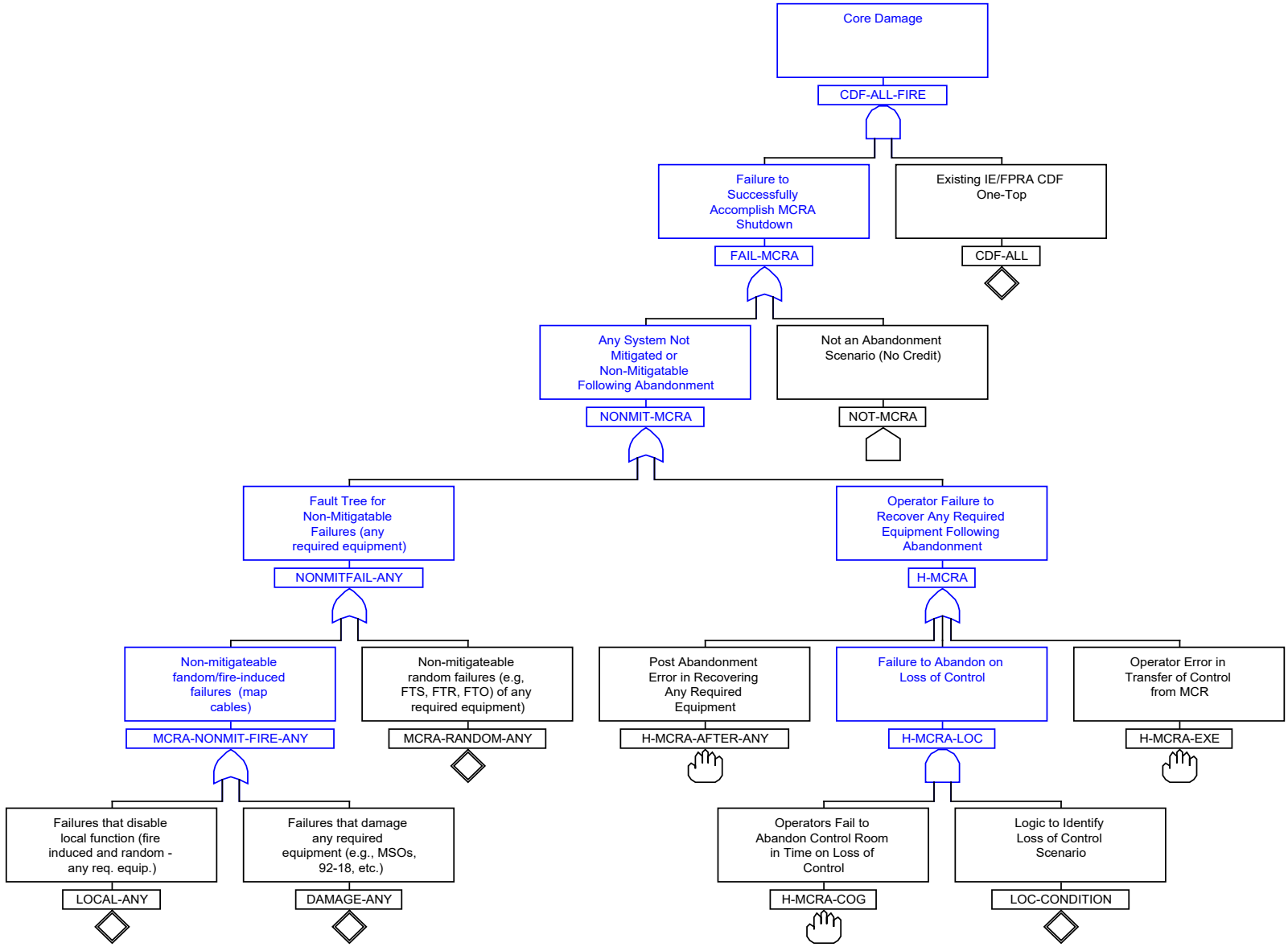


Figure 3-4
Example logic for single value approach for MCRA into the PRA model

There are similarities between this logic structure and the logic structure for the integrated modeling approach. This is expected, since the single value approach still needs to consider the same effects on MCRA. The key difference is where this appears in the overall logic of the model and how it is applied. Note that the logic shown is not input at the system level, but rather at the highest level as an adjustment to CDF (or LERF). For the integrated approach described in Section 3.6, the tree structure is developed for each system required for MCRA and, therefore, appears at a number of places in the tree with many of the basic events being system oriented. In contrast, the “one-value” approach applies the logic rules only once to post-process the core damage cutsets by crediting MCRA actions and equipment.

The common elements of both models are NOT-MCRA, H-MCRA-COG, LOC-CONDITION, and H-MCRA-EXE.

The remaining elements are redefined to encompass the scope of all MCRA scenarios as opposed to the scope of a particular system. For example, LOCAL-ANY replaces SYS-X-LOCAL in the logic. LOCAL-ANY will consist of all of the local control functions that are used during the MCRA strategy, meaning that the failure of any local function will fail achieving safe-and-stable conditions following MCRA even if the automatic function for a particular system was not affected by the fire. In other words, no credit is taken for any system except those that operate as a result of local operator actions called out in the abandonment procedure. This is equivalent to completely shutting down every system (even if it was working) prior to leaving the MCR, then restarting each one after transition of command and control to the RSDP and/or local station(s).

If the plant is a SISBO plant, it may be a good candidate for this approach. Since the SISBO approach requires de-energizing all the systems and then restarting them manually, the assumption that all abandonment actions are required for all scenarios might be an appropriate simplification.

3.7.2 Modeling Alternate Shutdown with Scenario Bins

An alternative approach to modeling MCRA is to divide the scenarios requiring MCRA into scenario bins. This can be accomplished within a fault tree, such as grouping all decay heat removal scenarios under a single gate. Or, it can be accomplished outside of a PRA tool, such as in a spreadsheet. This approach can be easier to defend, since this approach can better capture the range of fire scenarios, such as those with no impact on systems, structures, and components (SSC) versus those that may be beyond the capability of the alternate shutdown procedure. The challenge with this approach is how to defend the groupings.

The purpose of the scenario binning approach is to remove some of the conservatism implicit in the single probability approach, but without adding the complexity of the full model integration. However, there are many ways to create the bins to represent different combinations of fire-induced functional failures in abandonment situations. If these failures are parsed too finely and too many combinations are used, then this approach becomes similar to the full-integration method in complexity and level of effort, but with less flexibility and more conservatism. Based on the authors' experience, using between two and five bins often produces acceptable results. For that reason, when establishing the bins, it is useful to think in terms of a few general categories of actions and equipment required for the MCRA scenarios.

Action and Equipment Categories. The operator actions and equipment for each scenario can generally be grouped into three categories:

- **Category 1 – Actions and Equipment Needed for All Scenarios.** This category of actions and equipment consists of those required to restore decay heat removal (e.g., auxiliary feedwater (AFW) in a PWR, torus or suppression pool cooling in a boiling water reactor (BWR)), injection (e.g., chemical and volume control system (CVCS) in a PWR, reactor core isolation cooling (RCIC) in a BWR), and associated support systems. This grouping of operator actions and equipment is the minimum set of systems necessary to provide safe shutdown. Failure of any of these actions or equipment leads to core damage.
  - Actions in this category should include start-up and control of systems for the PRA mission time. There can be a set of long-term actions to refill depleted tanks or maintain inventory. For example, depending on the size of the tank some plants will need to refill the diesel fuel storage tank, others will need to refill the condensate storage tank (CST) or provide an AFW suction source in order to support the PRA mission time.
- **Category 2 – Actions and Equipment Needed for Some Scenarios (Conditional Actions).** This category of actions consists of those that may be required in order to support the Category 1 actions, but in certain scenarios may not be initially failed and, therefore, do not need to be recovered. For example, there may be a need to restore power to an electrical bus in order to restore AFW. It would be expected in this case that, once the power had been restored to the bus, the restoration of AFW actions would still be required (i.e., AFW would not automatically start when power was restored). However, some scenarios may not be accompanied by failure of the bus power, and so the actions to restore power would not be required, and failure to perform those action would not prevent the restoration of AFW for those scenarios.
- **Category 3 – Additional Actions and Equipment Needed to Mitigate Spurious Operations.** This category of actions is modeled in addition to the actions taken for all scenarios (Category 1). This category consists of actions required to mitigate spurious equipment operation and restore the RCS and SG boundaries to a state where the AFW and CVCS systems can provide for safe shutdown. This category of actions for PWRs includes tripping the RCPs, isolation of RCS boundary valves (pressurizer PORV, RCS head vent, pressurizer vent, and RCS letdown), isolation of the SGs (closure of open MSIVs, closure of open SG atmospheric dump valves (ADVs), and closure of open SG blowdown valves), and termination of spurious safety injection. An example for BWRs would be actions to reclose spuriously-open safety relief valves (SRVs). These actions are required only when fire damage causes a spurious event that must be terminated.

Using these categories, bins can be constructed with combinations of the categories and/or the scenarios assigned to them. A typical set of bins is shown in Table 3-1.

Table 3-1
Example of binning for MCRA scenarios

Bin	Category 1 Failures	Category 2 Failures	Category 3 Failures
1	X	X	X
2	X	X	
3	X		X
4	X		
5			

A single, bounding CCDP would be defined for each bin to represent the probability that mitigating the event from the RSDP would not be successful.[19] Bin 1 is essentially the bounding bin described in Section 3.7.1. This would be the starting point for the other bins. For Bin 2, the equipment and actions associated with recovery from fire-induced spurious operation (e.g., isolating the PORV control circuits) would be removed from the total Bin 1 CCDP. For Bin 3, the equipment and actions associated with recovery of fire-induced failure of support systems (e.g., recovery of AC power to a vital bus) would be removed from the total Bin 1 CCDP. For Bin 4, both of these sets of equipment and actions would be removed from the Bin 1 CCDP. For Bin 5 (which would only be applicable to LOH scenarios) all actions associated with recovering from fire-induced failure of equipment would be removed from the CCDP, leaving only those actions and equipment required to establish control at the RSDP and complete the plant shutdown. These are just examples, and additional or alternate bins could be defined or fewer bins used. It is only necessary to ensure that the CCDP applied to each bin bounds the most restrictive scenario in the bin. That is, the representative scenario for the bin needs to be the worst possible combination of fire damage for the bin. For example, where the Category 3 (spurious operations) failures occur, then it must be assumed, for EVERY scenario where ANY (i.e., even if only one) spurious operation occurs,[20] that ALL spurious operation failures occur. This is conservative for most of the scenarios in the bin, but this is the penalty that must be accepted when using this simplified approach.

This approach does not take full credit for the lack of fire damage to each system in each scenario, but it does take credit for some equipment that remains free from fire damage in the applicable MCRA scenarios. Effectively, all of the requirements of the single value approach discussed in Section 3.7.1 still apply. However, in this case, they apply to the characteristics of the worst-case example of a recoverable MCRA scenario in each bin rather than the characteristics of the worst-case of all of the recoverable MCRA scenarios.

[19] Or two values, one for LOC and one for LOH, with the only difference being the addition of the HEP for the decision to abandon.

[20] Scenarios with non-mitigatable spurious operations would not fall into this bin. As previously discussed, the existence of any non-recoverable failures in a scenario automatically bumps it into the “no MCRA credit” bin.

For the purpose of illustration, let's consider a two-bin example. The bins will be labeled A and B to prevent confusion and allow comparison with the five bins presented in Table 3-1:

A. Bin A represents a situation for which all systems are assumed to be initially lost except for AC power (i.e., the MCRA strategy must include restoration of all required systems except for AC power), and

B. Bin B represents a situation for which everything, including AC power, initially fails (i.e., SBO - the failure of all systems needs to be mitigated by the abandonment actions).

An example of the logic to be implemented for this case is shown with Figures 3-5 through 3-7. While shown in fault tree structure, this logic could be implemented in any number of ways, such as using recovery rules. Since the worst case scenario in each bin is assumed to occur when developing the HFE for that bin, the non-SBO bin would have an HFE based on the need to perform all actions except those associated with AC power recovery. If the analyst considers the three categories of failure discussed above, the HFE for the non-SBO bin would have to assume that all the actions in Category 1, Category 2 (EXCEPT actions to mitigate fire-induced loss of AC power), and Category 3 are always needed for all scenarios, regardless of the extent of fire damage. The SBO bin would therefore have to assume that all Category 1, 2, and 3 actions are needed for all scenarios where SBO occurs, regardless of the extent of other fire damage. Any number of bins may be defined, and, for each bin, the worst case scenario becomes the reference scenario for the bin. Also, there must always be a bin for the case where all actions are required, since it is not possible to preclude this possibility.

This structure closely resembles the single-value case, but there are two different “single-value” cases in the logic – a single value for Bin B, abandonment scenarios that involve SBO, and a single value for Bin A, abandonment scenarios that do not involve SBO. Bin B would be equivalent to the Bin 1 case from Table 3-1. The CCDP for Bin B would be developed using the same methodology as the bounding single value case from Section 3.7.1. This bin, which represents the most severe abandonment scenarios, would always be required to be one of the bins used. The Bin A case would be equivalent to Bin 3 in Table 3-1. The use of only two bins in this example would be a simplification that would mean that scenarios that fell into Bin 2 in Table 3-1 would be represented by Bin B and scenarios that fell into Bins 4 and 5 would be represented by Bin A. The logic under gate FAIL-MCRA-SBO captures Bin B and it is the same as the single value approach, since it represents Bin 1 from Table 3-1. The logic under gate FAIL-MCRA-NOSBO captures Bin A and it represents Bin 3 from Table 3-1. The key difference between the logic under these gates is the need to implement logic that differentiates between SBO and non-SBO cases and to ensure the logic under gate NONMIT-MCRA-SBO and NONMIT-MCRA-NOSBO include the applicable set of equipment and actions.

Ultimately, this two-bin approach and the five-bin approach discussed are examples, and it is up to the analyst to determine what would work best for the NPP being modeled. The key is that the bins are defined in terms of a set of mitigatable fire-induced failures that represent the bin. However the bins are defined, the scenarios assigned to each bin can only have either exactly those mitigatable fire-induced failures or a subset of those mitigatable fire-induced failures. If a scenario has even a single mitigatable fire-induced failure not within the definition of the bin, then it must be assigned to a different bin that envelopes the failures in the scenario.

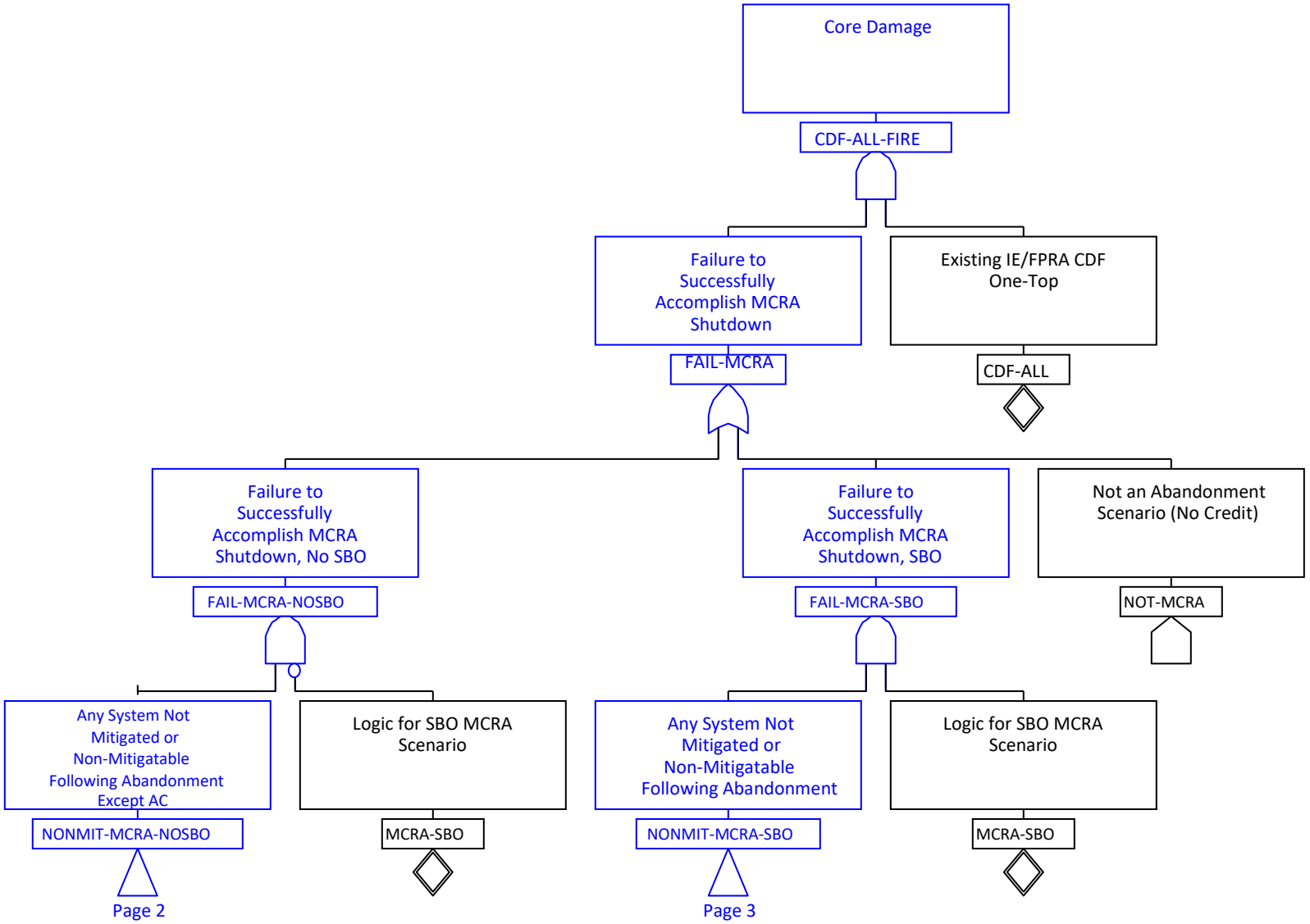


Figure 3-5
Example logic for scenario bin approach for MCRA into the PRA model (sheet 1 of 3)

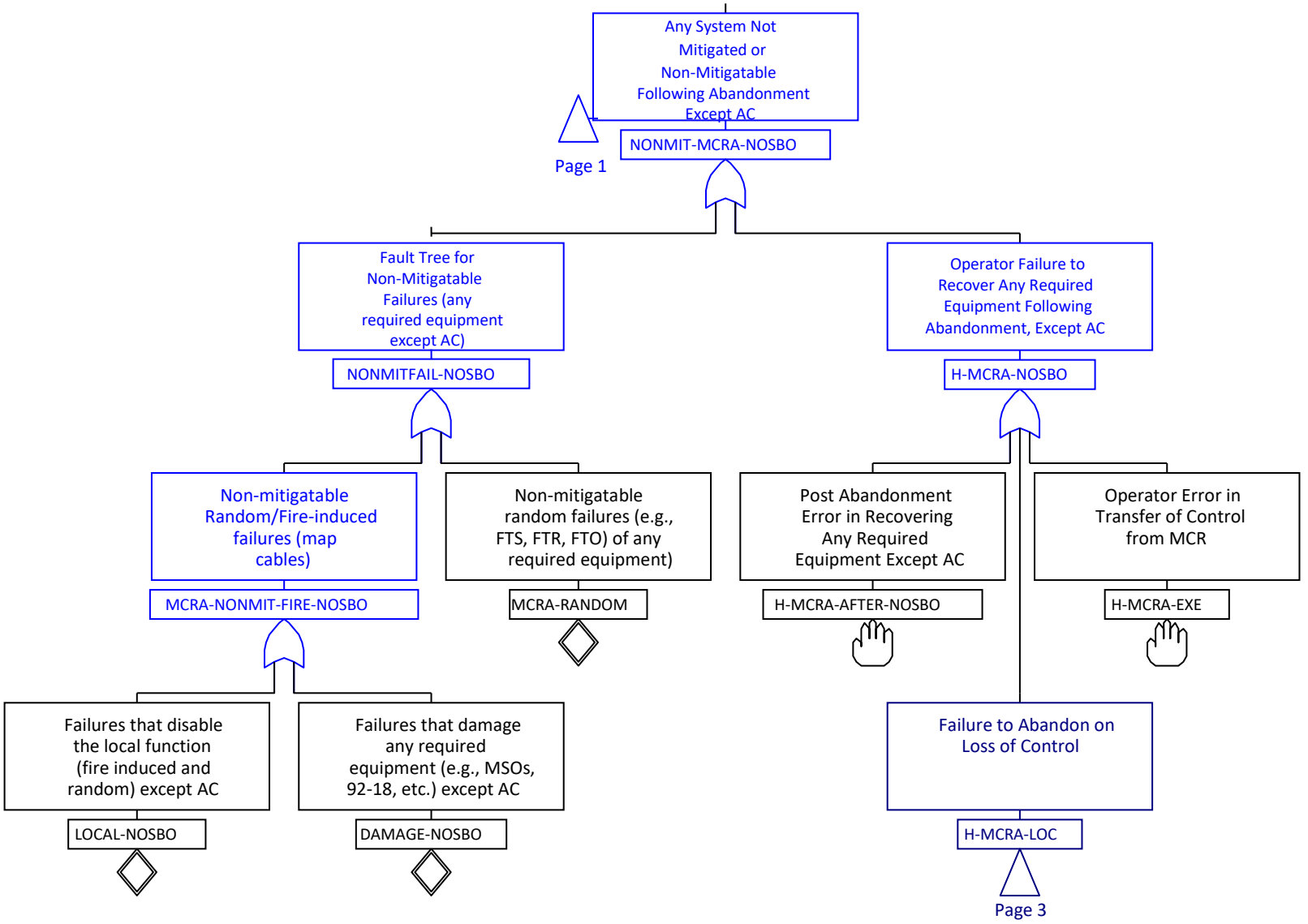


Figure 3-6
Example logic for scenario bin approach for MCRA into the PRA model (sheet 2 of 3)

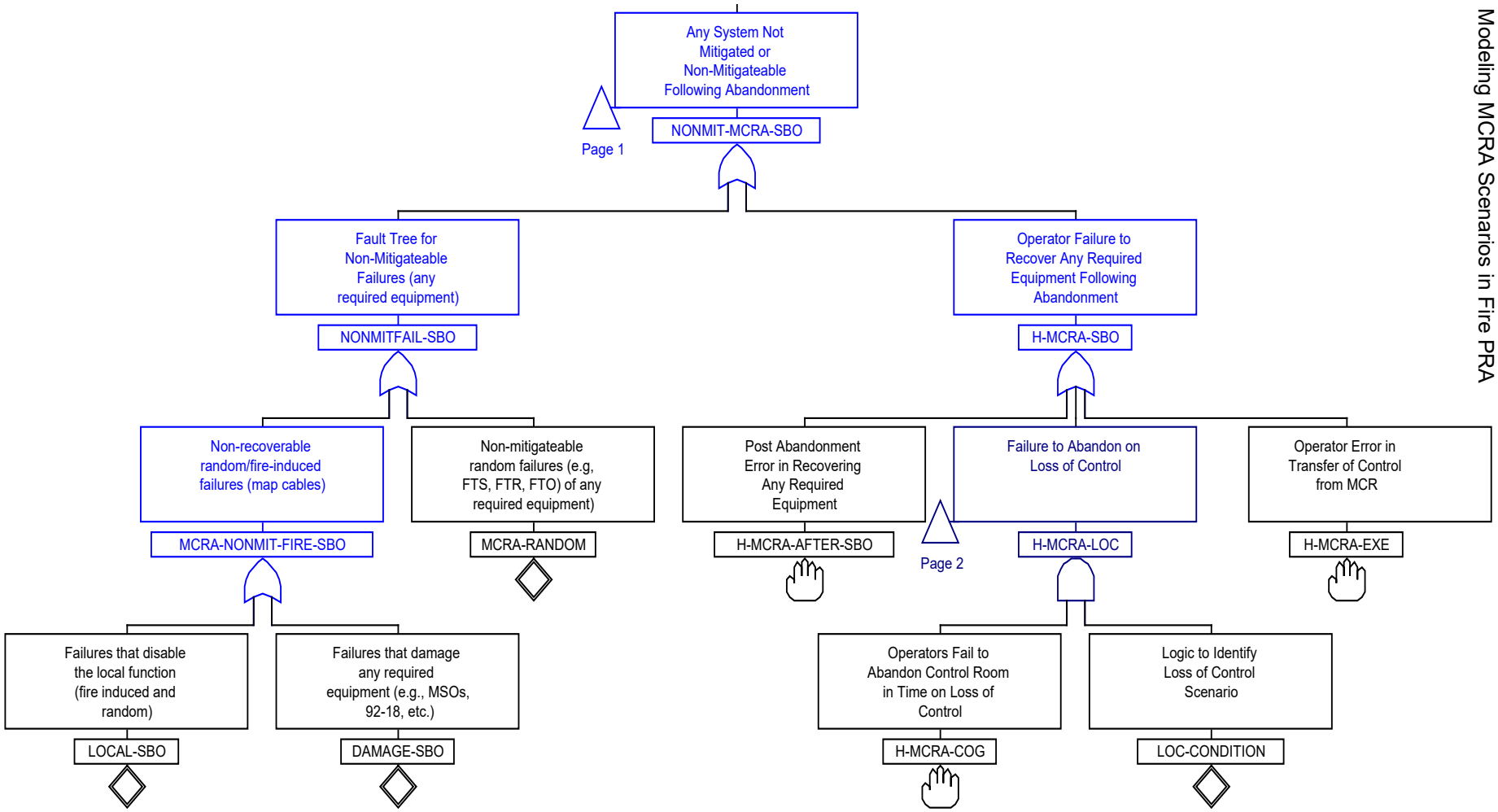


Figure 3-7
Example logic for scenario bin approach for MCRA into the PRA model (sheet 3 of 3)

3.8 References

1. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008*, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,* The American Society of Mechanical Engineers, New York, NY, February 2009.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD: 2005. EPRI 1011989 and NUREG/CR-6850.
3. U.S. Nuclear Regulatory Commission, NUREG/CR-6738, *Risk Methods Insights Gained From Fire Incidents,* Washington, D.C.: September 2001.
4. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.

4
ANALYSIS OF THE DECISION TO ABANDON

This section provides guidance for developing the definition and performing the qualitative assessment of the HFEs associated with the decision to abandon the MCR for both LOH and LOC. For LOH, fire-induced conditions lead to uninhabitable conditions in the MCR. For LOC, plant monitoring and control may not be achievable due to fire-induced damage. These scenarios may occur from fires either in the MCR or in other key plant areas such as the CSR.

4.1 Loss of Habitability

A fire-induced LOH in the MCR can result due to a fire in the MCR or due to a fire in a nearby compartment wherein smoke may enter the MCR rendering it uninhabitable. The decision to abandon the MCR is due to untenable environmental conditions within the MCR. Therefore, it is assumed that there is no contribution from the failure to diagnose and decide to abandon the MCR in time to execute a successful shutdown (i.e., the decision to abandon is always considered to be successful). Thus, for LOH, only the failure to shut down after abandonment is modeled in the PRA.

There are very clear criteria in NUREG/CR-6850 (Section 11.5.2.11) [1] related to concentration of smoke or room temperature that would result in an inability for the operators to effectively remain in the MCR. The criteria are summarized as follows:

- The heat flux at 6 ft (1.83 m) above the floor exceeds 1kW/m^2 (relative short exposure). This can be considered as the minimum heat flux for pain to skin. Approximating radiation from the smoke layer as $\dot{q}_r'' = \varepsilon\sigma T_{hgl}^4$, a smoke layer of around 95°C (200°F) could generate such a heat flux. In this approximation, ε is the emissivity assumed to be 1.0 to represent a perfect radiator, σ is the Stephan Boltzman constant and T is the hot gas layer temperature in Kelvin.

- The smoke layer descends below 6 ft (1.83 m) from the floor, and optical density of the smoke is less than 3 m^{-1}. With such optical density, a light-reflecting object would not be seen if it's more than 0.4 m away. A light-emitting object will not be seen if its more than 1 m away.

Under less hazardous conditions in the MCR, operators are assumed to stay if they are able to see through the fire-generated smoke. The visibility criterion of 3 m^{-1} optical density is intended to capture scenarios for lower intensity fires (that are not capable of forcing abandonment due to room heat up), but would generate enough smoke to cover the room and affect visibility. That is, the criterion captures the scenarios in which operators are not expected to be able to clearly see the procedures and equipment necessary to control the plant. Given the stated criterion, an operator would have to lean in to 0.4 m (i.e., less than 1.5 ft.) in order to read gauges. While they could see lights on the panel from 1 m (just over 3 ft.), operators would not be able to read the labels for these lights or to see the mimics from that distance, and certainly would not be able to see annunciators on the annunciator panels (which would be even farther away).

No criteria based on toxicity are established. Instead, it is assumed that the operators are able to use full-face masks and breathing equipment to protect against toxic/irritant gases. As long as the temperature and smoke visibility limits are not reached, the habitability criteria assume operators can use breathing apparatus and stay in the MCR for extended periods of time.

Technical Basis for Habitability Criteria

The technical bases for the habitability criteria were reviewed as part of this project and were determined to be valid for setting the time of abandonment. These criteria were developed through an iterative process that involved multiple disciplines amongst the NUREG/CR-6850 writing team, including fire modeling, human reliability analysis, and plant response modeling. Additional perspectives outside the writing team including HRA and PRA experts were consulted for their perspectives.

While MCRA was a consideration during the Individual Plant Examination of External Events (IPEEEs), there was no clear guidance provided at that time and MCRA was typically treated through a simplified approach. In instances where an actual analysis was performed, the NRC reviewers performed a detailed review. The NUREG/CR-6850 writing team reviewed the insights from the IPEEE insights report [2] and discussed past approaches with those involved in the IPEEE review process. The team drew on insights from the IPEEE when the current guidance was developed.

During the piloting of the NUREG/CR-6850 methodology, MCRA was also a topic that was discussed with operations and training. The answer was, as expected, conflicting. Some operators said that they would stay no matter what, whereas others would leave under certain conditions. Operations and training did not provide or suggest any specific threshold, although they did characterize the conditions qualitatively.

Ultimately, all of this information was assessed by the writing team and was used to develop qualitative criteria that were expressed in terms of physical discomfort (pain) and visibility (ability to see lights, signs, and gauges). As these measures cannot be directly calculated with fire modeling tools, further review was conducted to determine how the qualitative criteria could be converted into numerical criteria in terms of skin temperature and visibility, which were then related to heat flux and optical density, respectively, the latter being parameters that can be calculated, and the fire modeling engineers then formalized the criteria with the values presented earlier in this section.

With regard to formalizing the value for pain threshold, although an incident heat flux value of approximately 1 or 2 Kw/m^2 has been reported as a threshold for pain (i.e., no pain is experienced at values lower than this threshold [3]), skin exposed to temperatures in the order of 95°C (200°F) will generate irreversible damage/injury [4]. Consequently, the criterion of a temperature in the hot gas layer of 95° C (regardless of location) establishes the time at which operators are forced to leave the MCR because they will start experiencing untenable conditions (i.e., physical pain as opposed to simply severe discomfort). The habitability criteria are designed to represent conditions that would make it almost impossible for operators to stay in the MCR and perform their duties. Under such a scenario, the fire is assumed to grow unattended and generate thermal and visibility conditions that prevent operators from running the plant from inside the MCR, thereby requiring operators to implement the alternate shutdown procedure. It should be noted that operators may decide to enter MCRA procedures before fire

generated conditions reach the habitability criteria. Although the time to activate the alternate shutdown procedure is usually established based on plant operating procedures, in some cases the final decision to abandon may depend on habitability conditions as operators will not be able to physically perform their duties in the MCR.

The criteria above are engineered values to be determined by fire modeling. Since there is no formal “decision process” per se, there is no need to define an HFE for the decision, and so no further qualitative assessment is necessary. Section 3.2.3 discusses in detail how to credit LOH scenarios within a fire PRA.

4.2 Loss of Control

In addition to the LOH scenarios, there may be scenarios that involve damage to a sufficient set of cables to cause a significant loss of function (because redundant components/systems have failed), which renders the MCR ineffective for the purpose of reaching and maintaining the plant in a safe, stable state. Such fires (which could be in the MCR or in other plant locations) can result in the need for plant shutdown outside of the MCR (i.e., reliance on alternative shutdown features). In most plants, such locations have been identified by the plant's post-fire safe shutdown analysis. Typical examples of such locations include the CSR, auxiliary equipment room, and cable tunnels. These locations should be determined on a plant-specific basis.

Unlike LOH, where environmental cues like smoke and fire within the MCR are obvious, the cues for LOC in the MCR may not be as clear. Furthermore, entry criteria and/or procedural guidance to abandon the MCR given LOC may be vague or may not exist in the current procedures.

To a PRA analyst reviewing a particular LOC scenario, it may be obvious that the operators would need to abandon the MCR in order to prevent core damage. This conclusion is reached based on a full understanding of equipment and indication failures in the scenario (including all failures that occur over time), as represented by the basic events in the associated cutset(s).

The operators responding to an actual LOC scenario, however, do not have the benefit of the same understanding that the PRA analyst has. An actual fire (as opposed to the simplified scenarios developed in fire PRAs) would result in an evolving situation for the crew as they progress through the procedures and learn which equipment and indications have been impacted by the fire. In addition, operators expect, based on their training and experience, that the MCR is designed such that sufficient controls and indications needed to respond to an event will survive a fire. Consequently, the decision to abandon the MCR will be seen by operators as a last resort after all other options have been exhausted.

Because of both plant-to-plant variations and the likely lack of explicit cues for the decision to abandon, HRA modeling of the decision to abandon for LOC is typically more challenging than other fire HRA tasks. Consequently, additional guidance is needed to address this context.

As discussed in Section 3, the decision to abandon the MCR on LOC should be developed as a separate HFE. However, crediting MCRA due to LOC and modeling such an HFE must be based on a well-understood set of “cues” that the operators use to determine that a LOC condition has occurred. At present, there are two cases for establishing this basis:

1. The abandonment procedure contains explicit guidance on the "cues" for abandonment, as is typical in other formal operating procedures such as EOPs. (Currently, this case is the least common one for U.S. NPPs.)

or,

2. Explicit guidance for abandoning the MCR based on LOC does not exist, and thus a substantial amount of judgment is required. In this case, the identification (or, sometimes the development) of a set of well-understood cues is performed through interviews of operators and trainers, and requires that they provide a consistent message on "this is what we understand to be loss of control." (Currently, this case is the most common one for U.S. NPPs.)

Additional HRA modeling recommendations and qualitative analysis tips for the decision to abandon for LOC are given in Section 4.3.

4.3 Qualitative Analysis of Decision to Abandon the MCR

There is rarely any specific guidance on what constitutes a LOC and the definition of LOC is likely to be highly plant-specific. Even when MCRA is trained through simulator exercises and job performance measures (JPMs), the conditions for abandonment are generally presented to the operators as the entry to the training scenario. In other words, the decision-making process for abandonment is usually not part of the training session. In addition, there is often a credibility issue for operators in recognizing that fire-related damage could actually reach the point where the MCR is no longer the preferred center for command and control. In many cases, the conditions that could define a LOC scenario are not well known. Even if conditions that represent the definition of a LOC can be identified, there is significant uncertainty in defining fire scenarios that match these conditions, including which cables and equipment are damaged by fire and the timing of these fire-induced effects. These uncertainties further complicate predictions for the plant and operator response.

It, therefore, becomes the responsibility of the HRA analyst to evaluate the fire PRA inputs, fire response and MCRA procedures, and timing information to identify and define credible scenarios in which operators would abandon the MCR due to LOC. The HRA analyst must also evaluate whether there are scenarios for which reaching a decision to abandon the MCR is simply not feasible, given the timing, level of damage, and/or lack of cues.

The objective is to define an HFE that assesses the diagnosis and decision-making process for abandoning the MCR in time to permit the plant to be taken to a safe, stable condition. (Subsequent actions performed at the RSDP and locally in the plant are modeled as separate HFEs.) This process is likely to require several iterations as the HRA analyst develops a better understanding of the fire PRA modeling, procedural direction and training, time constraints, and PSFs.

In order to evaluate the decision to abandon, the analyst needs to understand:

- The entry criteria for the MCRA procedure(s)
- The impact of fire damage (specifically, the scenarios that could result in the inability or very high likelihood of the inability to achieve successful shutdown, if the operators remain in the MCR)

While some procedures explicitly identify specific cues (e.g., loss of identified instrumentation or equipment) that direct operators to transfer into an abandonment procedure (i.e., directions to relocate command and control outside of the MCR), this is the exception rather than the rule for U.S. NPPs today. Most MCR abandonment procedures leave the decision to abandon "up to the discretion of the operations staff," which could lead the operations staff to abandon with insufficient time to complete the necessary actions to reach a safe-and-stable state. Where such specific cues exist in the procedures, the evaluation of the cognitive HFE can be performed in a similiar manner as for other cognitive HFEs used in the fire PRA model, but additional guidance will be provided in the forthcoming HRA MCRA quantification report. Where such cues do not exist in the procedures, the process is more challenging. Regardless of whether the procedures are vague or prescriptive, the HRA analyst must still evaluate the effectiveness of the cues in providing the decision-making criteria for abandonment to the operator. The additional guidance in this section is intended to support the analysis for the more common case where the MCRA cues are not explicitly stated in the procedures.

There are a number of topics that play a role in performing the qualitative HRA of the decision to abandon, which are discussed below:

- Insights from the PRA assist in identifying the specific scenarios for which the plant can only be successfully shut down if the operators abandon the MCR. The plant conditions (e.g., plant response, equipment impacts) associated with these scenarios form the situational context under which the decision will be made.
- The scenario timeline defines the timeframe within which the decision must be made in order to prevent the scenario from progressing to core damage.
- The operator interviews provide the necessary understanding of how the operators will interpret the context as it regards the decision (i.e., what will they consider as LOC, and how does it apply to the scenarios of concern).
- The feasibility assessment determines whether the three items above, when taken together, indicate that making the critical decision to abandon within the available timeframe is possible.

4.3.1 Use of PRA Insights

Initially, the fire PRA will be constructed with no credit for MCRA. This modeling practice allows for identification of scenarios where abandonment credit would be beneficial to incorporate (e.g., scenarios with CCDP or CLERP that are 1.0 or very close to 1.0 and that also are significant risk contributors). Therefore, the PRA outputs will be a good source of example LOC scenarios to discuss in conversations with the operations staff to determine if credit can be taken for MCRA. Note that high CCDP and CLERP scenarios may end up being excluded if their overall risk contribution is low enough. That is, the model may indicate that the only way to

damage all equipment and/or instrumentation such that operators would consider abandoning the MCR would occur in rare event scenarios (e.g., multi-compartment scenarios). Based on the frequency of such an event occurring, this scenario may be screened or truncated from the model. The results of the PRA may also be a potential iteration point for elimination of conservative assumptions in the fire modeling, which may be influencing target inclusion and target damage states.

Examination of the high CCDP/CLERP scenario cutsets or accident sequences assists in developing the context that operators will face when deciding whether to abandon due to a LOC. By starting with cutsets or accident sequences related to high CCDP/CLERP scenarios, analysts can identify scenarios where shutdown will not be possible from the MCR and the benefit of crediting abandonment procedures will be apparent. When used in combination with the fire impact tables,[21] such cutsets or accident sequences would also provide information on what indications the operator will "see" in the MCR (especially in terms of what the indications are "doing") that can be discussed during the operator interviews. In particular, operator interviews could identify which combinations of indications and/or equipment states that the crew would consider to be part of the process of diagnosing a LOC (i.e., could they interpret what they see as a LOC?). For cases where some indications are not damaged by the fire and are, therefore, providing accurate information, it is necessary to consult the thermal-hydraulic analysis to specify what the operators will see (in terms of gauges and alarms) and when they will see it. The plant fire response procedure may even provide a list of MCR instrumentation that is protected (or, conversely, not trustworthy) in case of a fire in a given location. Since, at this point, the operators have not been interviewed as to what they may use to diagnose a LOC, it is necessary to go into the interviews with this information for any candidate cues that they *may* use to identify a LOC situation.

As a side benefit, providing specific example scenarios from cutsets or accident sequences can alleviate potential operator bias to remain in the MCR. Operations staff can be asked the question “how would you shut down the plant in this scenario?” This may also lead to a change in thinking as to what indications would be used for the diagnosis of LOC.

[21] For PRA software that generates cutsets, the cutsets generally do not show the fire-induced failures caused by the fire scenario since these are set to “TRUE” in the quantification process and subsumed out of the results. However, the cutsets will indicate which fire scenario is involved. By consulting the fire impact tables for the scenario, the analyst can determine which indications are affected and the potential for false or misleading information. Fire impact tables relate each scenario to the equipment that fails to perform its function through a relational “chain of links” from ignition source to fire model to affected cable trays to affected cables to component functional failure, thereby providing a list of functional failures associated with each scenario. In addition to including all the front-line and support components failed by the scenario, this list will be inclusive of all controls, indicators, and alarms affected by the fire scenario. This approach is also generally applicable for PRA software that generates accident sequences.

4.3.2 Consideration of Timeline

Per NUREG-1921 [5], since "... the decision to leave the MCR—and the timeliness with which this decision is made—can have serious ramifications for reaching safe shutdown, analysts will need to provide as reasonable an estimate as possible for the time at which the decision to abandon would be made." Fundamentally, the issue in the decision process is not if the decision to abandon is made, but if it is made in time to restore control and prevent core damage (i.e., before core damage is inevitable regardless of what is done).

Specific guidance for the development of the timeline for the decision to abandon is provided in Section 7.3.3. Figure 7-1 discusses the three time phases that occur during an abandonment scenario.

4.3.3 Operator Interviews

When the procedure's entry criteria do not contain specific, objective cues to be used for determining whether to abandon, the HRA process of interviewing the operations staff takes on a greater role in the cognitive HFE definition and assessment for MCRA. It is, in fact, the only way to determine if any conditions could exist that would lead operators to abandon the MCR. Thus, the decision to abandon on LOC is a plant-specific question. One of the goals of plant-specific operator interviews is to establish, in the absence of explicit proceduralized cues for when to abandon, that the operational staff has a consistent interpretation of what would be considered a LOC. The second goal of the operator interviews is to develop timing information associated with the decision to abandon. Multiple interviews may be involved in this process in order to gain the perspective of different operations crews to establish the existence of a consistent interpretation. This interview process should also include a walk-through of the MCR panels, pointing out specifically what they would see (and not see) in the scenario(s) of interest, since this visualization is more concrete. If possible, running the scenario on the simulator would provide an even better perspective. In general, operators are biased to use field operators to perform local operations, rather than initiating an MCRA, given the familiarity and comfort operators have in responding to plant transients from the MCR. Specific questions should be asked in order to determine what equipment (including controls and indications), if any, would direct an operator to lose confidence in the ability to safely shut down the plant from the MCR. A distinction should be made between fires that occur in the MCR versus fires that occur in other areas covered by the MCRA procedures and how they influence the decision to abandon.

Follow-up discussions are likely to be needed to clarify information from the interview or to ask additional questions. These follow-up inquiries should also be organized to make the best use of limited operator availability.

4.3.3.1 Interview Questions

The interview process needs to be structured in order to be effective and complete. Below is a suggested list of questions that address the information needed from the operators in order to formulate the qualitative (and eventual quantitative) analysis of the decision to abandon the MCR for LOC. While useful in guiding the discussion, they are not intended to limit the scope of the interactions between analysts and operators. (More information on talk-throughs can be found in Section C.3.1.) The analysts should allow the discussion to follow a course dictated by the answers in order to have sufficient depth of understanding of the decision process. However, the analyst should make certain that all of these questions are addressed.

1. In general, under what conditions would you consider leaving the MCR?
2. What procedure(s) are used for this situation? How do they interact with the plant fire procedure and EOPs/ Abnormal Operating Procedures (AOPs)?
3. What are the entry criteria for abandonment?
4. Which staff person makes the decision to abandon? Does the procedure specifically indicate the conditions for which abandonment for fire is required? If not, which systems or functions would you have to lose to make the decision to abandon the MCR?
5. Describe the training for MCRA:
    a. Is there simulator training on when to leave the MCR?
    b. How often is training performed on MCRA? For fire?
    c. Does training cover the decision to abandon (e.g., what it means to have a LOC?)?
    d. Does training focus on time critical actions? If so, what are the timing requirements and timing pinch points?
6. Do you have a feeling for how long it would take to make that decision to abandon? Is this covered in training (and timed)?
    a. Under what conditions would you leave the MCR sooner?
    b. Under what conditions would you remain in the MCR longer?
7. Using the fire PRA, we have identified the most likely scenarios that would lead to a situation where remaining in the MCR would ultimately lead to core damage. We are going to describe the conditions you would face in these scenarios (what you would see on your indications). We will ask you what you would do in such situations. [Option to add the following: Note that we may include scenarios that would not lead to core damage if you remain in the MCR.][22]

For the last question, it would not be surprising to get the response, “I will never leave the control room on loss of control.” This response can be reinforced by the fact that there has never been any actual simulator training on a true LOC situation. Training is generally focused on the “Appendix R” scenarios that are designed to be recoverable while remaining in the MCR.

[22] In cases where the decision guidance is particularly vague or the answers vary quite a bit, it may be useful to add this and to have available some scenarios that are quite serious, but would be best served by staying in the MCR. This can provide a good perspective on the “transition point” for their decision.

Years of training on these scenarios, which are often (erroneously) referred to as “worst case,” may make it impossible for the operators to envision a situation where there is even such a thing as a fire that cannot be responded to successfully from within the MCR. It is important to re-direct the conversation from generalities to the very specific scenarios and the associated equipment failures, then walk-through the procedures step-by-step explaining what they will see (or not see) happening. If the interviewer gets the reaction “That’s not possible” they need to remain on track and make clear that the PRA shows it is not only possible, but it is a high risk if the response is not successful.

4.3.3.2 Post-interview Assessment

The post-interview assessment is focused on determining the feasibility of the diagnosis, which to a large extent relates to the impact on PSFs. Overall guidance on fire PSFs is provided in Section 4.6 of NUREG-1921[5]. These PSFs are applicable to varying degrees when modeling the cognitive decision to abandon the MCR. Section 4.3.5 provides additional specific insights on PSFs associated with the decision to abandon in a LOC. PSF insights for actions taken after the decision to abandon are made are outlined in Section 8. Note that, if the determination is made (based on the operator interviews) that a consistent interpretation of LOC does not exist and cannot be justified, then abandonment on LOC cannot be credited. Command and control would be assumed to remain in the MCR regardless of how many operators may be dispatched to perform local operations, and the modeling and HRA for all non-LOH scenarios would be performed in accordance with NUREG-1921 (i.e., not using this report).

As stated previously, the scope of this report does not include guidance for situations where the MCR does not need to be abandoned.[23]

4.3.4 Key Feasibility Assessment Considerations

As this section focuses on the decision to abandon, the issue of feasibility is the answer to the following question:

> Are the characteristics of the abandonment decision-making process sufficiently clear such that it is feasible that the decision to abandon would be made in time to successfully shut down from outside the MCR?

Therefore, one of the keys to this assessment is time. The only operator action modeled is the decision to abandon, and this decision must be made in time.

[23] However, the scope does cover the situation where command and control is transferred out of the MCR, but an operator either remains in or is dispatched to the MCR to perform actions under the abandonment procedure. In this case, this operator is treated in the same way as other operators who perform local actions under the direction of the individual who has command and control authority under the abandonment procedure at the new location.

Until the interviews are conducted, analysts do not know what cues will actually be understood by the operator to represent a LOC. Also, analysts may not know how the decision to abandon will be made, or if operator biases could support or delay a timely decision. There are two key considerations that could result in a determination that the decision to abandon cannot be made within the time available:

1. At what time does the minimal combination of cues occur (the cues that the operators say would lead them to determine that LOC has occurred and that they should consider abandoning the MCR)? Is this time less than the total time available for the decision to abandon? If so, this time becomes the delay time for the decision to abandon in the timeline (see Section 7 for a full discussion of timing and timing terms).[24]
2. The delay time for the decision to abandon is added to the estimated time needed for the operators to make the decision to abandon (i.e., time needed for cognition - see Section 7 for further discussion). If this sum is less than the total time available to make the decision to abandon, then the decision to abandon is considered to be feasible.

This feasibility determination needs to be made in the context of the key scenarios that were identified by the PRA (Section 4.3.1), which were used in the interview process. A single determination is often sufficient to cover all of the abandonment scenarios (LOC being a defined condition based on the interviews). In some cases, it may be necessary to bin the scenarios, then perform the feasibility assessment for each bin (including consideration of the associated delay time and cognition time).

Only two PSFs are directly relevant to this feasibility assessment as discussed above (i.e., two considerations play directly into the determination of these two time elements). The other PSFs associated with the decision to abandon (discussed in Section 4.3.5) would form the full characterization of the HFE and affect the subsequent determination of the HEP. The two PSFs are:

1. **Cues and indications** will vary with the effect of fire damage to the associated cables. There may be a number of “soft cues” such as spurious cycling of plant equipment due to fire damage or unreliable indications. Due to the nature of the scenario, there is generally not a single clear cue or set of clear cues to direct the abandonment of the MCR. The decision may be based on, for example: a) the inability to operate equipment from the main control board (MCB); b) visible MCB panel damage; c) loss of indications; or d) spurious equipment operation AND the nature of the fire is such that there is concern about maintaining the ability to safely control the plant. Cues used by operators to determine that they have lost the ability to control the plant from the MCR should be identified based on the interviews.

[24] Example: Fire causes total loss of feedwater (FW) because control circuits of all AFW pumps are impacted. FW must be re-established in 60 minutes. It takes 25 minutes from the time when the decision is made to abandon until feedwater can be re-established, leaving 35 minutes to make the decision. The operators state that they would not consider control lost until they had attempted to try bleed-and-feed and it did not work. The time it takes to get to the point where they would try bleed-and-feed and would have indication it would not work is 45 minutes. The cue is too late.

2. **Procedures and training** that are relevant to identifying LOC conditions and deciding to abandon the MCR are plant-specific. Typically, the fire-damage-related conditions that would result in the Shift Manager (SM) or Shift Supervisor (SS) calling for MCRA due to LOC are not well-specified in the procedure. The basis for determining how the procedures are interpreted and implemented in making the decision to abandon need to be based on interviews with operations and training personnel, as previously discussed. This interview-based information is also needed to describe and model the scenario(s) properly, identify relevant fire compartments and equipment impacted, and to determine the crux of the abandonment decision. The HRA analysts need to review both the procedures and the training discussed during the interview to understand the level of detail provided to the SM/SS in aiding the decision to abandon. When the decision criteria for abandonment are ambiguous, the decision to abandon may be at the discretion of the SM/SS, which would influence the cognition time associated with the abandonment timeline.

4.3.5 Other PSF Considerations

Even if the feasibility of the decision to abandon has been established (i.e., there is procedure guidance, training, and/or there are cues and indications), it is still likely that the crew will be hesitant to leave the MCR. This hesitancy is based on the quality of training, quality of the procedures, and the crew's confidence that the shutdown strategy outside the MCR will lead to success. The following factors could influence the decision to abandon:

- **Capability of RSDP**. Every plant has a unique RSDP and the capability of the RSDP may influence the decision to abandon. For example, in new reactor designs, the RSDP is a computer system nearly identical to the MCR and all systems available inside the MCR are also available outside the MCR. In these NPPs, the operators would likely be less hesitant to leave the MCR than operators at NPPs where only a limited number of systems and indications are available at the RSDP.
- **Complexity**. For current MCRA strategies, complexity is more of an issue for the post-decision actions than for the abandonment decision itself. In other words, complexity is more of a concern after abandonment. However, it is possible that cognitive complexity could be considered for the decision to abandon. Further guidance for both execution and cognitive complexity are deferred for a later report on MCRA HRA quantification guidance.
- **Workload, Pressure, and Stress** are addressed in NUREG-1921 [5]. That guidance will be sufficient for the decision to abandon HFE because there is minimal difference between the workload, pressure and stress of a very serious non-abandonment scenario and an abandonment scenario and the associated decision process. After abandonment, the actions required would result in increased workload, pressure and stress, which are all discussed in Section 8.
- **Environment** is addressed in NUREG-1921 [5], which considers both fires outside and inside the MCR. The fact that a scenario might lead to LOC does not alter this guidance.

- **Crew Communications, Staffing, and Dynamics** are, for the most part, sufficiently addressed in NUREG-1921 [5] to cover the needs of MCRA due to LOC. While communication between the MCR and the fire location is essential for determining the severity and controllability of the fire (if that assessment is part of the abandonment strategy), this generally applies to the assessment of all fires as part of the fire procedures (whether or not the scenario leads to LOC). There is one special consideration for crew dynamics because the decision to abandon is based on discretion of the SM or SS, as opposed to clearly mandated by procedure. The crew dynamics in this case may be different from other decisions made in the MCR during fire scenarios. The extent to which this is an important aspect of the decision depends on both the way the procedure is written (e.g., who has the authority to make the decision), and also the culture of the operating crew (e.g., would such a decision be made in an "executive" fashion by the SM or would the decision be more of a consensus process). This clearly affects the potential for recovery from a decision to not abandon the MCR (when, according to the PRA, the only viable course of action is to abandon). This type of information can be obtained through interviews and/or simulator exercises.
- **Additional PSFs** are outlined in NUREG-1921. However, no special considerations need to be taken for the human-machine interface (HMI), special equipment or special fitness needs as these PSFs typically affect execution and will not impact the cognitive decision to abandon the MCR.

4.4 References

1. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD: 2005. EPRI 1011989 and NUREG/CR-6850.
2. *Perspective Gained From the Individual Plant Examination of External Events (IPEEE) Program*, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Washington, DC: April 2002. NUREG-1742.
3. *Predicting 1st and 2nd Degree Skin Burns from Thermal Radiation.* SFPE Engineering Guide. RPT 200802817. 2000.
4. Wieczorek, C. and Dembsey, N., *Human Variability Correction Factors for Use with* Simplified *Engineering Tools for Predicting Pain and Second Degree Skin Burns.* Journal of Fire Protection Engineering 11, 2 (May 2001) pp. 88-111 J200501350.
5. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.

5
IDENTIFICATION AND DEFINITION OF HFEs FOR MCRA SCENARIOS

5.1 Introduction

The objective of this section is to provide guidance on how to identify and define the HFEs credited for MCRA scenarios. The identification and definition tasks are used in conjunction with the fire PRA modeling guidance (presented in Section 3) and the guidance on developing MCRA timelines (presented in Section 7) by analysts in order to: 1) develop the necessary understanding of the expected progression to safe shutdown, and 2) identify the actions needed in the fire PRA to evaluate the reliability of safe shutdown given an MCRA fire scenario. In particular, the concepts of feasibility assessment and timelines for MCRA scenarios are needed to fully understand this section on HFE identification and definition.

5.2 Background

As described in NUREG-1921[1], MCRA actions are a special case, or a subset, of fire response actions. As discussed earlier in Sections 1 and 2, what is different from other fire response operator actions addressed in NUREG-1921 is that the MCRA actions are a collective set of actions that typically involve more coordination and communication than other fire response actions. In addition, Section 3 of this report describes PRA modeling strategies that start the HRA tasks of HFE identification and definition by providing guidance to: 1) identify if and how the fire PRA model needs to be modified based on the operator actions, and 2) identify critical actions whose failure will be modeled as HFEs. This section will complete the needed guidance regarding HFE identification and definition tasks for MCRA scenarios.

The following steps summarize the identification and definition steps, as originally documented in NUREG-1921, with notes to indicate what additional guidance is needed for these steps to address MCRA scenarios:

- Identify and categorize HFEs:
  - Internal events HFEs that are also used in the fire PRA – MCRA HRA may credit some actions taken before operators leave the MCR and these actions may already have been modeled in the internal events PRA. Additionally, the internal events HRA may provide useful insights into some of the critical tasks needed to accomplish the actions modeled in the MCRA HRA.
  - Fire response HFEs – These are new actions added to the fire PRA. Actions taken following the decision to abandon fall into this category.

  - HFEs associated with MCRA. Although briefly discussed in NUREG-1921, it is likely that these HFEs have not been previously identified and defined. Some of these actions associated with these HFEs may be based on procedures used in the MCR. However, all of the HFEs associated with actions taken after abandonment are typically based on a separate, stand-alone procedure (or set of procedures). Section 2.2 and Appendix A noted that this procedure addresses multiple reasons for MCRA with fire being one of them.
  - HFEs corresponding to undesired operator responses to alarms and indications – This category is addressed in NUREG-1921 and is not addressed in this report.

- Define the context and initial conditions for evaluating the HFE (including an initial assessment of the feasibility - see next bullet)
- Feasibility Assessment - Because the feasibility assessment is crucial in MCRA HRA, the topic is discussed in greater detail in Section 6. However, the feasibility check will be an ongoing step throughout the MCRA HRA process.

5.3 Understanding of Expected Plant Response for MCRA Scenarios

The first step of the MCRA HRA process is to understand the expected plant response for MCRA scenarios. In order to build this understanding, the deterministic safe shutdown analysis for MCRA[25] is reviewed in conjunction with the fire PRA's plant response model and timelines. This review should specifically consider the fire progression, accident progression, and operator's progression through procedures. The deterministic safe shutdown analysis begins with the decision to abandon and does not include any actions taken inside the MCR before the decision to abandon has been made. The fire PRA considers both actions taken before MCRA occurs and the actions taken after the decision to abandon the MCR has been made. See Section 7 for additional discussion of time phases of MCRA. The following process can be used to incorporate insights from the safe shutdown strategy into the fire PRA for MCRA scenarios.

- **Review the list of fire scenarios that may cause MCRA**. The HRA/PRA analyst needs to understand what components/systems are impacted by the fire and which fire-induced initiating events the MCRA scenario is trying to mitigate. For example, fire-induced initiating events could include:
  - Loss of main feedwater (MFW)
  - Transient
  - Loss of offsite power (LOOP)
- **Review and comparison of the fire PRA description of the expected sequence of events versus the safe shutdown strategy.** In reviewing the MCRA procedure, the HRA analyst must understand that the strategy followed by each plant after MCRA is heavily controlled by the plant-specific installed features and controls. The existence (or not) of a RSDP, the extent of its functionality, and the need for actions at other locations will dictate

[25] The deterministic safe shutdown analysis is an assessment of the ability of the plant to achieve a safe shutdown given a fire that affects the entirety of a designated fire area. In the United States, these are referred to as the "Appendix R fires," some of which are fires that assume MCRA is required.

the format of the procedure (e.g., use of MCRA procedure attachments dedicated to establishing certain functions) and, therefore, the development of logic structure for modeling MCRA in the fire PRA. See Section 3 for additional discussion. This interaction is what makes MCRA HRA uniquely challenging.

- **Review and comparison of the initial conditions assumed by the fire PRA and safe shutdown.** This review should also include which systems are assumed failed at the start of the event. For example, the safe shutdown scenario may assume main feedwater is unavailable for all scenarios whereas the fire PRA may credit main feedwater in scenarios for which it is known to be available.
- **Specifically, review operator actions related to LERF, since LERF was not addressed during the plant updates to meet Appendix R fire protection requirements.**
- **Review the expected operator response based on the MCRA procedural direction in comparison with the fire PRA expected response and safe shutdown response.** The operator actions in the fire PRA are developed based on fire PRA success criteria and this may or may not align with expected actions in the MCRA procedure (see also Section 3.3). This comparison identifies the positive and/or negative impacts the operators' expected actions can have on the scenario, even if the actions are not explicitly modeled for MCRA.

5.4 Information Gathering Using Talk-Throughs and Walk-Throughs

This section provides a brief overview of information gathering using talk-throughs and walk-throughs, but further details, including templates for questions and information collection, are provided in Appendix C. In this context, a "talk-through" involves interviews and discussions with appropriate personnel, while a "walk-through" involves physically walking down the plant and/or scenario.

The expected plant response for MCRA scenarios is typically evaluated by the HRA analyst by conducting walk-throughs, talk-throughs, and other discussions with operators, operator trainers, and other operations personnel.[26] The purpose of these interviews are to understand:

- Proceduralized operator actions expected during the accident sequence progression through the fire scenario, for both the success path as well as failure paths. This understanding should include operator actions for both CDF and LERF.
- Any assumption(s) with respect to the expected plant behavior, system response, equipment response, and operator response (e.g., what equipment is assumed to be unavailable, single failures of systems assumed to have occurred).

The operator interviews should include a discussion of the expected plant behavior and operator response during the three time phases of MCRA as described in Section 7. Phase I includes the expected response before the operators leave the MCR; Phase II includes the decision to abandon and how this decision will be made; and Phase III includes the expected plant response after the decision to abandon has been made.

[26] This collective set of plant personnel is used to represent anyone at the plant familiar with the expected plant response for MCRA. It is often helpful to get multiple points of view. So, in many cases, more than one individual is interviewed.

The emphasis during the talk-throughs is: 1) to understand how operators use the procedures, 2) to understand what are the key decision points and time constraints of the process, and 3) in general, to gain a sense of the operations and training perspective on the scenario, how it evolves, and how it has been trained.

In comparison, the walk-through provides the analysts the opportunity to view the locations, conditions, and interfaces with the RSDP and other equipment cited in the MCRA procedure steps. It allows the analysts to identify particularly challenging actions due to equipment location (e.g., time required to get there), access (e.g., cramped workspace or ladder use), or physical workload (e.g., number of turns and force required to manually align a valve). Insights can be gained into the travel times from one point to another and performance times for key tasks. Knowing what needs to be done in a timely manner in the MCR prior to abandonment and at the RSDP afterwards could even help identify potential procedure changes or plant modifications (e.g., installation of kill switches) that could simplify actions, save time, and impact operator reliability.

As part of the walk-through preparation, there is a key interface between the PRA and the HRA that needs to take place. Since the talk-through will have covered all the actions in the procedure, and an understanding will have been developed regarding all of the actions and the operators' perspective on why the actions are performed, it is necessary to get the PRA perspective on the risk significance of the various actions so that during the walk-through a conversation can be started with the operators regarding any actions that might detract from the swift completion of the actions that are shown in the PRA to be critical.

Based on the initial talk-through, the analysis team should have identified the locations associated with the PRA-relevant procedure steps in the MCRA strategy that they would like to see during the walk-through. These locations should be identified prior to the walk-through to ensure that the appropriate access is obtained. The walk-through needs to be organized, even if informally, so that the analysis team can see what they need to see during the time allotted. Viewing the RSDP and other local action locations is crucial since the analysts must understand the plant-specific displays, capabilities, and limitations.

The travel time and the time to perform each procedure step identified during the talk-through should be determined during the walk-through. The time required for operators to communicate with other remote operators to give orders and receive report-backs should also be determined during the walk-through. A member of the walk-through team should record these time measurements for future use during qualitative/quantitative analyses and feasibility assessments. The walk-through should focus on the Phase III actions and specific consideration should be given to the time to complete difficult HMI tasks (such as physical exertion needed to turn a hand wheel), as well as tasks related to complex coordination and communication among operators. Information that will be useful to the assessment of the PSFs discussed in Section 8 also should be considered during the walk-through. This information includes the nature of the HMI (e.g., presence of mimics, type of display being read, type of manual control), whether the equipment is one among many in a similar grouping, and whether there is clear and unambiguous labeling of equipment.

The walk-through also provides an excellent opportunity to gather information to assess feasibility criteria such as communications, lighting, and accessibility of tools/keys/personnel protective equipment. See Section 6 on feasibility assessment for further details.

5.5 Actions Required for MCRA Safe Shutdown

Each plant should have a pre-defined deterministic safe shutdown strategy for MCRA.

This section describes some of the different approaches identified at different plants. It is the HRA analyst's role to identify the plant-specific strategy. The analyst may find that reviewing other plants' approaches can be helpful. It is extremely important to understand that the variations discussed in this section are not necessarily mutually exclusive within the plant's abandonment strategies. For example, it is entirely possible that a plant may have different types of installed features used for recovering different functions, different communication strategies for implementing different parts of the abandonment procedures, and so forth.

5.5.1 Actions Taken Before Transfer of Command and Control Outside the Main Control Room

Most fires will not lead to immediate abandonment following the start of the fire and reactor trip. Consequently, the operators will have the time to implement some actions. For slower progressing scenarios, the crew may have time to perform many EOP actions before abandonment. Such actions could include, for example in PWRs, tripping the RCPs (to minimize the risk of a seal LOCA in case RCP seal cooling is lost), tripping the turbine, and closing the MSIVs (to ensure there is no uncontrolled steam flow).

Once the decision to abandon has been made, most plants require a few actions to be completed in the MCR just prior to abandonment. These actions could include:

- Trip the reactor, if not already tripped
- Activate and transfer control to the RSDP or equivalent
- Obtain keys inside the MCR (which are then used to power up the RSDP) and actuate disconnect switches that isolate key controls of the MCR
- Disconnect power switches to isolate the MCR from additional spurious operations

5.5.2 Actions Taken After Transfer of Command and Control Outside the Main Control Room

Once the MCR is abandoned and command and control has been established outside the MCR, bringing the plant to safe shutdown will rely on actions taken outside of the MCR.

Most, if not all, RSDPs do not have all the functionalities of the MCR. Severe fire scenarios could cause damage that, to be mitigated, would require controls beyond those available at the RSDP (i.e., some actions would need to be performed locally). Also, in order to reach safe shutdown, actions may need to be performed at multiple locations. Performing multiple actions at multiple locations will require communication among operators, because, in most cases, there is not enough time for a single operator to perform all of the actions sequentially.

Consequently, to address timing requirements, the majority of remote shutdown strategies require the coordination of multiple operators performing actions at different locations at the same time. Actions required at multiple locations will require the role of each operator to be well defined. If this is not done, a timely execution may not be achieved. Some abandonment procedures may stipulate the assignment of each crew member, while others may assign a

specified role only to some key personnel (e.g., reactor operator, turbine building operator), giving leeway to other personnel to provide assistance where needed. In cases where the site has several units and one of the units is not adversely affected by the fire, some crew members from the non-impacted unit may be assigned to assist the affected unit.

As is done in the MCR, the best communication plan would be to have all operators performing communications face-to-face. However, this is not always possible for MCRA scenarios due to multiple actions being performed at multiple locations. There are various communication strategies that have been implemented in abandonment procedures, which can be summarized into three broad groups:

- Face-to-face communication, where the operator controlling the abandonment process is co-located with operators performing the abandonment actions
- Hard-wired communication (i.e., plant phone system), where the operator controlling the abandonment process is not co-located with operators performing the abandonment actions, but the action locations are well-delineated (i.e., compact) and the area is equipped with fixed, dedicated communication stations
- Radio communication, where the operator controlling the abandonment process is not co-located with operators performing the abandonment actions, but for each operator either: 1) the action locations are well-delineated but the area is not equipped with fixed dedicated communication stations, or 2) the action locations are not well-delineated and so the operator must move between multiple locations

It is not unusual for a plant to have a combination of these communication strategies within their overall abandonment strategy. For example, a higher capability RSDP would allow more actions to be co-located with command and control, minimizing the need for radio communications.

One way that plants can address time-critical MCRA actions is to minimize the time needed to establish control at the RSDP by preparing the RSDP in advance of the decision to abandon the MCR. In the first minutes after the fire is detected, operators will get briefed on the severity of the fire. For severe fires, an operator is dispatched to the RSDP to pre-stage it for potential operation. This pre-staging typically consists of ensuring that switches at the RSDP are in their appropriate initial position and performing all the steps required to ensure that, when notified, the RSDP can immediately be made operational. Because this strategy is performed concurrently with the decision-making process of abandoning the MCR, it gives shift supervision additional time to decide whether or not to abandon. A drawback of this approach, however, is that it removes an operator from the MCR, which will require other operators to assume his/her role.

5.5.3 Actions Taken That Use the Main Control Room as a Local Station During Abandonment

An infrequent variation on the strategies discussed in Section 5.5.2 is the use of the MCR as one of the local stations manned by an operator when the control room is abandoned on LOC (but not LOH). This allows the potential to operate equipment or observe other plant parameters that cannot otherwise be operated or observed from the RSDP and is not electrically isolated when the RSDP is fully activated. This may provide an additional response option if the fire did not cause a failure of equipment that could back up a safety function.

5.5.4 Non-MCRA Scenarios: Command and Control Remains in the Main Control Room

The strategy discussed in this section is not an MCRA scenario, but involves the use of the RSDP to achieve safe shutdown. Since this is not a MCRA situation, this document does not provide detailed guidance. The existing guidance in NUREG-1921 and NUREG/CR-6850 is deemed sufficient.

In this strategy, command and control remains in the MCR, but operators are dispatched to the RSDP and other locations to perform local actions. It is only applicable to scenarios in which the MCR remains habitable. This strategy draws its appeal from the fact that the MCR: 1) remains the central hub for communications in the plant, 2) is a location that the operators are used to working in with well-established communication protocols, and 3) has the entire set of procedures needed for safe shutdown, which helps for informed decision-making. Drawbacks of this strategy, for severe fires, include: 1) it can be expected that key monitoring parameters will be lost in the MCR, or will provide misleading information, 2) the designated command operator will need to know which instruments or indications are unaffected by the fire and can be used as reliable cues for action, and 3) the designated operator will need to communicate with individual operators at local stations where reliable indicators are available in order to control the plant.

5.6 Identification of MCRA Operator Actions

Once the expected plant response following MCRA is understood, then the MCRA operator actions can be identified and defined as HFEs, then incorporated into the overall fire PRA model.

The same HRA identification steps apply as for other fire response actions described in NUREG-1921:

- Review of plant procedures, identify proceduralized actions.
- Review of the PRA model, specifically the accident sequence development and success criteria portions, in order to understand:
  - Context for the actions including the fire-induced initiating event and the fire damage
  - HFEs already identified as being a part of the fire PRA
- Review of the PRA results to identify actions that could mitigate fire-induced failures. This could include identifying actions that are currently not in the procedures, but, if added, could provide a reduction to the overall risk. For example, the fire PRA considers MSOs for a given fire scenario and these scenarios may not be considered for safe shutdown; and therefore, procedure guidance may not currently exist.

These steps are typically conducted in an interactive manner. Before the procedure review can be effective, the fire progression and impact on SSCs should be understood, including how the progression fits with the MCRA timeline(s) described in Section 7 of this report.

For MCRA, the HRA analyst will need to first identify MCRA scenarios included in the PRA and for each scenario identify a set of operator actions required by the PRA to mitigate each scenario.

For MCRA scenarios, there are several types of operator actions to consider modeling as HFEs as summarized below:

- Decision to abandon for LOC scenarios (further details provided in Section 4)
- Actions in the MCR taken after the decision to abandon has been made but before the operators leave the MCR - these actions can include reactor trip, turbine trip and isolation of the MCR circuits
- Actions to establish command and control at the RSDP (or other control station outside of the MCR) including establishing instrumentation at the RSDP
- Actions to start-up and control support systems and front-line systems, as needed, in order to fulfill the following key safety functions. The fire impact may range from only affecting a single function to challenging several safety functions, simultaneously. These functions implicitly include the support systems and instrumentation necessary to start and sustain the function for the mission time modeled in the MCRA analysis. The safety functions include:
  - Ensure subcriticality
  - Provide injection
  - Ensure decay heat removal
  - Provide containment isolation
- Actions to mitigate fire damage (e.g., shut a primary PORV block valve given a spurious opening of a PORV)
- Actions to establish long-term control for support systems and front-line systems to meet the PRA mission time. These long-term control actions are often considered to be negligible contributors for internal events HRA, but long-term control from the RSDP could be more challenging and these actions should not be screened from consideration initially. Examples of long-term actions could include:
  - Maintain RCIC control at RSDP or maintain reactor pressure vessel (RPV) level by any means necessary
  - Maintain decay heat removal at RSDP
  - Maintain RPV pressure and/or depressurization
  - Maintain EDGs by either load shedding systems or refilling fuel tank
  - Maintain AFW inventory by refilling CST or aligning alternate suction source to AFW

The potential mapping of these operator actions to HFEs are shown in Table 5-1, and is further discussed in Section 5.7.

Most MCRA procedures end when the front line systems are established as operating. Following startup of a system there is often a procedure step or two that will say “maintain control.” Typically, this implies simply monitoring a level and/or pressure and making small adjustments due to decay heat. Additionally, there is a second set of actions in which inventories deplete and the operators must respond with more complex execution steps to maintain inventory. An example of such an action is to refill a tank. Tank depletion and battery depletion are two failures to be considered to support the PRA success criteria. These actions can be identified by reviewing the internal events set of operator actions and PRA success criteria. In many cases, the response to performing these long-term actions maybe the same as for scenarios modeled in internal events. However, the cue for the internal events actions are often alarms and indications within the MCR. Following abandonment, the cues for these actions need to be defined and available.

Not all plants and/or fire scenarios require all the types of actions identified above; the need for these types of actions is based on the success criteria and the plant’s specific MCRA strategies. Only after the fundamental strategy for achieving shutdown is understood can the analyst then identify which portions of the strategy are feasible (as discussed in Section 6) based on the capabilities of the RSDP, the procedural and training guidance provided to the operators, and the time available for the procedure-driven actions to be performed.

5.7 Definition of MCRA HFEs

Once the scenarios and associated actions are identified, the next step is to define HFEs that can be incorporated into the PRA. MCRA is different from internal events HRA in that MCRA requires defining the collective set of individual operator actions. For a given fire scenario, the success (and associated failure) criteria need to be defined for each HFE. This includes the definition of critical tasks and the time window for operator response. HFE definition uses input provided in support of the MCRA timeline(s) described in Section 7.

The definition of HFEs to represent individual MCRA operator actions will follow the same guidance as for fire response actions. This is described in Section 3 of NUREG-1921. The human failures of fire response actions are defined to represent the impact of the human failures at the function, system, train, or component level as appropriate, consistent with requirement HRA-B1 of the ASME/ANS PRA Standard [2]. The definition should start with the collection of information regarding the context of the fire scenario. This comes from the PRA accident sequence, success criteria, and associated engineering analyses such as the following:

- The high-level (train level) task required to achieve the goal of the response (that should form the basis for the individual HFE)
- Applicability to accident sequences based on the initiating event, the fire damage, and the subsequent system and operator action successes and failures (see Section 3)
- Procedural guidance (including MCRA, fire procedure and EOPs/AOPs)
- Cues, instrumentation and other indications for detection and evaluation
- Accident sequence-specific timing of cues and the time available for successful completion (as discussed in Section 7)

- Locations where the actions are taken
- Systems and components needed for success
- Communications plan and systems
- Command and control, including staffing assignments and roles

Because each HFE is part of a collective set of actions for a given MCRA scenario, part of the definition should include a discussion of dependencies among actions. This includes defining when coordination among actions is required, identifying actions that are based on the same cues and indications, and identifying situations in which actions will be occurring simultaneously. Section 9 provides a discussion on how to account for dependencies.

For MCRA actions, the definition goes beyond that typically needed for non-MCRA HFEs. As discussed in Section 2.3, when command and control resides in the MCR, decision-making by the Shift Supervisor (or Shift Manager) is supported by additional management or staff, either required to be present (e.g., the STA) or expected to arrive due to typical response to a serious plant upset. Such support and extra help (as well as probably multiple phones) also eases the burden of necessary communications, whether it be fire brigade updates, notifications to the NRC, or reports from field operators or health physics.

However, in MCRA scenarios, command and control is likely to lose some of these supports. For example, staffing may change during MCRA due to fire brigade responsibilities (although plants are required to ensure that a basic level of staffing is maintained) and procedure assignments, perhaps even increasing for multi-unit sites where an “all hands on deck” approach to severe events is used. Consequently, command and control in MCRA scenarios typically relies upon a different level and mode of information acquisition, staffing and communications.

This in turn impacts the definition of an HFE, in that it should include a description of the following:

- Communication strategies that would be employed once outside the MCR
- Command and control structure once outside the MCR
- For plants that share a MCR between units, the impact on the non-fire damaged unit
- For a shared control room, if both crews leave the MCR due to habitability concerns, the impact on staffing, and command and control structure once outside the MCR

Appendix B provides background on the topic of command and control (C&C), examples of events where C&C has been an issue, and preliminary guidance on incorporating C&C aspects into HFE definition.

The definition task initially scopes out various HFE characteristics and allows individual HFE designations to be made within the context of the MCRA scenarios. These same characteristics, however, become the topics for further qualitative analysis, which can be done by assessing the HFE-specific aspects in greater detail, as discussed in Section 7 on timelines and Section 8 on PSFs.

Table 5-1 provides examples of the types of operator actions needed to respond to different MCRA scenarios, followed by the identification of the operator actions required for success and identification of potential HFEs. As seen in Table 5-1, actions that occur in several different scenarios, such as those taken to establish decay heat removal, can be modeled using the same HFE as long as the context, timing, and associated PSFs are similar or bounding.

Figure 5-1 shows an event tree that illustrates which actions apply to which MCRA scenarios. This event tree only shows operator actions and it is assumed that all hardware required for success is available. From Figure 5-1, the successes and failures can easily be identified. For example, if the operators fail to abandon the MCR (in time) then core damage will result irrespective of what happens next. Figure 5-1 shows there are 14 different end states. Within the 14 different end states, there are eight different operator actions identified. Following construction of this event tree, the analyst can then define HFEs to represent each scenario and, in many cases, the same HFE can be used in more than one scenario assuming that bounding success criteria is defined.

Table 5-1
Example of HFE identification for MCRA scenarios

Reason or Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
Loss of Habitability	**Scenario 1** Back panel fire with lots of smoke with no SSC damage (no fire-induced initiating event) Reactor trip occurs due to the decision to conduct manual shutdown as required by the decision to abandon.	Decide to abandon Electrically isolate the MCR and transfer control to the RSDP. Establish and maintain control of decay heat removal outside the MCR for PRA mission time. Establish containment isolation.	Decision to abandon is not modeled following a LOH	
			Operators fail to transfer control from MCR to RSDP	The action to transfer control to the RSDP would involve electrical isolation of the MCR. The electrical isolation could be performed from the MCR or at the RSDP depending on plant design.
			Operators fail to establish instrumentation at RSDP	Establishing instrumentation at the RSDP could be defined as a single HFE or it could be included as part of the success criteria for other HFEs. For example, most operator actions will require some instrumentation and by defining an HFE to establish instrumentation at the RSDP the dependency concerns among HFEs which share the same set of instrumentation can be explicitly addressed.
			Operator fails to start-up a feedwater pump, including restoration of support systems, and control feedwater for 24 hours	Long-term control actions should be considered following abandonment. Long-term control actions are typically considered to be negligible for fire scenarios which do not require abandonment.
			Operators fail to shut containment purge line	Containment isolation actions would impact LERF and the identified set of operator actions should include both CDF and LERF actions.

Table 5-1 (continued)
Example of HFE identification for MCRA scenarios

Reason or Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
	Scenario 2 Fire-induced LOCA due to open primary relief valve	Same actions as in Scenario 1 to transfer control outside of the MCR and establish decay heat removal; plus the following: Mitigate spuriously opened primary relief valve	Same actions as in Scenario 1	
			Operators fail to shut spuriously opened PORV or block valve	The HFE for failure to establish long-term decay heat removal would only be required if operators fail to close PORV or block valve.
			Operators fail to start and control Safety Injection (SI)	The HFE for failure to establish long-term decay heat removal would only be required if operators fail to close PORV or block valve.
			Operators fail to terminate SI after PORVs closed	
			Operators fail to establish long term decay heat removal	
	Scenario 3 Fire-induced SBO	Same actions as in Scenario 1 to transfer control outside of the MCR and establish decay heat removal; plus the following: Start and maintain EDGs for PRA mission time	Same actions as in Scenario 1	
			Operators fail to locally start EDGs or re-establish other source of electrical power	
			Operators fail to restore power to hydrogen ignitors	

Table 5-1 (continued)
Example of HFE identification for MCRA scenarios

Reason or Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
	Scenario 4 Fire-induced spurious SI	Same actions as in Scenario 1 to transfer control outside of the MCR and establish decay heat removal; plus the following: Terminate spurious safety injection	Same actions as in Scenario 1	
			Operators fail to terminate spurious SI	
			Operators fail to mitigate the LOCA given pressurizer (PZR) overfill	
Loss of Control	**Scenario 5** Fire with significant SSCs and instrumentation lost due to fire; automatic reactor trip.	Decide to abandon Electrically isolate the MCR and transfer control to the RSDP. Establish and maintain control of decay heat removal outside the MCR for PRA mission time. Impact of fire on instrumentation and control may affect the actions needed to start-up a feedwater pump, restore support systems, and control feedwater for 24 hours. Establish containment isolation	Decision to abandon is modeled following a LOC	
			Operators fail to transfer control from MCR to RSDP	The action to transfer control to the RSDP involves electrical isolation of the MCR. The electrical isolation could be performed from the MCR or at the RSDP depending on plant design.
			Operators fail to establish instrumentation at RSDP	Establishing instrumentation at the RSDP could be defined as a single HFE or it could be included as part of the success criteria for other HFEs. Most operator actions will require some instrumentation and by defining an HFE to establish instrumentation at the RSDP the dependency concerns among HFEs which share the same set of instrumentation can be explicitly addressed.
			Operators fail to start-up a feedwater pump, and control feedwater for 24 hours	Long-term control actions should be considered following abandonment. Long-term control actions are typically considered to be negligible for fire scenarios which do not require abandonment.

Table 5-1 (continued)
Example of HFE identification for MCRA scenarios

Reason or Abandonment	MCRA Scenario	Identification of Operator Actions	Examples of HFEs to be Defined	Additional Discussion
			Operators fail to shut containment purge line isolations	Containment isolation actions would impact LERF and the identified set of operator actions should include both CDF and LERF actions.
	Scenario 6 Fires that include: LOCA or SBO or Spurious SI	Same actions as in Scenario 5 to transfer control outside of the MCR and establish decay heat removal; plus the following: Start and maintain EDGs for PRA mission time.	Same actions as in Scenario 5 including modeling the decision to abandon	Decision to abandon is modeled following a LOC
			Operators fail to mitigate a LOCA	
			Operators fail to restore electrical power or EDG	
			Operator fails to terminate SI given instrumentation is impacted by the fire.	

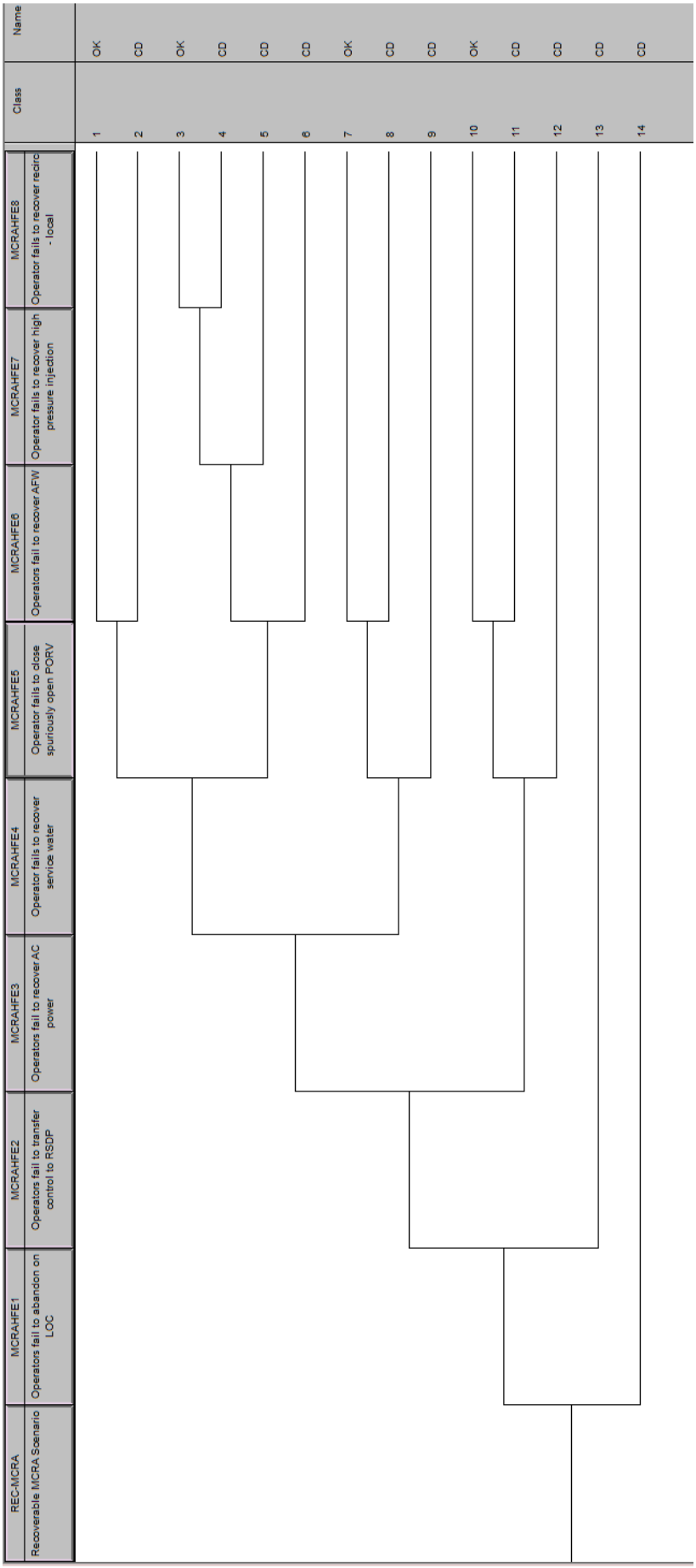


Figure 5-1
Sample event tree of MCRA operator actions

5.8 Examples of HFE Definitions

This section provides examples of HFE definition for three of the eight HFEs shown in Figure 5-1:

- MCRAHFE1: Operators fail to abandon MCR on LOC
- MCRAHFE2: Operators fail to transfer controls to RSDP after decision to abandon MCR
- MCRAHFE6: Operators fail to perform decay heat removal (DHR) function via motor-driven auxiliary feedwater (MD AFW) Pump 3 at RSDP (non-LOCA scenarios)

5.8.1 Example 1: Operators Fail to Abandon MCR on LOC (Basic Event ID MCRAHFE1)

Summary of HFE:
Fire scenarios in the MCR and cable spreading room (CSR) may involve damage to redundant trains of safe shutdown equipment.

The MCR will need to be abandoned due to LOC.

This HFE constitutes the cognitive (i.e., diagnosis and decision-making) error for failing to abandon in time to successfully shut the plant down from outside the MCR.

The consequence of failure of this action is core damage.

Cues and Indications:
Primary Cue: Alarm for fire in CSR

Additional Cues:
Pressurizer level unavailable from MCR
RCS temperature unavailable from MCR
Steam generator level unavailable from MCR
Fire suppression system initiated
Normal high-pressure injection (HPI) indications unavailable from MCR
Local verification of CSR fire by Nuclear Operator

Operators will get an indication of fire in the CSR; once operators in the MCR identify this alarm, they will send a nuclear operator to verify the presence of a fire in the CSR.

The senior reactor operator (SRO) communicated during interviews that indication parameters never fail as is; instrumentation would either fail erratic, high, or low. It would be very obvious to operators that instrument indications have failed. The procedure also has sufficient cautions that indications can become unreliable in fires, and the operators would clearly understand that conflicting and nonsensical indications cannot be trusted. This is considered equivalent to warning/alternates in a procedure. It was stated that this is also covered in training.

However, the cues in the abandonment procedure are not definitive (the Shift Supervisor still has to make a determination that the plant cannot be controlled from the MCR).

Procedures:
Cognitive: Fire Response-Cable Spreading Room
There are two possible entry conditions into the CSR fire procedure: automatic fixed suppression actuation or visual confirmation of CSR fire.

Step: 11
Instruction: ASSESS IF CONTROL ROOM EVACUATION REQUIRED
Normal Charging in-service and controlling pressurizer level between 20% and 60%
RCS Pressure stable or trending to 2235 psig
RCS Temperature trending to 547 °F
All vital 4KV buses energized
Steam Generator levels in at least two generators trending to 65% Narrow Range Level
Shift Supervisor determines plant control not available in the MCR

This action models cognition only. There are no execution sub-tasks required for success.

Assumptions:

High workload is assumed due to fire conditions.

Timing:

The operator must abandon the MCR within 25 minutes of the start of the fire.

It will take approximately 10 minutes from the start of the fire until the cues for the decision to abandon to appear in the MCR. Once cues for abandonment are present, it will take the shift supervisor approximately 1.5 minutes to make the decision to abandon.

Training:

MCRA scenarios are trained in the classroom once every two years at a minimum.

Manpower:

The shift supervisor is responsible for making the decision to abandon.

Communications:

While command and control is inside the MCR, face-to-face communication with 3-way communication is used. Once the shift supervisor has made the decision to abandon, he will hold a short crew brief to inform all control room operators what is going on. Then just prior to abandoning, a reactor operator (RO) will make an announcement that the MCR is being abandoned due to a fire.

Location:

This action takes place in the MCR.

5.8.2 Example 2: Operators Fail to Transfer Control to RSDP After Decision to Abandon MCR (Basic Event ID MCRAHFE2)

Summary of HFE:

This action is predicated on the operators successfully making the decision to abandon. This HFE addresses the actions operators take inside the MCR prior to leaving the MCR (e.g., tripping the reactor and RCPs, dispatching an operator to be stationed at the RSDP, and isolation of letdown) and the subsequent implementation of procedure steps to set up control from the RSDP.

The high-level tasks required for success of this action include:
1. Ensure reactor trip from inside the MCR
2. Close the MSIVs and bypass valves from inside the MCR
3. Trip all RCPs from inside the MCR
4. Transfer charging suction to the refueling water storage tank (RWST) from inside the MCR
5. Establish control at the RSDP. This involves turning three hand switches at the RSDP.

The consequence of failure of this action is core damage.

Cues and indications:

This action is predicated on the operators successfully making the decision to abandon (modeled as a separate HFE). Once the decision to abandon is made the operators will follow the MCRA procedure. Therefore, this action models execution and cognition is based on the decision to abandon.

Procedures:
Procedure OP 1 directs operators to commence procedure OP 2A upon the decision to abandon MCR. Operators need to implement Attachment 4 and Appendix F of OP 2A to set up for control from the RSDP.

OP 1,
Step 4. Ensure Reactor Trip
Step 5. CLOSE the MSIVs and Bypass Valves
Step 6. TRIP ALL RCPs
Step 8. TRANSFER Charging Suction to the RWST
OP 2A - Step 12. ESTABLISH Control from Remote Shutdown Panel

Timing:

Operators have 60 minutes from the start of the fire to avoid core damage by starting an MD AFW pump and/or a charging pump. It was estimated that operators will have 25 minutes from the start of the fire to determine if abandonment is required and the remaining 35 minutes are allotted to the execution portion of abandonment. The execution portion was estimated by using operator simulator data. An average of four minutes is conservatively used as the manipulation time for the in-MCR actions and an average of 3.25 minutes for the actions to establish control at the RSDP. This includes travel time. However, operator interviews indicated that operators have often delayed execution of actions because of increased stress due to the limited capabilities of the RSDP. Conservatively an estimate of 6.5 minutes is used for the actions to enable the RSDP, leading to an overall manipulation time of 10.5 minutes.

Training:

There is bi-annual training on the fire and MCRA procedures, which covers the topics in the OP 2A Lesson Guide and the System Training Guide for the RSDP. The simulator includes a real mock-up of the RSDP and it actually transfers control from the MCR. The simulator training staff interject realism into the simulations by saying how overloaded people are and sometimes telling the operators that someone is no longer available if they have been tasked with too much to do during the simulation. They also interject time delays to allow time for task performance.

Manpower:

The shift supervisor is responsible for making the decision to abandon and for giving the cue to the other operators to take the actions to enable the RSDP. The actions required in OP 1 will be performed by a single RO and peer checked just before leaving the MCR. Once at RSDP, the shift supervisor will designated a specific person responsible for manipulation of actions.

Location:

This action takes place in both the MCR and the RSDP.

The MCR is on the 140' level of the Aux Building. The stairs would take the operators down to the RSDP on the 100' level.

5.8.3 Example 3: Operators Fail to Perform DHR Function via AFW MD Pump 3 at RSDP (Non-LOCA Scenarios) (Basic Event ID MCRAHFE6)

Summary of HFE:
After transferring control to the RSDP, operators will follow procedure OP 2A and will realize the need to provide DHR to the RCS, then operators will start AFW.

The high-level tasks required for this action include
1. Diagnosing the need to start AFW.
2. At RSDP Take MAN-AUTO switch to MANUAL and start the AFW pumps and place AFW supply to manual for affected SG.

The consequence of failure of this action is core damage.

Cues and Indications:
Initial Cue:
AFW Flow (Low)

Additional Cues:
Steam Generator Level (RSDP indications: LI-201 through LI-204)

Procedures:
OP 2A, Step 20. CHECK AFW System Status
Step 20.a (RNO). Take MAN-AUTO switch to MANUAL and start the AFW Pumps
Step 20b. (RNO). Place AFW Supply to Manual for Affected SG

Timing:
Operators have 60 minutes from the start of the fire to avoid core damage by starting a MD AFW pump and/or a charging pump.
Decision to abandon is made at T= 25 minutes

Time to transfer control to the RSDP after the decision to abandon is 35.5 minutes from the start of the fire.

The cue for the AFW action is available at 4.5 minutes, based on the time it takes for operators to reach step 20 of procedure OP 2A from simulator exercises. The time operators take to monitor the parameters described in Step 20 (AFW pumps running) until they realize that they need to recover the secondary heat removal capabilities via AFW pumps is estimated at only 0.5 minutes since it is a very easy and straight forward step.

The time it will take once operators transfer control to the RSDP until they realize they need to start an AFW pump is estimated as 10 minutes, based on the allotted time operators have to complete the JPM.

Training:
There is bi-annual training on the fire and MCRA procedures, which covers the topics in the Lesson Guide and the System Training Guide for the RSDP. The simulator includes a mock-up of the RSDP and it actually transfers control from the MCR. The simulator training staff interject realism into the simulations by saying how overloaded people are and sometimes telling the operators that someone is no longer available if they have been tasked with too much to do during the simulation. They also interject time delays to allow time for task performance.

Manpower:
The shift supervisor is responsible for making the decision to abandon and for giving the cue to the other operators to take the actions to enable the RSDP.

Communications:
Once command and control is outside the MCR the communication protocol is to communicate via face-to-face, if possible. In some instances, local operators (not at the RSDP) will need to

communicate with operators at the RSDP and, in these situations, radios will be used. Prior to leaving the MCR each operator will pick up a pre-staged radio. For starting the AFW pumps at the RSDP, face-to-face communication is all that is required.

Location:
This action takes place at the RSDP.

5.9 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report,* U.S. Nuclear Regulatory Commission, Rockville, MD and the Electric Power Research Institute (EPRI), Palo Alto, CA: July 2012. NUREG-1921, EPRI 1023001.
2. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,* The American Society of Mechanical Engineers, New York, NY, February 2009.

6
FEASIBILITY ASSESSMENT FOR MCRA SCENARIOS

This section provides guidance for performing a feasibility assessment for MCRA scenarios and associated HFEs. Certain aspects of a feasibility assessment are also discussed in the following sections of this report:

- Section 3, Modeling MCRA Scenarios in Fire PRA
- Section 4, Analysis of the Decision to Abandon
- Section 5, Identification and Definition for MCRA Scenarios
- Section 7, Timing and Timelines for MCRA Scenarios
- Section 8, Performance Shaping Factors for MCRA Scenarios

6.1 Introduction

Section 4.3 of NUREG-1921 [1] discusses feasibility assessment in the broad context of operator actions during a fire at a NPP. Specifically, within the context of fire HRA, NUREG-1921 defines *feasibility assessment* as the qualitative determination of whether the operator action is go/no-go, considering the most influential PSFs. A review of NUREG-1921, especially Section 4.3, is recommended to better understand the considerations inherent in a feasibility assessment for fire HRA.

Additional guidance is provided in NUREG-1852 [2] on assessing the feasibility of local fire operator manual actions (OMAs)[27] performed outside the MCR to either: 1) protect critical safety equipment that might be failed, or might be spuriously affected, and rendered unavailable by the fire, or 2) locally and manually align critical safety equipment to perform its function when needed. NUREG-1852 defines a feasible OMA as one "that is analyzed and demonstrated as being able to be performed within an available time so as to avoid a defined undesirable outcome." It should be noted that NUREG-1852 combined feasibility criteria with reliability criteria such that if all the criteria are met the operator action would be highly reliable. However, NUREG-1852 does not provide a definition for "highly reliable." Therefore, in some cases, the feasibility criteria for the HRA, provided in this report or in NUREG-1921, may be less restrictive than what is specified in NUREG-1852, since the ultimate goal of the HRA is to quantify the reliability rather than simply make a distinction between deterministic concept of "highly reliable" versus "not highly reliable."

[27] Note that for plants transitioning to NFPA 805, there are special considerations for MCRA OMAs and their treatment as NFPA 805 recovery actions, as discussed in RG 1.205 [3], Section 2.4, Recovery Actions.

The basic purpose of a feasibility assessment per NUREG-1921 is unchanged for MCRA scenarios. Also, as discussed in NUREG-1921 and in Section 5 of this report, MCRA feasibility assessment will be an iterative process throughout the MCRA HRA. In other words, MCRA feasibility assessment is likely to be performed initially when operator actions and HFEs are first identified, then again as further information becomes available to the qualitative HRA (and later, during HRA quantification).

However, there are some important differences that are unique to MCRA feasibility assessment and are further discussed in this section. Namely,

1. Because an infeasible MCRA HFE or scenario may not be an acceptable final result for the HRA/PRA, the HRA analyst may be involved in identifying and defining what improvements could be made that would change the assessment to "feasible." In general, for internal events and fire HRA, the HRA scenarios are reliable and very few HRA resources are spent developing plant or procedure modifications to improving the reliability associated with operator actions. For some MCRA scenarios, the HRA analyst may spend considerable resources developing a modification to the existing strategy to ensure the scenario is feasible and reliable.
2. Feasibility assessments should be performed at the individual HFE and at the scenario level for MCRA scenarios
3. Criteria for MCRA feasibility assessments have been expanded to address additional factors that are important to the MCRA context. In addition, both these expanded criteria and the different context(s) for operator activities outside the MCR require additional information collection and assessment. (See Appendix C for more guidance on information collection.)

6.2 Feasibility Assessment – Scenario Level versus Human Failure Event

Feasibility assessments are usually performed at two points in the development of the PRA models. The feasibility of a scenario is assessed when first developing the accident sequence (event tree) models. Infeasible scenarios do not need to be considered further. An operator action feasibility assessment is performed once the accident sequences have been developed in the PRA model to determine whether specific operator actions can be considered for detailed assessment using HRA methods or should be not represented since they are infeasible.

6.2.1 Scenario Feasibility Assessment

In internal events PRA and most of fire PRA, scenario-level feasibility is typically performed in the accident sequence analysis task, and may not involve input from the HRA analyst.

However, for MCRA, the level of involvement by the HRA is different. As discussed in FAQ 13-0002 [4], “Main control room abandonment is a complex issue in that the PRA modeling consists of a wide range of scenarios and the plant response consists of a collective set of operator actions.” Consequently, a different approach is needed for scenario feasibility assessment. Namely, the HRA analyst will need to be involved in this assessment.

Section 3 provides guidance to define MCRA scenarios. Scenario feasibility assessment begins with the accident sequence development and ends with the HRA quantification of individual actions and is evaluated by demonstrating that the following criteria can be met:

- The plant design and shutdown strategy can mitigate the fire scenario. This includes review of the procedures to ensure that actions modeled in the fire PRA are included in the procedure guidance and systems and/or components are available with respect to the given scenario.
- There is sufficient time to complete the collective set of actions. This includes all actions required after the start of the fire.
- A walk-through or talk-through of the given scenario confirms that there is sufficient manpower available to support all required actions within the required time.
- Once outside the MCR, the plant has identified and defined a command and control structure and operators have been trained on their expected roles and responsibilities following MCRA.
- If communication is required once outside the MCR, then the plant has defined a communications strategy and has shown that any required hardware (e.g., radios or phones) will be available and not impacted by the fire.
- For LOC scenarios, the criteria for abandonment have been defined and the operating crew would be aware of the need to abandon for the given scenario.

Examples of MCRA scenarios that were determined to be infeasible include:

- Based on a review of procedural guidance and capabilities of the RSDP, it was determined for one plant that feed and bleed actions were not feasible from the RSDP. This action was not analyzed further and was not credited in the abandonment portion of the fire PRA model.
- At another plant, closure of MSIVs from the RSDP was not credited for MCRA. Even though these actions were included in the MCRA procedure, the operator actions were not developed because circuit analysis showed that MSIV control from the RSDP would be lost due to fire damage.
- For a LOC scenario at one plant, 11 SRVs could spuriously open at the same time as reactor trip and the start of the fire. With 11 SRVs opening at the same time, the operators only have 13 minutes to respond before core damage. Closing a single SRV (outside the MCR) was estimated to take approximately 15 minutes, and therefore the overall scenario was determined to be not feasible.
- An MCRA scenario is not feasible if circuit analysis cannot demonstrate availability of the remote shutdown transfer switches.

In summary, the HRA analyst uses information from the accident sequence analysis and the fire-induced failures leading to abandonment. Certain fire-induced failures may make certain scenarios infeasible. The MCRA HRA analyst then conducts the initial review of the MCRA and related procedures to identify functions that can or cannot be implemented at the RSDP.

Using this information, the HRA analyst then scopes out individual MCRA HFEs and subjects them to the feasibility criteria discussed in Section 6.4.

There are iterations that occur between the scenario feasibility and the individual HFE feasibility assessments. NUREG/CR-6850 [5] Task 11.b guidance suggests that timelines developed for MCRA scenarios should be evaluated for feasibility as follows:

> …accident sequence timing modeled in the plant model (i.e., fault trees and event trees) should be compared with the alternate shutdown procedure timeline. The comparison should ensure that the planned operator action times upon which alternate shutdown procedures are based will be less than the operator actuation or recovery times postulated for the applicable fire-induced accident sequences.

Within a given MCRA scenario, there may also be different configurations involving various combinations of credited or non-credited functions, which may, in turn, be subsequently developed as individual HFEs, as shown in Table 5-1. Scenario feasibility assessments on the basis of time cannot be calculated until the individual HFE timing is developed and the combination of actions is compared to the overall timeframe by which the actions must be accomplished. Sufficient time must be assessed at the scenario level (i.e., for the collective or entire set of actions), taking into consideration potential dependencies between actions (e.g., "hold points" where Operator A waits to complete his/her actions until Operator B's actions are complete, as reported by the shift supervisor). Examples of these timing evaluations are provided in Section 7.

6.2.2 HFE Feasibility Assessment

Once MCRA scenarios have been identified (these can be grouped or binned, depending upon the strategy of the analysis[28]), the HRA identifies the relevant operator actions for the scenarios using the MCRA procedures.

The evaluation of feasibility is then performed at the operator action level, generally associated with a HFE. A discussion of the MCRA feasibility criteria is provided in Section 6.4.

6.3 MCRA Scenarios – How to Deal with Infeasibility?

Similar to other fire scenarios, there may be MCRA scenarios and associated HFEs for which an assessment of "not feasible" is acceptable with respect to the fire PRA results. For example, the fire PRA for a specific NPP may not credit some LOC MCRA scenarios because the actions are not feasible from the RSDP based on detailed circuit analysis or fire modeling. There may also be instances when infeasible scenarios may have a significant impact on the overall fire PRA insights.

In such cases, the fire PRA team and operations staff, may be involved with identifying improvements in some of the following areas to ensure the scenario is feasible:

- Remove initial modeling conservatisms from the PRA scenario description. This could include:
  - Refinements to detailed fire modeling to better understand the fire impacts
  - Refinements to PRA model to credit additional systems/components, if required

[28] See Section 3.7 for guidance on grouping and binning MCRA scenarios.

  - Refinements/improvements to the thermal hydraulic analysis to show additional time is available
  - Review and confirmation of assumptions associated with the scenario/or action
  - Collection of additional information to support the timeline
  - Additional demonstrations (more than walk-through or talk-through) to show feasibility criteria can be met. A demonstration could also be used to collect or verify timing of key actions, which may have been based initially on analyst judgment
- Recommend procedure modifications, which could include:
  - Prioritization of key actions vs. those that are less critical from the PRA standpoint
  - Additional guidance on communication and command and control structure once outside the MCR
  - Revisions to ensure the procedure guidance is in alignment with the PRA scenario
  - New procedure guidance be developed for actions/scenarios not currently included in the procedures
- Recommend plant modifications be made to ensure action/scenarios are feasible, such as:
  - Protect or re-route cables for important components to ensure they are not impacted by the fire.
  - Improve HMI of the RSDP if actions are currently not feasible from an HMI standpoint - NUREG-0700 [6] provides guidance on human factors and ergonomic design for MCR operator response to reactor trips that can be used as a measure for creating an environment for highly reliable operator response.
  - Improve plant design such that the scenario can be mitigated (e.g., add additional back-up systems or automatic actuation features to the plant)

Being able to provide such feedback to the plant based on the PRA risk insights is one of the most important benefits of HRA/PRA. (Section 10 provides more discussion on examples of the kind of interface with the plant that fire HRA/PRA can provide.) However, there may be some aspects of the MCRA scenario/HFE context that are unalterable (e.g., time available for operator actions, accessibility of the action location, operability of relevant components and systems), making it unlikely that the scenario and/or action can be credited in the fire PRA.

The approach taken by the HRA/PRA team will be highly plant-specific and could be resource intensive, depending on the level of detail to ensure feasibility. Operations staff are likely to be the most useful resources in identifying workable improvements. However, there may be resistance to some improvements (e.g., modifying procedures). It may be necessary to demonstrate the source of the infeasibility to operations (e.g., discuss the timeline that indicates there is insufficient time to complete the tasks) to get their feedback and support for these changes.

6.4 MCRA Feasibility Assessment Criteria

The criteria presented in this section guide the analyst through the conditions likely to affect feasibility of an action. If the action is not feasible, an HEP of 1.0 is assigned, or the HFE is not credited in the fire PRA. For actions determined to be feasible, further qualitative assessment is performed as discussed in the timeline (Section 7) and PSF (Section 8) sections that provide input to the quantitative evaluation of the likelihood of success of the operator action.

Note that the feasibility assessment criteria align closely with the PSFs discussed further in Section 8 and may inform the PSF analysis, but the focus is different. The feasibility assessment uses the criteria to make a “go/no-go” evaluation of an HFE; this should not be substituted for the more in-depth analysis of the PSFs that is done once an action has been determined to be feasible.

Feasibility assessment criteria for MCRA are discussed in this section as follows:

1. Additional criteria specific to MCRA, and
2. Feasibility criteria from NUREG-1921 clarified to address the context of MCRA.

In addition, Section 4.3.4 discusses some feasibility considerations that are specific to modeling the decision to abandon.

6.4.1 Additional HFE Feasibility Assessment Criteria for MCRA Scenarios

For non-abandonment scenarios, the command and control structure is well established and communications inside the MCR are generally considered to be face-to-face, leading to a negligible PSF. However, based on review and understanding of MCRA scenarios, additional feasibility assessment criteria are needed to address: 1) changes that occur in the shift in location of command and control (discussed in detail in Appendix B) when the MCR is abandoned and 2) the fact that communications can become a significant PSF, and in some cases can prevent the success of the action. These issues are discussed further below.

6.4.1.1 Command and Control

Command and control is simply defined as "the exercise of authority and direction" [7], and more specifically, as the need for a central body of authority to make decisions but have them carried out by a distributed group. In the MCR, the shift supervisor, supported by the Shift Technical Advisor (STA) and shift manager, is the focal point for command and control. Following a reactor trip, the shift supervisor's direction in implementing the EOPs is the expected and principal display of command and control. The issue of command and control, for both inside the MCR and for MCRA, is discussed more extensively in Appendix B.

In contrast, depending on the RSDP capability and plant procedures, changes in command and control for MCRA with respect to the existing feasibility assessment factors inside the MCR may include:

- Staffing:
  - Fewer staff available to directly support command and control (e.g., STA and SM may have other duties and be assigned to different locations).
  - The SS (or whoever serves in the role of C&C) may need to direct, and possibly to coordinate, more staff than were needed in the MCR for the same shutdown activities.
- Cues:
  - Instrumentation supporting decision-making (performed by whoever serves in the C&C role) may not be available (e.g., no alarms at RSDP) or may only be available at a local panel.
- Procedures and Training:
  - Command and control structure may not be defined in emergency response plans or procedures.
  - Training for MCRA may not include specific command and control activities at the RSDP (e.g., communications/coordination with field operators) or specific delegation of field operator responsibilities.

Criteria: In order for an action or scenario to be feasible, there must be a pre-defined plan for command and control once outside the MCR. Additionally, operators should be aware of their expected roles following abandonment.

As a result of the above considerations, staff responsible for command and control are likely to experience a need for more and different communication (e.g., phone or radio, rather than mostly face-to-face). For this reason, "Sufficient Communications" has been added as a feasibility assessment criterion for MCRA and is discussed in Section 6.4.1.2.

6.4.1.2 Sufficient Communications

NUREG-1921 [1] did not consider communications as a separate feasibility criterion and instead addressed parts of it under ‘Sufficient Manpower’. However, given the importance of communication between multiple crew members across multiple locations for MCRA actions, it is called out as a separate factor. For MCRA scenarios, the likelihood that the crew is primarily reliant on two-way radios or other forms of distance communication (e.g., sound-powered phones) is greatly increased with the need to distribute crew around the plant both to perform local actions and to potentially monitor cues and parameters. Communications are required for relaying tasks and for ensuring sequential tasks or tasks requiring coordination are performed correctly. As NUREG-1852 [2] states, “therefore, effective communications equipment, to the extent it is needed, should be readily available and meet the functionality and accessibility criterion.” In addition, assessment of communications should include consideration of possible background noise and inter-unit communications using the same frequency (if a two-unit shutdown is required).

Criterion: Feasibility, in this case, means that the NPP has a clear communications plan in place and any equipment (e.g., radios, phone) required to implement the communication plan is available and not impacted by fire damage.

6.4.2 MCRA-Specific Issues in Existing Fire HRA Feasibility

This section summarizes the MCRA-specific differences in evaluating the feasibility assessment criteria given in NUREG-1921 [1].

6.4.2.1 Sufficient Time

Determining that sufficient time exists for diagnosing and completing a given action or a set of actions for a particular HFE is critical for assessing its feasibility. Section 7 on timeline development provides detailed guidance for assessing scenario and HFE timing for MCRA.

For MCRA, the time required to make the decision to abandon is particularly important and factors into the subsequent ex-MCR actions as well. In addition, extra time needed for communication between operators, or between operators and command and control, must be included in the time required to complete the action. This extra time should include consideration of the potential workload increase related to command and control.

Criterion: If the time required to perform all the task(s), taking into account any dependencies and/or coordination between actions, is greater than the time available (including time required to access necessary plant locations), then the MCRA scenario/HFE is infeasible.

6.4.2.2 Sufficient Staffing

The feasibility assessment for MCRA should consider whether there are sufficient personnel available to support the varied and dispersed actions. For a fire scenario, this becomes critical in the consideration of a sufficient number of trained personnel that will not be occupied with other duties such as serving on the fire brigade. For MCRA actions, the number of crew members required may be increased due to the significant number of local actions and ex-control room locations to be visited. Also, staffing for command and control should be addressed.

Once the decision to abandon has been made, all U.S. plants have procedure guidance to ensure that, for the design basis MCRA scenarios, there will be sufficient staff available to fight the fire and perform the required actions. However, there could be PRA scenarios that require more actions than the design basis scenarios and the availability of crew members must be verified to ensure there is sufficient manpower.

Criterion: Following MCRA, there should be sufficient staff available to support command and control at the RSDP and to perform all the required local plant actions. Crews should be able to demonstrate this during walk-throughs or simulator exercises that include simulation of local actions in order to validate that the crew can be positioned at all required plant locations to complete all the tasks in the various MCRA scenarios properly and in time.

6.4.2.3 Primary Cues Available/Sufficient

In general, this criterion for feasibility follows the same definition and concerns as identified in NUREG-1921 [1] and focuses on the assumption in HRA that all operator actions are taken in response to cues.[29] Following MCRA, the crew may be relying upon cues and indicators that are less obvious (e.g., alarms at the RSDP are not the same as in the MCR) than those presented in the MCR or less easily used (e.g., cues are only available on local panels). It will be even more important in these settings that sufficient cues be available for directing the operators' actions. First, the analyst needs to identify the cues necessary for diagnosing the required MCRA actions, then the analyst must determine whether the instruments supporting the necessary cues:

1. Are available to support the decision to abandon the MCR
2. Have been verified to be free from the fire effects to support post-abandonment actions

The fire PRA equipment (component) selection task is responsible for determining the availability and functionality of these cues, so the HRA analyst needs to provide inputs (e.g., list of instruments to be cable-traced) and obtain results from that task.

Examples of the types of cues that need to be evaluated for availability and functionality are:

- Fire alarm in the CSR, MCR, or other potential abandonment location
- Indications of:
  - Automatic fixed suppression initiated
  - Pressurizer level
  - RCS temperature
  - Vital 4 kV buses energized
  - Steam generator level
  - Normal charging

Criterion: If sufficient cues required for success of an action (or scenario) are unavailable then the action is considered to be not feasible. For those actions performed after abandonment has occurred, the cues necessary at the RSDP must be available at the RSDP or be available to locally stationed operators to allow credit for the action.

6.4.2.4 Proceduralized and Trained Actions

NUREG-1921 [1] discusses that the feasibility assessment should address the availability and applicability of procedure guidance. There are some MCRA scenarios for which the existing procedure guidance does not include the required actions. For such cases, if the procedure guidance is followed, the fire scenario will still result in core damage. Therefore, all actions required by the fire PRA should either be addressed by procedure guidance or be considered skill-of-the-craft actions in order for the action to be deemed feasible. The MCRA HRA analyst should note that procedure and training guidance could come from a variety of sources, such as:

[29] A cue may be instrumentation, a procedure step, or a plant condition.

- MCRA procedure
- AOP for Fire Response – Fire in CSR
- Instructor Lesson Guide on MCRA
- System Training Guide: RSDP

The coordination of actions required after MCRA can be complex due to coordination required among operators at various locations (see also Section 6.4.1.1 on Command and Control). The procedure guidance should account for this coordination and communication.

Criteria: There are two sets of MCRA criteria related to proceduralized and trained actions:

Criterion 1: Each of the following needs to be affirmative for the procedure and other trained actions to be considered feasible:

- Procedures exist for the MCRA scenarios identified by the PRA and include the actions needed for the MCRA scenarios.
- Training covers the procedure steps included in the MCRA scenarios and have been demonstrated to be viable through walk-throughs or observation of simulator exercises to account for coordination and communication.

Note that the feasibility assessment is based on whether the procedures and training are so deficient that the MCRA actions would not be able to be performed. Otherwise, the evaluation would be related to procedure and training PSFs as part of the qualitative analysis that evaluates action reliability.

Criterion 2: Other non-PRA actions incorporated in the procedures should not prevent the PRA-related actions from being completed in time. (Note that this criterion correlates to the timeline development discussed in Section 7.)

6.4.2.5 Accessible Location

The location(s) where the action(s) must be completed, the location of command and control, and any travel paths must be evaluated to determine feasibility of the action. If any of these locations are inaccessible, the operator action is considered infeasible. In addition, the travel path(s) of the operators should be reviewed to ensure that the defined access route is not blocked for any of the following reasons:

- **Smoke and toxic gas effects.**
- **Obstructions.** Including fire suppression efforts (e.g., such as from charged fire hoses).
- **Heat stress.**
- **Radiation.** For the feasibility analysis, the analyst needs to determine whether the radiation level or rating of an area would preclude access or otherwise prevent the action from being feasible. In addition, the analyst should consider any extra time that may be needed to prepare for entering such areas (e.g., the need to don personnel protective clothing).

- **Locked doors.** The fire may cause electric security systems to fail locked. In this case, the operators will need to obtain keys for access. If operators do not routinely carry the keys to access a secure area, the HRA analyst must ensure that there is enough time for the operators to obtain access. Normally locked doors should also be considered.
- **Lighting.** Analysis should determine that the lighting is adequate for the action area as well as the areas to be traversed.

Criterion: Each MCRA action location, including command and control actions, must be shown to be accessible through a detailed walk-through or talk-through that addresses: 1) reaching the location, and 2) remaining in place for the needed duration of the action(s).

6.4.2.6 Availability and Accessibility of Equipment and Tools

For the availability and acceptability of equipment and tools in a MCRA, the only difference beyond the guidance provided in NUREG-1921 [1] is that since the RSDP will (most likely) be where command and control is located, keys (and other equipment and tools, such as radios and flashlights) that are ordinarily the responsibility of MCR staff must be obtained during the abandonment and taken to the RSDP. In addition, HRA analysts must verify that the tools and equipment required for local MCRA actions will be available and functional when needed.

Criterion: The ability to gather necessary tools and equipment (including protective gear such as self-contained breathing apparatus (SCBA)), get them in place, and demonstrate their use should be shown in a detailed talk-through, walk down, or training exercise to be considered feasible within a MCRA scenario.

6.4.2.7 Operability of Relevant Components and Systems

A specific issue unique to fire is the potential disablement of the NRC IN 92-18 [8] motor-operated valves (MOVs). Spurious operation of these valves can cause their motors to be damaged and render them unable to be operated further. It is unlikely that controls for 92-18 valves will be located on the RSDP; however, local actions may be included in the plant fire or MCRA procedure to manually reclose them after a fire. The HRA analyst should ensure that local operator actions to manipulate such valves after a spurious operation are not credited.

Beyond what is already stated in NUREG-1921 [1], the key point for MCRA is confirming the availability and functionality of the required controls at the RSDP or at local control stations during MCRA scenarios. This requires input from the fire PRA and fire modeling tasks. In addition to instrumentation, the feasibility assessment factors could also include interlocks, automatic equipment starts, and automatic equipment trips that are normally available in the MCR, but are not available at the RSDP.

6.5 Example Feasibility Assessment

Table 6-1 provides an example of feasibility assessments for MCRA according to the feasibility criteria presented in Section 6.4. These are intended to illustrate to the analyst the thought process involved in performing the assessment. Summaries such as these provide useful documentation tools for feasibility assessment.

Table 6-1
Example MCRA scenario feasibility assessment summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
1	Command and Control	A central body of authority has been identified to make decisions for MCRA but have them carried out by a distributed group.	The MCRA procedure is organized with the main body of the procedure associated with Control Room Supervisor (CRS) actions to direct the evacuation process and the actions taken by the other operators through the use of separate attachments of the procedure. The CRS remains stationed at the RSDP and communicates and coordinates the actions of the following operators, each of which follows a specific procedure attachment: 1. Reactor operator 2. Balance of plant operator 3. Auxiliary building operator 4. Intermediate building operator 5. Electrical maintenance technician
2	Sufficient Communications	The communications system should be evaluated to determine the availability of communication, where required for coordination of actions.	As referenced in the administrative procedure, communications consist of pre-job briefs, three-way communication, and use of the phonetic alphabet during any communication having to do with the operation or manipulation of plant equipment. A new plant radio repeater system for use by plant operations, maintenance, and fire brigade personnel has been installed to meet emergency communications requirements. The existing plant paging system is considered as a back-up system.

Table 6-1 (continued)
Example MCRA scenario feasibility assessment summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
3	Sufficient Time	As stated in section 4.3.4.1 of NUREG-1921, "The fire HRA must evaluate whether a given action or set of actions for a particular HFE can be diagnosed and completed within the available time" and also that "an operator action is considered feasible if the time available to complete the action (after the cues for the action reach the operator) exceeds the time required." Sufficient time to travel to each action location and perform the action should exist, and the location of all actions should be considered when sequential actions are required.	Sufficient time was evaluated not only for the individual MCRA HFEs, but for the entire MCRA scenario (the combination of HFEs needed to bring the plant to a safe and stable condition). A MCRA scenario timeline was developed to ensure that all the individual HFE actions could be completed prior to the thermal-hydraulics evaluation of time to core damage. For the individual HFEs, the time windows were developed using the accident progression and fire response timelines. Review of the fire procedures and table-top discussions with operators were used to identify when the actions were expected to occur relative to the start of the fire. In addition, the most conservative times from the timed plant walkdowns conducted by plant operations were utilized to evaluate the feasibility of the execution times. Actions that were not essential to the PRA but took time away from the MCRA key functions were discussed with operations to move them to a lesser priority in the procedure, and walkdowns were performed again for verification. As a result, the MCRA scenario is considered to be feasible.
4	Sufficient Staffing	Walk-through of operations guidance (modified, as necessary, based on the analysis) should be conducted to determine if adequate resources are available to perform the actions within the time constraints (before an unrecoverable condition is reached), based on the minimum shift staffing. The use of essential personnel to perform actions should not interfere with any fire brigade or MCR duties.	The minimum staffing consists of 2 SROs (CRS and the shift supervisor), 2 ROs, an STA, and 5 non-licensed operators. Three of the five non-licensed operators are on the fire brigade. The five non-licensed operators consist of a control building operator, upper and lower auxiliary building operators, intermediate and turbine building operators. The shift manning sheet ensures that operators who have fire brigade duties are not responsible for emergency operator actions. The MCRA procedure is organized with the main body of the procedure associated with CRS actions to direct the evacuation process and the actions taken by the other operators and the electrical maintenance technician through the use of separate attachments of the procedure. The MCRA procedure has been evaluated through timed walkdowns to validate that the actions can be performed properly and within the time required with the staff assigned.

Table 6-1 (continued)
Example MCRA scenario feasibility assessment summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
5	Primary Cues Available/Sufficient	Consider availability of cues and indications essential to perform the action.	The operator actions credited after MCRA are either taken at the RSDP or locally. The indications at the remote locations are free from fire damage as determined from circuit analysis.
6	Operability of Relevant Components and Systems	Consider availability of systems and components essential to perform the action.	The availability of the systems and components are addressed by the fire PRA model. Relevant HEPs are assigned based on the characteristics of the scenario. For example, separate SBO-related HEPs were developed to address the unavailability of power, and the need to locally start the diesels and strip loads from the associated busses. The operability of the RSDP and remote action locations for the MCRA scenarios have been verified through circuit analysis and cable routing.

Table 6-1 (continued)
Example MCRA scenario feasibility assessment summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
7	Proceduralized and Trained Actions	Written procedures and training should be provided. The proposed actions should be verified in the field to ensure the action can be physically performed under the conditions expected during and after the fire event. Furthermore, periodic drills should be conducted that simulate the conditions to the extent practical (e.g., communications between the MCR and field actions, the use of SCBAs and, the appropriate use of operator aids).	The HRA team participated in an interview and a plant walkdown of the key steps of the MCRA procedure with a SRO to collect information on the MCRA strategy, procedures, and training. The MCRA procedure provides step-by-step instructions for the actions required to successfully avoid core damage by bringing the plant to a safe, stable condition. Operators receive licensed operator re-qualification training every 5 weeks. With administrative weeks (such as fire brigade training), this schedule provides operators with simulator training about 7 times/year. Subsequent to the site visit, the operations staff conducted several timed walkdowns of the procedure. The timing and insights obtained from the site visit walkdown and the operations walkdowns validated the feasibility of the actions and provided input to estimate operator action reliability. The MCRA procedure is part of a new set of safe shutdown procedures. The walkdowns by operations were used to optimize the procedure and insights from these walkdowns are being factored into the training process. Operators are commonly re-trained on fire procedures every two years. The walkdowns of the MCRA procedure simulated the communications, tools implementation, and SCBA use to the best extent possible. The walkdowns were timed to evaluate feasibility and efficacy of communications and use of operator aids and were used to optimize the procedure to ensure that operators could efficiently enact the procedure steps required. Going forward, the plant will conduct drills on this procedure as part of bi-annual training.

Table 6-1 (continued)
Example MCRA scenario feasibility assessment summary

	Feasibility Criterion	Criterion Description	Example of How the Feasibility Criteria can be Assessed
8	Accessible Location	The areas visited and any areas required to be traveled through should be shown to be tenable and the fire or fire suppressant damage should not prevent the action from being performed. Specific elements within the area (e.g., lighting level, locked doors, and radiation level) should be evaluated.	The MCRA procedure is implemented for fires that occur in fire areas that impact the MCR and CSR. MCRA scenarios were walked down by the PRA/HRA team to identify the travel path and identify any accessibility issues, which may be caused by the fire. Emergency lighting is controlled by a fire protection procedure, which currently requires monthly operational testing of each 8-hour emergency lighting unit and maintenance to verify that all lamps illuminate the appropriate equipment/target or means of access/egress. The walkdowns of the MCRA procedure evaluated the availability of adequate emergency lighting in the locations where the MCRA actions are performed. A plant modification will include relocation of lights in switchgear rooms to ensure the cubicles for the RCPs are illuminated. Impacted maintenance and test procedures will be updated based on identification of the required emergency lighting units and their mission duration. To perform all actions credited after abandonment, the expected travel routes do not included any locked doors or special access restrictions.
9	Availability and Accessibility of Equipment and Tools	Any tools, equipment, or keys required for the action should be available and accessible. This includes consideration of SCBA and personal protective equipment, if required. (This includes staged equipment for repairs).	A fire protection procedure provides the limiting condition for operations (LCOs)/actions/surveillances for fire protection-related emergency tools. An administrative procedure governs the tools and equipment utilized by the MCRA procedure. This procedure provides an example of the equipment that is contained in the RSDP emergency tool locker and is inventoried on a quarterly basis. The availability and accessibility of tools required for the actions, as cited in the MCRA procedure steps, were verified during the timed walkdowns performed by plant operations. The site walkdown also verified that the tools and equipment required for the MCRA actions were available per the fire protection and administrative procedures.

6.6 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.:2012. 1023001/NUREG-1921.
2. U.S. Nuclear Regulatory Commission. NUREG-1852*, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,* Washington, D.C. October 2007.
3. U.S. Nuclear Regulatory Commission. *Risk-Informed, Performance-Based Fire Protection For Existing Light-Water Nuclear Power Plants,* Washington, DC. December 2009. Regulatory Guide (RG) 1.205 Revision 1.
4. Nuclear Energy Institute, Fire PRA Frequently Asked Question (FAQ) 13-0002, “Modeling of Main Control Room (MCR) Abandonment on Loss of Habitability,” August 2013. Available through ADAMS Accession Number: ML13249A249.
5. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD: 2005. EPRI 1011989 and NUREG/CR-6850.
6. U.S. Nuclear Regulatory Commission. NUREG-0700 Revision 2*, Human-System Interface Design Review Guidelines,* Washington, D.C. May 2002*.*
7. Globalsecurity.org, Mission Command: Command and Control Army Forces. Last retrieved February 1st from: http://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm
8. Information Notice No. 92-18: Potential for Loss of Remote Shutdown Capability During a Control Room Fire, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC: February 28, 1992.

7
TIMING AND TIMELINES FOR MCRA SCENARIOS

7.1 Introduction

The purpose of this section is to describe the various timing considerations associated with MCRA. Some of these timing considerations are identical to that previously discussed in existing fire HRA guidance, NUREG-1921 [1], such as timelines for individual HFEs. Specifically, the concepts that the *Time Available* must exceed the *Time Required* and that the amount of exceedance impacts the reliability of the action are key parameters for many HRA methods and remain valid for MCRA. That being said, there are several differences, primarily additional considerations, which must also be taken into account in order to ensure that the MCRA actions are both feasible and reliable.

What is particularly unique and important for MCRA scenarios is: 1) there are likely to be multiple operator actions associated with restoring required functions, represented by unique timelines, and these may be performed simultaneously; and 2) it is important that the HRA analyst combine all of these timelines and other timing information in order to develop an integrated understanding of the overall MCRA scenario. Consequently, one of the important goals for MCRA HRA is a combined representation of the MCRA timeline(s).[30] Understanding the combined timeline as part of MCRA analysis is a concept introduced in NUREG/CR-6850 [2] Task 11.b; and has been expanded upon in this report.

The development of the combined MCRA timeline serves several purposes as listed below:

- First, the timeline helps the analyst collect and understand the plant response following fire ignition, specifically:
  - Fire growth and propagation as it develops from ignition to damage
  - Systems response following reactor trip, including component failure times (such as time to fire damage or time to battery depletion)
  - Operator response associated with the procedures needed to mitigate fire damage and to achieve safe shutdown
- Second, the timeline helps with the qualitative analysis by providing a means to check feasibility and providing insights on PSFs (such as the relationship between the time required and procedures, training, communications, and cues).

[30] The MCRA timing information is complex and may require several depictions to convey this information. For example, in this section, there are multiple, complementary depictions of the timing information presented. This collective set of information is referred to here as the combined MCRA timeline, although it is recognized that it may be several timelines taken together.

- Third, the timeline supports the quantitative analysis by providing a measure of the margin between the time required to complete MCRA actions and the time available to complete those actions.
- Additionally, dividing the timeline into time phases is a modeling tool to decompose the timeline into time periods governed by different cognitive aids such as procedures, plant information available, and availability of additional, supporting staff.

In summary, the MCRA timeline helps the HRA analyst understand the complex relationships between the fire progression, plant response, and the interactions among operators. By incorporating additional timing considerations into a single "picture," the HRA analyst develops a better understanding for the plant response, which also improves the qualitative analysis. In addition, the timeline can be used as a tool to better understand different cognitive aids such as procedures, available plant information, and availability of additional supporting staff. This understanding results in a better operational narrative, which ultimately supports communication with plant operations, procedure writers, and training as described in Section 10.

7.2 MCRA Timeline and Time Phases

The MCRA timeline requires integrating timing information from different sources to collect and identify the following timeline components:

- Fire progression
  - Time of fire damage
  - Time when LOH criteria is met
- Accident progression (event tree sequence)
  - Time of expected plant trip
- Procedure progression consisting of the expected operator response in transitioning through procedures (e.g., emergency procedures and/or fire response procedures) and executing the appropriate steps. This includes:
  - Time when LOC conditions are met
  - Time at which the decision to abandon is made
  - Time for actions performed just before leaving MCR
  - Time when operators leave MCR
  - Time for travel from MCR to RSDP
  - Time for operators to establish control at the RSDP
  - Time for RSDP actions (including local actions) to lead to a safe, stable conditions
  - Timing of key communications and coordination among actions

The MCRA timeline starts with fire ignition and detection by plant personnel. When collecting timing information, the raw timing data will be collected from various starting points and will then need to be adjusted such that all parameters are defined with respect to the start of the fire. For example, typically the thermal-hydraulic plant response timeline will define T=0 as reactor

trip, but the fire growth timeline will define T=0 as the start of the fire, and the operator response timeline sometimes starts once the decision has been made to take an action. The HRA MCRA timeline defines T=0 as the start of the fire and it is a reasonable PRA assumption given the severity of fires associated with MCRA that the reactor will trip at T=0. Any data collected for the development of the MCRA timeline many need to be adjusted to ensure T=0 is consistent.

Using the same reference point helps the analyst to capture the complexity and multiple interactions of the MCRA scenarios. To understand the collective set of operator actions required for MCRA, the timeline can be conceptualized as consisting of the three time phases shown in Figure 7-1:

- Phase I – Time period before the operators recognize that abandonment may be required
- Phase II – Time period associated with the decision to abandon
- Phase III – Time period after abandonment during which the transitional and post-abandonment shutdown actions are performed

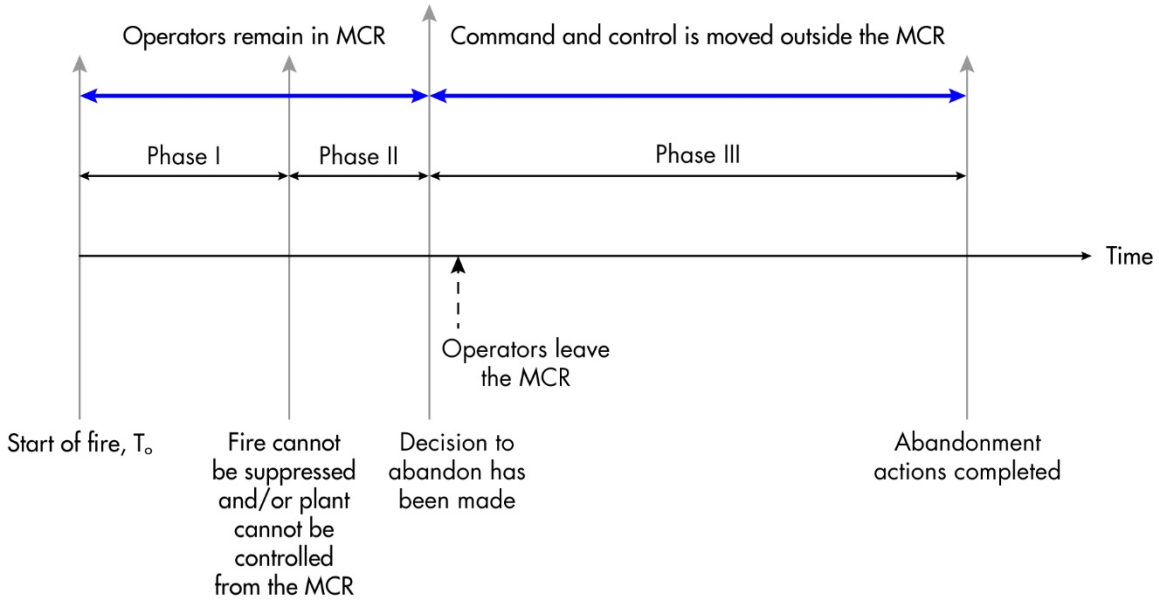


Figure 7-1
Three time phases of MCRA

Phase I is the time period before the operators recognize that abandonment may be required. This phase begins at the start of the fire and ends when the cue for the decision to abandon occurs.

In Phase I, command and control remains in the MCR and the operators will be interacting with the fire brigade and performing any necessary MCR actions, such as EOP and plant fire procedure actions.

Phase II is the time period associated with the decision to abandon. This phase starts when the operators receive the cue that abandonment is needed. The cues(s) for MCRA could be one or more of the following:

- The fire cannot be suppressed and the smoke levels are becoming life threatening,
- Operators begin to believe that the plant cannot be controlled from the MCR, or
- The MCRA procedure direct the operators to abandon.

Phase II ends when the decision to abandon has been made. This time period includes the three elements of cognition: detection, diagnosis, and decision-making. The detection of the fire should be obvious and will occur in Phase I. For LOC scenarios, the detection in Phase II is related to detecting fire damage and fire growth such that LOC can be diagnosed. Detection of fire damage may require local confirmation or operability of a system if its status cannot be determined in the MCR. For LOH scenarios, Phase II ends when the criteria for LOH is reached. (See Section 4.1 for more discussion on LOH scenarios and the decision to abandon.)

As discussed in Section 4, LOH in the MCR can result due to a fire in the MCR or due to a fire in a nearby compartment wherein smoke may enter the MCR rendering it uninhabitable. The decision to abandon the MCR is assumed to be forced due to untenable environmental conditions within the MCR. Therefore, the decision to abandon is always considered to be successful once the physical criteria are met (i.e., there is no HFE for the decision to abandon for LOH).

For LOC scenarios, the time required to diagnose and make the decision that a particular fire has impacted the MCR to the point of requiring abandonment could be complex, depending upon the level of guidance provided in the MCRA procedure. At many plants, specific cues for abandonment are not provided in the MCRA procedure and the simulator training often does not specifically cover the decision-making process, with trainers instead providing the cue to abandon to the crew being trained. This leads to significant uncertainty in the operators' ability to reliably make the decision to abandon in time to safely shutdown the plant. For this reason, the HRA analyst should work with the PRA team to identify the equipment and functional failures leading to MCR inoperability and recommend the inclusion of more specific abandonment cues based on these equipment/functional failures to the MCRA procedure. Detailed information on modeling the decision to abandon the MCR is provided in Section 4.

Phase III starts once the decision to abandon has been made. Most MCRA procedures contain specific actions that are required to be performed just before leaving the MCR. These actions could include reactor trip (if not automatic or already manually done), turbine trip, and isolation of critical MCR panels to allow control to be transferred to the RSDP. The time it takes to perform these actions should be incorporated into the overall operator response timeline and are considered to be in Phase III.

Once command and control moves outside the MCR, the plant response typically consists of the following sub-parts:

- Actions required for completing the transfer of control to the RSDP, alternate shutdown panel, or local control stations (depending upon the plant-specific MCRA set-up)
- Local actions to implement systems and functions required for safe shutdown
- Long-term control of plant parameters

Phase III should consider the time it would take to travel from the MCR to the RSDP. This time can range from less than a minute to greater than 5 minutes depending upon the plant layout. Once at the RSDP, it is not uncommon for the SS or SRO[31] to review the next steps of the MCRA procedure with the crew before delegating procedure steps to them, often organized into specific procedure attachments. Then, the main objective is to establish control of the plant at the RSDP so that it can serve as the new command and control center to which the other operators report the status of their local actions. The operations team then takes actions to implement systems and functions, which may include time-critical actions, to bring the plant to a safe, stable condition.

Phase III ends once the plant reaches a safe, stable state. This includes starting the required systems, and maintaining long-term control of the plant. The timeline should include any long-term actions required to maintain the safe, stable plant condition (i.e. actions to refill CST or EDG fuel oil tank).

It is important to note, that the three timeline phases are used to designate where command and control will be located. If necessary, the SS can send crew members locally to start a system before the decision to abandon has been made. In this case, there would need to be procedure guidance or control room indications to direct such actions.

7.3 Timing Sources Used as Input to MCRA Timeline

The MCRA timeline combines several individual timelines based on different information sources. This section identifies the different sources of information to be reviewed and incorporated as appropriate into the MCRA timeline.

7.3.1 Fire Progression Timeline

The fire progression timeline consists of fire ignition, growth, propagation, detection, suppression, and the time to component damage. The fire growth and suppression times are typically a function of the heat release rate, physical layout and arrangement, and control room heating, ventilation, and air conditioning (HVAC) system line-up.

The fire progression timeline is used to develop inputs for both Phase I and Phase II of the MCRA timeline and provides the following key times within the MCRA timeline:

- **Time the fire starts.** In the MCRA timeline, this is defined as T=0.
- **Time the fire is detected.** In many cases this may be T=0. However, in other cases, it could take several minutes for smoke or component failures to develop.
- **Time of the cue(s).** The fire may provide a direct cue. For example, fire in Cabinet X leads to specific section of fire procedure. Additionally, the fire may indirectly provide a cue via fire-damage to an SSC, such as when the fire fails an electrical bus causing reactor trip.
- **Time at which fire suppression starts** (to the extent that it is required to ensure realism in the dominant MCRA scenarios). Manual suppression is not addressed by the fire HRA;

[31] SRO is used here as an example of the person leading command and control after the decision to abandon has been made. Each plant will specify a person assigned to this role. It could be the SRO, RO, STA, CRS, shift manager, or shift supervisor. SRO has been used here as an example title.

instead, it is addressed in the fire modeling task. Even when plant staff are used as part of the fire brigade (or until the fire brigade arrives), the staffing for MCRA has usually been specified such that sufficient personnel are available for safe shutdown actions. However, this should be verified by reviewing the plant fire procedures and discussions during operator interviews.

- **Time at which LOH criteria are met.** This time is based on when the smoke levels become life threatening and is primarily a function of fire damage, but it could also be a function of the operability of the MCR HVAC system and associated system alignment. For LOH scenarios, zone or computational fluid dynamics software can be used to determine the time at which the smoke levels becomes life threatening.
- **Time at which fire is extinguished.**
- **Time of component damage.** In some cases, detailed fire modeling may be able to provide the times at which key components are impacted by the fire. However, in most MCRA scenarios the time to component damage is modeled conservatively such as “all components failed at the start of the fire.” The expected operator response is highly dependent on when components are impacted. If all components are assumed failed at T=0 then the operator response should reflect this assumption.
  - In some scenarios, a system may successfully start and run for a defined amount of time. This may provide additional time to core damage. If these times are known, they can be used in the MCRA timeline to provide a best estimate timeline. For example, if AFW successfully starts following reactor trip, then runs until the operators have removed power to the components, then the time to core damage would be longer than if AFW fails to start following the reactor trip.

In general, the fire progression timeline requires inputs from detailed fire modeling. The more detailed fire modeling information is available, the less uncertainty there will be related to the timeline development.

7.3.2 Accident Progression Timeline

The accident progression timeline represents the thermal-hydraulic modeling relevant to the event tree sequence. As such, this timeline consists of the progression from the initiating event, through success or failure of systems and actions modeled in response to the initiating event, to the point of core damage or a safe, stable end state. The progression includes the PRA success criteria for systems, components, and operator actions. The accident progression includes the following timing information:

- Time of reactor trip
- Time of cues (T_{delay}) for individual actions
- Times for successful operator actions (if applicable)
- Times that component failures are modeled as occurring (if applicable)
- System time window (T_{sw}) for individual actions as well as for the overall MCRA scenario; see Section 7.4.2 for additional discussion.

The accident progression timeline links to the fire progression timeline through the component failure timing and the time of reactor trip. In most MCRA scenarios, the fire starts and all components affected by the fire are assumed to be failed at the same time.

It is important to identify the time of reactor trip with respect to the start of the fire because most thermal-hydraulic data collected to support the system time windows consider T=0 as reactor trip. If the fire damage causes reactor trip, then the “clock starts” for many operator actions at T=0. However, if the reactor trip is delayed, then the “clock starts” for the operator actions later in the scenario when the reactor trip occurs.

For many MCRA scenarios, the severity of the fire and loss of functionality of the MCR and significant systems and functions would be expected to lead to fire-induced reactor trip shortly into the scenario, if not immediately, and is therefore taken to occur at T=0. The accident progression can define the time available for an HFE (see Section 7.4). In many cases, the time available will start only when a SSC is impacted by the fire. In this case, the system time window will need to include the time at which the SSC is failed (with respect to the start of the fire) and the time available for the action. For example, an action to restore power to a DC bus by locally re-aligning the power supply could have success criteria based on battery depletion time. However, the time to battery depletion only starts when the batteries are demanded. This may or may not be the start of the fire, or may start once the operators remove power from the MCR just before abandoning. Regardless of method or reason, the starting point for the use of batteries is likely shifted in time from T=0. In addition to potential shifts such as these, the system time window may be longer depending on the system or function implemented, such as long-term control actions.

The accident progression timeline produces timing information related to cues that are a function of parameters being monitored by instruments (e.g., RCS pressure, temperature, and SG level). The accident progression timeline generally starts with the success criteria from the internal events PRA and uses additional thermal-hydraulic cases developed for the fire PRA. The accident progression timeline is usually linked to the other timing sources at the time of reactor trip.

7.3.3 Phase II Timing Associated with the Decision to Abandon

For LOH scenarios, the timing associated with the decision to abandon is very short since the decision to abandon should be obvious given the environmental conditions in the MCR. However, as with any operator action, the decision to abandon could take up to one minute after the cue is received and this period should be included in the timeline.

For LOC scenarios, the time required to make the decision to abandon could take several minutes since the conditions inside the MCR will not be life threatening. For LOC, the decision to abandon will be based on procedure cues, training, and is typically at the discretion of the SRO in charge of the operating crew. For most U.S. NPPs, the criteria for abandonment are typically not clearly defined and are often ambiguous. Section 4 provides additional guidance on the decision to abandon for LOC scenarios.

7.3.3.1 Phase II Timing Parameters

In Phase II of the MCRA timeline, there are four timing parameters, which should be identified, including:

1. Time at which the abandonment criteria are met relative to the start of the fire,
2. Time required for the Shift Supervisor (or Shift Manager) to make the decision to abandon,
3. Time available for the decision to abandon, and
4. Time margin for the decision to abandon.

For LOH scenarios, the time at which the habitability criteria for abandonment are met will be based on the fire progression timeline. For modeling purposes, the timing associated with Phase II for LOH scenarios is typically defined as a point estimate. However, it would be good practice to recognize that there could be a range of times, depending on the scenario. In contrast, for LOC scenarios, the cue for the decision to abandon will be based on procedure guidance, discussions with operators/plant personnel, and, in some cases, engineering judgment. For LOC scenarios, the Phase II time should be reflected as a range.

The time available for the decision to abandon is defined by the HRA analyst by: 1) identifying how long it will take to perform all actions following abandonment (both cognition and execution of each action need to be considered), and 2) working backwards to determine the latest time at which the operators must leave the MCR. (Phase III timing will therefore need to be developed before Phase II timing.)

The time required for making the decision to abandon is the expected time it will take the MCR crew to make the decision, which could range from one minute to several minutes depending on the clarity of the guidance in the procedures and whether it is covered in training. For LOH scenarios, the time required will be very short and in many cases less than one minute. For LOC scenarios, the time required could be up to several minutes because of the need to obtain confirmation of the severity of an ex-MCR fire or of the status of systems or equipment.

The time margin[32] for the decision to abandon is the difference between the time required to make the decision and the time available. The time margin must be greater than or equal to zero in order for the MCRA scenario to be feasible.

7.3.3.2 Example Approach for Phase II Decision to Abandon Time Estimation for LOC Scenarios

In most cases, the timing associated with the decision to abandon for LOC scenarios will be determined by engineering judgment. One approach to determining these timing parameters is described here.

[32] Time margin can be expressed as a *percentage*, which is the approach used in the Fire HRA Scoping method in NUREG-1921 [1]. However, a time margin expressed as a *percentage* can be a poor metric for very short time frame and very long time frame actions. Instead, time margin, here is defined as the difference between time available and time required. Consistent with the definition of time margin in [1], this metric is intended to convey the excess time available that could offset variability and uncertainty in the time estimates.

The time available (not the time required) for the decision to abandon will overlap into Phase III. (See Figure 7-2; note that the timeline is not drawn to scale.) By definition, Phase II ends when the decision to abandon is made. The time available for the decision to abandon is defined as the longest time in which the operators can remain in the MCR and still prevent the undesired end state. Therefore, the maximum time available for the decision to abandon can be defined mathematically to be:

$$\textit{Maximum time available for decision to abandon} = T_{SW} - T_{Delay} - T_{Req,III}$$

Where;

T_{SW} = System time window for the overall MCRA strategy. The system time window is defined from T=0 until the time when the MCRA strategy can no longer be successful.

T_{Delay} = Time at which MCRA criteria are met

$T_{Req,III}$ = Time required for Phase III

The timing parameters associated with Phase II are shown in blue in Figure 7-2 and the timing parameters associated with Phase III are shown in red.

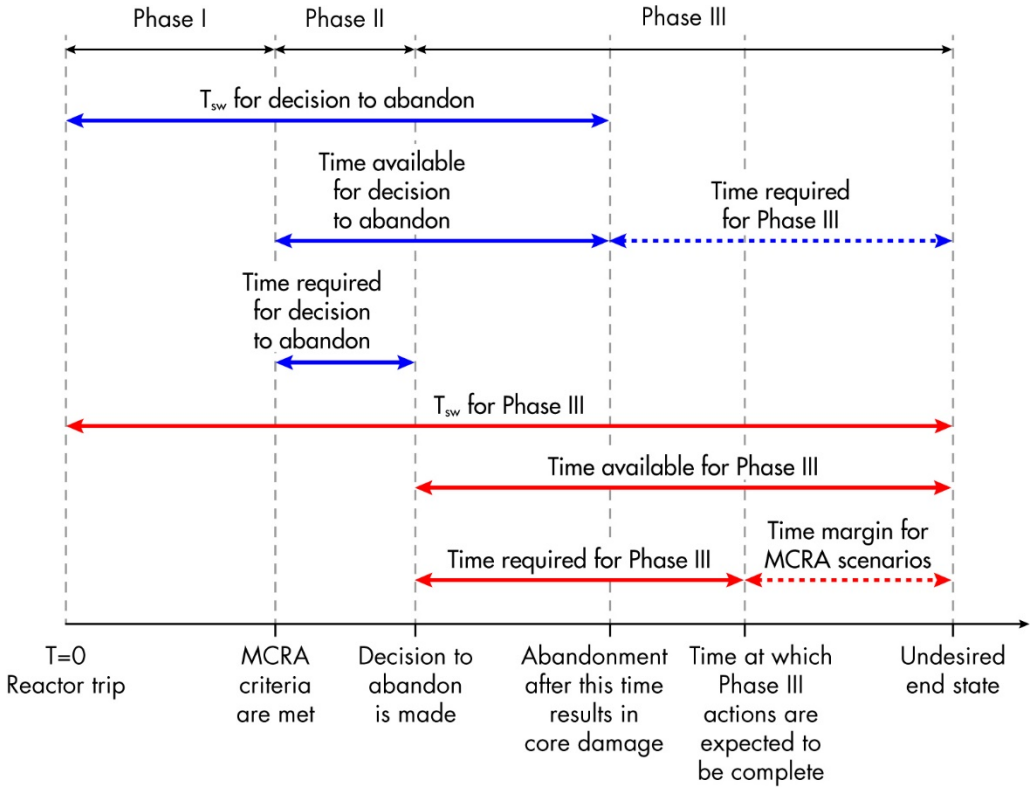


Figure 7-2
Overlap between phase II and phase III timing for LOC scenarios

Figure 7-2 includes a red dotted line for the time margin for the MCRA scenario. This extra time is for both the decision to abandon as well as Phase III actions.

From a practical standpoint, the analyst would want to define both a time margin for Phase II and for Phase III. Therefore, the HRA analyst will need to split the time margin shown in Figure 7-2 into two time margins shown in Figure 7-3 (note, figure not drawn to scale). The total time margin for Phase II and Phase III is shown in green on Figure 7-3.

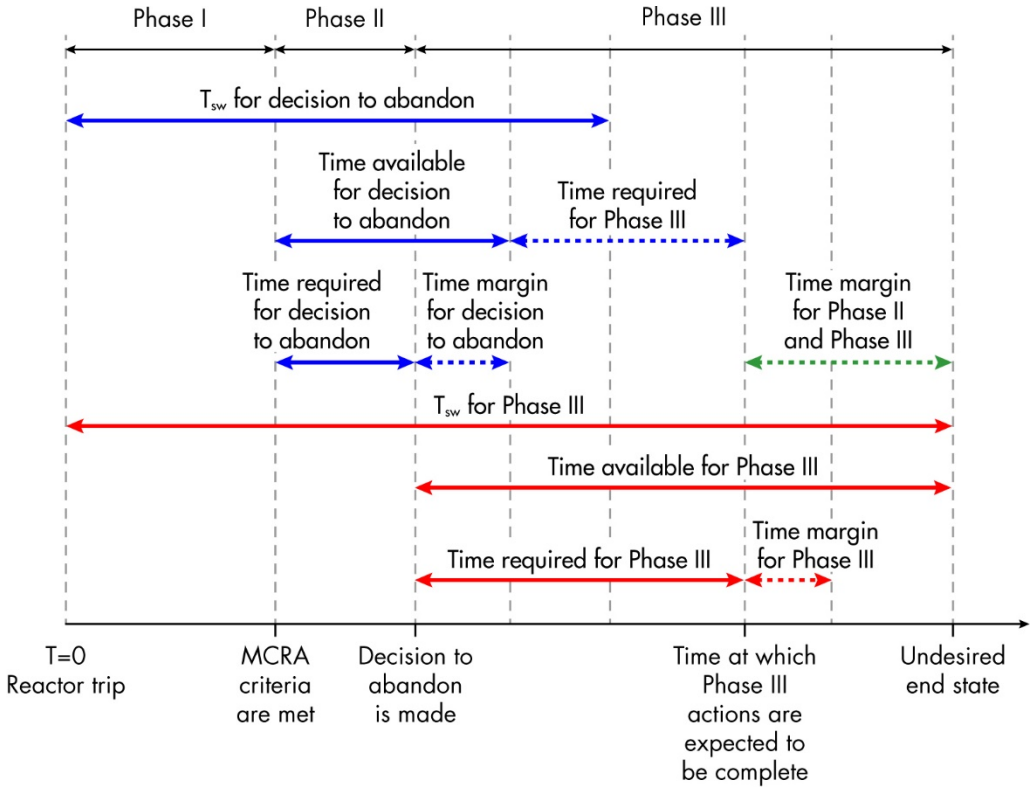


Figure 7-3
Split between time available for phase III actions and time available for decision to abandon for LOC scenarios

For the purposes of the MCRA HRA, the timing parameters associated with the decision to abandon should be identified as best-estimate point estimates because many of the actions required after abandonment are predicated on the time at which abandonment occurs. In reality, it is recognized that there is significant uncertainty associated with each timing input related to the decision to abandon.

When determining the timing associated with the decision to abandon, the margin for the decision to abandon must be greater than or equal to zero in order to show that the MCRA scenario is feasible. Section 9 provides additional discussion on this uncertainty.

After the initial best estimate timing parameters are developed, the analyst can consider performing sensitivity studies to determine the impact of the uncertainty associated with the decision to abandon. One way to assess the sensitivity of the uncertainty in the timing values is to conduct a trial increase in the time parameters to see how much the HEP is impacted. It may be prudent to utilize a conservative value initially to determine the impact on the overall results. If the conservative HEP is not acceptable, then the HRA analyst can assess what would be needed qualitatively to improve the time estimate (e.g., clearer entry criteria, better training, etc.).

7.3.4 Procedure Progression Timeline (Operator Response)

The timing sources described above primarily define the time available for operator response and provide additional information such as when key cues and plant parameters occur during the response. This section focuses on the time required for response.

As described in NUREG-1921, the time required for response consists of the time for cognition and the time for execution ($T_{cog} + T_{exe}$). The time required for response depends on what procedures are being used, including the time to transition through different procedures, as well as the time needed to implement the procedures.

For all phases, the procedure progression timeline is typically constructed by the HRA analyst with input from the plant operations staff. Operational input is essential in order that the plant response times reflect the “as-operated” plant (or “as-to be operated” plant when crediting upcoming changes to the plant procedures). Input is collected from the operators based on the talk-through/walk-through guidance in Appendix C. As part of this discussion, the HRA analyst should review the timing of the fire and hardware failures with plant operations in order to understand the context and development of timing for both Phase II and Phase III.

During Phase I, typically, the plant EOPs/AOPs remain in effect and are used in conjunction with the plant's fire procedure. The modeling of the time required for response follows the same considerations as described in NUREG-1921. During Phase I, the fire-induced initiating event and the associated reactor trip are affected by the fire growth timeline (Section 7.3.1) and accident progression timeline (Section 7.3.2).

During Phase II (i.e., the decision to abandon), the operators are typically following EOPs and/or AOPs and fire procedures, and accessing the MCRA procedure to decide whether MCRA is warranted. For Phase II, the time at which abandonment occurs should be based upon the specific criteria the crew will use for making the decision to abandon, as discussed in Section 4 and Section 7.3.3.

During Phase III, most MCRA procedures include several actions that are performed just before leaving the MCR. These actions typically can be accomplished quickly and include reactor trip (if not already done), turbine trip, and isolation of critical MCR panels as a first step to transferring control to the RSDP. The time it takes to perform these actions should be incorporated into the overall operator response timeline. When conducting these steps, the actions are typically accomplished independently without the need for communications, coordination, or command and control.

Later, during Phase III the operators may be using only the MCRA procedure or may still be using EOPs/AOPs and the plant fire procedure. Which procedures would be used is a question that should be asked during operator interviews. The evaluation of the Phase III portion of the MCRA timeline requires a combination of both talk-throughs and walk-throughs of the MCRA procedures with knowledgeable plant staff since the control room simulator has limited use for evaluating actions outside of the MCR. If the plant has a simulator for the RSDP this can be useful for determining the time to complete actions at the RSDP, but actions performed away from the RSDP will need to be based on walk-throughs and talk-throughs and should cover the time it takes to perform each action individually as well as the collective set of actions.

The MCRA procedure may contain steps that are not considered essential by the PRA, but are done to facilitate the ability of the operators to restart the plant at a later time. These steps, however, can take time and attention away from the critical actions and could compromise the ability of the operators to complete the PRA-relevant steps in time to bring the plant to a safe condition. Conducting timed walkthroughs can identify the time constraints on the MCRA strategy and can help demonstrate to operations and training the importance of focusing on the PRA-relevant steps of the procedure. The HRA analyst can then recommend moving the non-essential steps to a later point in the procedure after the critical steps are completed.

The MCRA procedure needs to be evaluated not only in terms of individual actions, but as a collective set of actions to ensure that the entire set of actions can be completed in time to avoid core damage. Each plant has a unique MCRA strategy and procedure. Some plants rely heavily on the shift supervisor directing each action one-at-a-time with confirmation that each step has been completed before proceeding to the next step. Conversely, other plants provide each operator with a stand-alone attachment to complete a series of steps. Each operator is expected to work relativity independently and then report back following completion of their attachment. The timeline of the Phase III portion can be highly complex and requires the analyst to understand the expected procedure response. The timing should include any time for communication among operators in multiple locations as well as account for time delays due to feedback required by or from other operators before subsequent procedure steps can be taken.

The MCRA timeline ends once a safe, stable plant condition has been reached. Operators will need to maintain long-term control of the plant, typically involving the use of the decay heat removal and injection systems. This includes maintaining inventory of tanks or systems, which may need to be refilled at some point during execution of the strategy. The duration of such long-term control actions is the mission time of the function or system being modeled and should be included in the fire PRA as actions required for success. In contrast, for internal events HRA, the time available generally considers the time at which the system must first be started, and actions for long-term control are often not required or are considered negligible. For MCRA, the long-term control portion may no longer be negligible contributors to the overall failure probability. The operator(s) may need to control the system multiple times in order to remain in a safe and stable condition. When modeling these steps, the actions typically require some level of communications, coordination, and/or command and control and the time required to accomplish these actions must be addressed.

The timing considerations and sources of data in Section 4.6.2 of NUREG-1921 [1] apply to MCRA; specifically, the following sources of information may be useful in determining the time required to complete each action:

- **JPMs.** Many plants have a specific JPM for each MCRA action. The JPM can provide a reasonable estimate for the time it takes to perform an action. However, the HRA analyst should review what is and is not included in the time required to perform this action. Often times the coordination between operators is simulated via a phone call and not actually walked down as part of the training. Additionally, the JPM training may use a different starting point than the fire PRA. For example, T=0 for the JPM may start once the operator is already in the field whereas for MCRA T=0 is the start of the fire.

- **Training exercises.** Times recorded during simulator exercises can help estimate the overall time the MCRA strategy takes or time points for when key actions need to be started and completed.
- **Appendix R feasibility demonstrations.** As cited in NUREG-1852 [3], Section III.I.2 of Appendix R states the following:

  > Practice sessions shall be held for each shift [crew] to provide them with experience in [performing the operator manual actions] under strenuous conditions encountered [during the fire]. These practice sessions should be provided at least once per year for each [operating crew] ... [and] performed in the plant so that the [crew] can practice as a team.

- **Information from the assessment of a similar action.** Examples of characteristics for similar actions are:
  - The actions themselves are similar
  - The timing related to when the actions have to be performed and how long it would take to implement the actions is similar
  - Locations of the actions are not so different that travel time to the locations is not significantly affected
  - Similar environments exist for the locations of the actions

Timing information from the assessment of similar actions can be used as a bounding case when it is clear that the actions being evaluated would not require more time than the similar action.

Evaluation of time required (T_{cog} + T_{exe}) to complete the actions should consider both cognition and execution. The cognition time includes diagnosis, detection and decision-making, and the execution time includes time to travel to each action location, as well as the time necessary for performing the action, including communications if necessary. This may be complicated if multiple locations are visited in the course of sequential actions, in which case, the various action locations need to be considered. This is especially important for post-MCRA actions when a large number of actions will be performed in distributed locations.

The evaluation of the time required (T_{cog} + T_{exe}) should include the time required for coordination and communication. Once outside the MCR, each plant has a unique communications strategy (or strategies). Consideration of the command and control structure at the plant should be made as part of the communication and operator dynamics assessment. (See Section 8 on PSFs and Appendix B on Command and Control for further discussion.) The HRA analyst should identify the times at which key communications would be required between the RSDP (or wherever C&C is located) and local stations.

For example, starting a pump may require one operator to start the pump locally and a different operator to control the pump flow at a different location. Starting and controlling the pump could require one operator to start the pump and then communication with the operator located at the RSDP to determine the flow rate. The flow rate indicators may or may not be available at the pump. The time at which this communication occurs is dependent on how long it takes the operator to travel to and start the pump.

Both Section 4.3.4 of NUREG-1921 [1] and Section 4.2.2 of NUREG-1852 [3] mention equipment access, environmental conditions, and expected variability between individuals and crews as potential contributors to timing uncertainty. It is therefore important that the analyst recognize the potential for uncertainty in the time estimates and be vigilant for cases in which a small change in the estimation of the time required could change the operator action from feasible to infeasible. See Section 6 for additional discussions on the feasibility assessment.

7.4 Individual HFE Timelines

Section 7.3 described the evaluation of the overall MCRA timing and the different timing sources available to the HRA analyst. This section discusses the evaluation of timelines for the individual HFEs modeled to represent the operator actions to implement the systems and functions for the MCRA scenarios. In addition to the overall MCRA timeline, an individual timeline should be developed for each HFE. The HRA analyst should work together with operations staff to identify the time required to perform each action individually and their timing relationships as part of the definition for each HFE. The time required must include the transit time as well as the time required for coordination and communication. If the action involves the longer-term control of plant parameters, then a mission time is also needed. All of these elements of time should use the same time reference point (usually T_0). The combination of all the actions within the definition of an HFE are necessary to estimate the overall time required for the abandonment actions to be complete.

In addition to the time required, the MCRA HRA evaluates the time available for response using the considerations provided in Section 7.3. Once the individual HFE timeline is constructed, it is used for feasibility assessment and quantification.

The individual timeline for each action should be defined following the basic guidance and timing concepts in NUREG-1921, which is repeated below for completeness, but with specific MCRA examples added. During Phase I (before the decision to abandon), this modeling is the same as in NUREG-1921. There are seven timing parameters defined in NUREG-1921 including; T_0, T_{SW}, T_{delay}, T_{cog}, T_{exe}, T_{avail}, and T_{reqd}, associated with each HFE, and their relevance is discussed in the following subsections. If applicable, the subsections have been annotated to provide a reference back to the timing considerations presented in previous sections. For MCRA, the timing relationships between actions are important. For each action, a T_{SW}, T_{delay}, T_{cog}, and T_{exe} must be defined. Each of these parameters must be defined with respect to the same time origin and, in many cases, these parameters are dependent on timing parameters associated with other HFEs in the scenario.

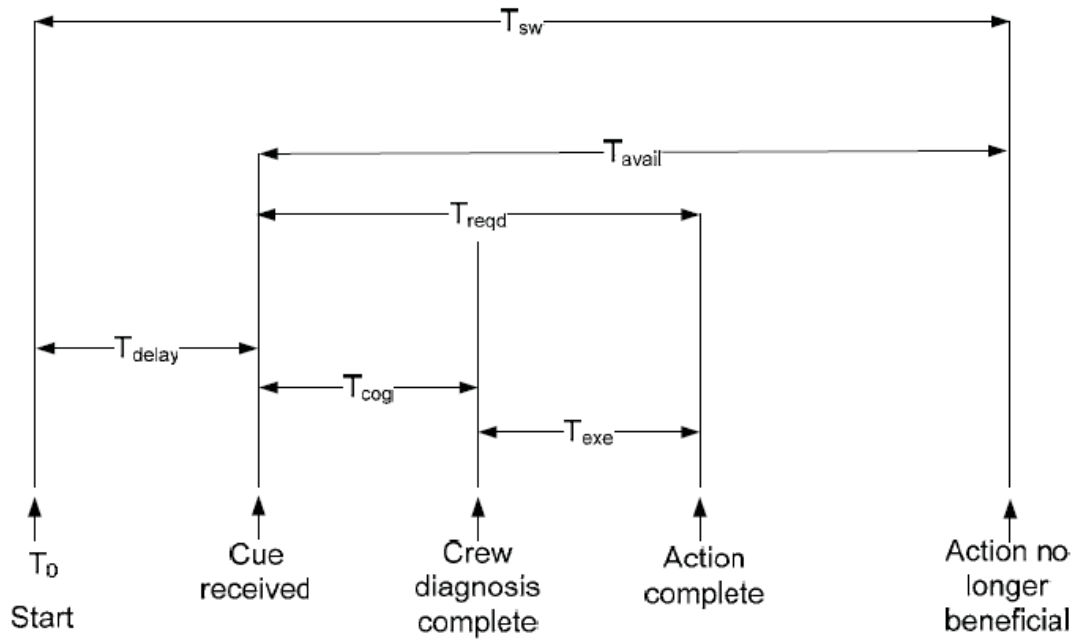


Figure 7-4
Illustration of individual HFE timing concepts from NUREG-1921

The terms associated with each timing element are summarized in each of the sub sections below.

7.4.1 Reference Time (T=0)

T=0 is defined as the start time or reference time. This may be fire ignition and detection by plant personnel as described in Section 7.3.1 and/or the start time of the accident progression as described in Section 7.3.2. As discussed in Section 7.3.2, most MCRA scenarios model the fire leading to an immediate reactor trip, so the start of the fire coincides with reactor trip. Establishing T_0 provides a reference time that can be used to relate any of the timing sources listed in Section 7.3.

7.4.2 System Time Window (T_{SW})

The system time window is designated as T_{sw} and is defined as the time from the reference point until the action is no longer beneficial. This time is typically derived from thermal-hydraulic data and, for HRA quantification, is considered to be a static input. Because the thermal-hydraulic analysis typically models the start time of the time window as the reactor trip, it is important to relate this to the start of the fire using a reference time (see Section 7.4.1). The system time window represents the maximum amount of time available for the action.

In many cases, T_{sw} is determined based on a thermal-hydraulic calculation for the most limiting conditions. For example, consider the operator action at a PWR to recover AFW outside the MCR after the decision to abandon has been made. A thermal-hydraulic calculation is performed for a scenario in which all secondary cooling (e.g., AFW, MFW, condensate) is lost at T=0 to determine the time to steam generator dry out assuming no feed and bleed. In this example, this time was calculated to be 60 minutes and represents the total time available from T=0 until this action must be completed. Note that 60 minutes represents the most limited case

and there could be scenarios in which the most limited case is overly conservative. For example, if AFW successfully runs for 20 minutes before operators trip the pumps inside the MCR, as directed by the MCRA procedure then T_{sw} would be longer than 60 minutes. At a minimum, in this case,

$$Tsw = 20 + 60 \text{ minutes} = 80 \text{ minutes}.$$

For the HFE associated with the decision to abandon, the system time window is defined as the time from the start of the fire until the point at which operators must make the decision to abandon in order to successfully perform all Phase III actions. As described in Section 7.3.3 this time will be defined by the HRA based on how much time is required for the Phase III actions.

The two examples below illustrate how T_{sw} is determined for decision to abandon.

T_{sw} Example 1 – PWR example for T_{sw} associated with decision to abandon

Scenario description: Fire starts in cable spreading room. AFW is failed, MFW is failed, one PORV fails open, charging pumps are failed, and bleed and feed cannot be performed from the MCR.

Based on thermal-hydraulic calculations, operators have 60 minutes to avoid core damage by starting a motor-driven AFW pump and/or charging. In order to establish and control AFW and charging, control and instrumentation for these systems must first be established at the RSDP. The Phase III actions credited in the PRA and time required to complete ($T_{cog} + T_{exe}$) are summarized in Table 7-1; Figure 7-5 provides a diagram of the timing information, consistent with the generic diagram in Figure 7-2.

Table 7-1
Example 1: actions credited and time required

Action	$T_{cog} + T_{exe}$ (Minutes)	Basis
Establish control at RSDP	15	The JPM allotted time is 15 minutes. This time includes both cognition and execution.
Establish AFW locally	15	Obtained from simulator training session data as the time to go from Step 11 *Implement Appendix Y* to Step 22 *Check reactor sub critical*.
Establish charging locally	20	Obtained from operator talk-through.
	Total time for Phase III actions = 50 minutes	

T_{sw} for the decision to abandon equals 60 minutes – 50 minutes = 10 minutes. This assumes that the time margin of the Phase III actions is 0. See Section 7.3.3 for additional discussion.

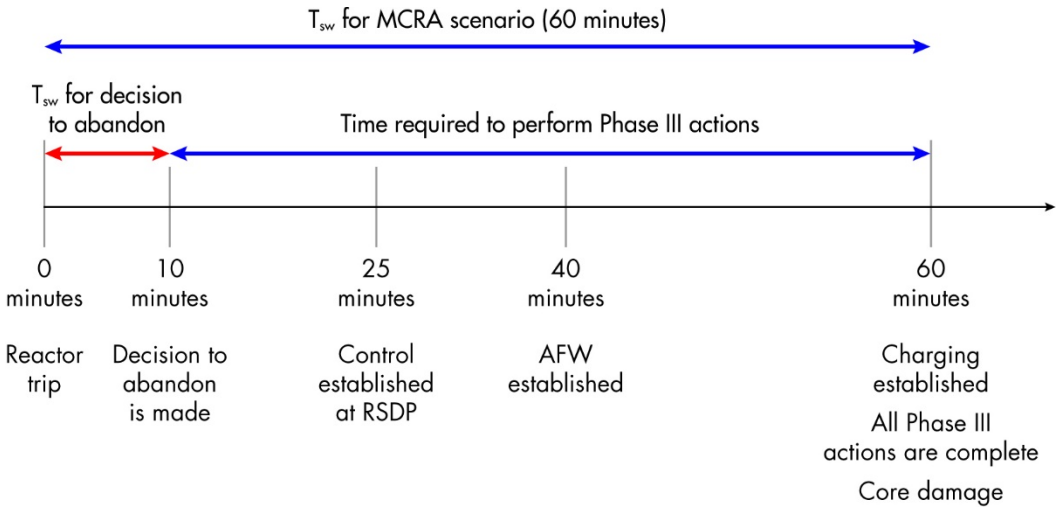


Figure 7-5
Example 1 timeline showing how T_{sw} is determined for decision to abandon

Tsw Example 2 – BWR example for Tsw associated with the decision to abandon

Scenario description: Fire starts in the CSR. At T=0, all sources of injection are lost, 5 SRVs spuriously open, and power to bus A is lost.

Based on thermal-hydraulic calculations, operators must establish low-pressure injection within 20 minutes after a loss of all high-pressure injection. The Phase III actions credited in the PRA and time required to complete (T_{cog} + T_{exe}) the actions are summarized Table 7-2. Figure 7-6 provides a diagram of that timing information.

Table 7-2
Example 2: actions credited and time required

Action	T_{cog} + T_{exe} (minutes)	Basis
Establish control at RSDP	10	Talk-through of abandonment procedure steps 1-10
Re-establish power to bus	3	1 min cognitive and 2 min execution based on talk-through. Same timing as used for internal events action.
Start low pressure injection at the RSDP	4	2 min cognitive and 2 min execution based on talk-through of procedure steps.
	Total time for Phase III actions = 17 minutes	

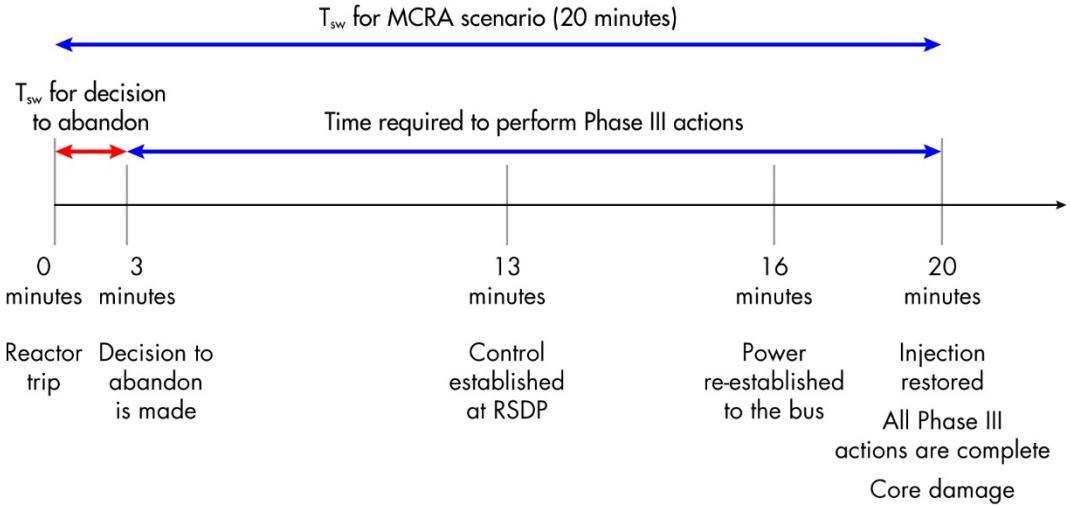


Figure 7-6
Example 2 timeline showing how T_{sw} is determined for decision to abandon.[33]

T_{sw} for the decision to abandon is calculated as 20 minutes –17 minutes = 3 minutes. With a system time window of only 3 minutes, the HRA analyst must ensure that this scenario is feasible. If the time required to make the decision to abandon is greater than 3 minutes then this scenario is not feasible. The T_{sw} of 3 minutes assumes that the time margin of the Phase III actions is zero. See Section 7.3.3 for additional discussion.

7.4.3 Delay Time (T_{delay})

The delay time, T_{delay}, is defined as the time of the cue from the reference time.

For MCRA scenarios, the time of the cue could be the time of abandonment, the time to reach a procedure step (or if coordinating with another operator, the time the associated operator reaches a procedure step), or the time a parameter reaches a certain level.

Table 7-3 shows the inputs to the estimation of T_{delay} for starting an injection system following MCRA.

T_{delay} corresponds to the time from T=0 to the arrival of the cue signaling loss of inventory and need to start charging pumps. Review of the fire procedures and discussions with operators shows when the actions are expected to occur all relative to the start of the fire.

[33] This example shows a time margin of zero (i.e., the time required to decide to abandon and the time required to perform Phase II actions is equal to the system time window). Technically, this case is feasible but may require more treatment in quantification (which is not addressed in this report).

Table 7-3
Inputs to estimation of T_{delay}

Action	Expected timing (minutes)	Basis
Start of the fire	0	
Decision to abandon has been made	25	Time at which the decision to abandon has been made.
Time at which control is established at RSDP	7	Once the decision to abandon has been made it will take the operators 7 minutes to establish control at the RSDP. This is based on walk-through and talk-through of the MCRA procedure. Establishing control at the RSDP is a prerequisite for injection.
Cue for injection	3.25	A simulator demonstration showed that, once the operators established control at the RSDP, it takes 3.25 minutes to reach the procedure step to start charging.
	T_{delay} = 25+7+3.25 = 35.25 minutes	

7.4.4 Cognition Time (T_{cog})

The cognition time, T_{cog}, consists of detection, diagnosis, and decision-making. During Phase I, and in most fires, the cues prompt an immediate response based on procedures such that cognition time is typically short. During Phase II, the time required for detection, diagnosis, and decision-making may be longer as the operators conduct activities such as verification of the fire (especially if it is outside of the MCR) and to evaluate the impact of their ability to control systems. During Phase III, after the decision to abandon the MCR, there are fewer cognitive activities such that each operator action is largely execution. Even so, there are still cognitive considerations including command and control, coordination, and communications which must be included in the time required for response. If the MCRA procedure is written such that each action must be performed in chronological order and the action requires no additional information other than what is written in the procedure, then T_{cog} could be short (e.g. under a minute). However, if the operator performing the action must obtain additional information by either communicating with an additional operator or interpreting hard to read indicators, then this time could be on the order of minutes. Any travel time related to obtaining information used in detection, diagnosis, or decision-making should also be included in the cognitive time.

7.4.5 Execution Time (T_{exe})

The execution time, T_{exe}, is defined as the time it takes to perform the action, including travel, collection of tools, donning of personnel protective equipment (PPE), and manipulation of relevant equipment. This time should also include time for communication. For HFEs modeling the long-term control of plant parameters, the time required for execution should extend to cover the mission time required for the action.

In Phase I, most actions occur in the MCR and the execution time can be based on simulator observations for MCR actions or JPMs for local actions. For Phase II, there will be no execution time associated with the decision to abandon, the decision to abandon is considered to be cognition only. For Phase III actions, the execution time can come from walk-through, talk-through, and JPMs (if available). In many cases, a combination of several sources will be needed to obtain an estimate, as shown in Tables 7-4 and 7-5.

T_{exe} Example 1: The execution time associated with the operator action to locally start an EDG.

Table 7-4
Example 1: collection of timing information associated with locally starting EDG

T_{exe} for starting EDG locally	Source of timing information
10 minutes	JPM – Allocated time required to be met by all operators
7 minutes	Operator interviews indicated that it would take no longer than 7 minutes to start diesels from the beginning of the fire scenario
6.5 minutes	Walkdown time

In the above example, a conservative estimate of 10 minutes is used as the execution time. Since operators do not have a direct procedural path to locally start the diesel, the dispatch of the operator to manually start the diesel could be delayed.

T_{exe} Example 2: The execution time to establish command and control at the RSDP contains several sub-tasks and the timing associated with each sub-task can come from different sources.

Table 7-5
Example 2: development of timing information associated with establishing command and control at RSDP

Subtask	Time (Minutes)	Source of timing information
Transferring control in the MCR to RSDP prior to leaving MCR	2	A simulator observation was performed to observe how long Steps 1-8 of the abandonment procedure would take prior to leaving MCR
Travel from MCR to RSDP	6	Walk down
Enabling control at RSDP	2	Walk down
	Total T_{exe} = 10 minutes	

7.4.6 Time Available (T_{avail})

Time available, T_{avail}, is defined as the time available for the action. T_{avail} begins at the cue to perform the HFE and it ends when the action is no longer beneficial, so it is calculated as $T_{avail} = T_{sw} - T_{delay}$. T_{avail} is one of the two inputs used to evaluate feasibility.

7.4.7 Time Required (T_{reqd})

The time required, T_{reqd}, is defined as the time needed to accomplish the action, including both cognition time and execution time (i.e., $T_{reqd} = T_{cog} + T_{exe}$). This time is one of the two inputs used to evaluate feasibility. By definition, time required includes both cognition and execution but, in many cases, the cognition time is minimal compared to the execution time and/or the cognition time cannot be observed separately from the execution time.

Once all of these timing parameters (i.e., T_{sw}, T_{avail}, T_{reqd}) are collected, the analyst may evaluate feasibility.

7.5 Integrating Timing Sources into MCRA Timeline

As described in Section 7.2, the MCRA timeline consists of three phases. Table 7-6 shows the key timing parameters in each phase and describes how the information is used to form the combined MCRA timeline.

Table 7-6
Integration of timing sources into MCRA timeline

MCRA Timing Phase	Timing Parameter	Timing Sources	Notes
Phase I	Start of the fire (T_0)	Fire response timeline	All timing inputs in the MCRA timeline should be estimated with respect to the same T=0
	Time of reactor trip	Fire response and/or operator response timeline	For many MCRA scenarios, the severity of the fire and loss of significant systems would be expected to lead to fire-induced reactor trip shortly into the scenario, if not immediately, and therefore taken to occur at T=0. For LOH, where equipment failures have not caused a reactor trip, this defines the start of system time window and time at which the operators enter the EOPs.
	Following reactor trip, time at which key EOP and fire PRA actions are started and the time at which the cue for each of these actions is received.	Operator response timeline	In many cases, the procedure progression can be used to define the cues for many individual actions.
	Time at which fire is suppressed and times at which firefighting occurs	Fire response timeline	If the operations staff is also on the fire brigade, this may take staff away from MCRA response. The time at which fire is suppressed could impact the time at which crew members become available to take additional actions.[34]

[34] All U.S NPPs have procedure guidance to ensure that for design basis MCRA scenarios there will be sufficient staff available to fight the fire and perform the required actions. However, there could be fire scenarios that require more actions than the design basis scenarios and the availability of crew members must be verified.

Table 7-6 (continued)
Integration of timing sources into MCRA timeline

MCRA Timing Phase	Timing Parameter	Timing Sources	Notes
Phase II	Time at which the abandonment criteria are met relative to the start of the fire	Fire response/accident progression timeline	Identifies plant-specific cue (T_{delay} with respect to T_0) of need to abandon MCR.
	For LOC, time required for the control room crew to make the decision to abandon	Decision to abandon timeline	Determined by defining the LOC abandonment criteria, if not already specified in the MCRA procedure and through operator interviews. If well-specified, this could be as short as one minute for the decision process.
	Time available for Phase II	Decision to abandon with input from accident progression and fire response timeline	The time available for Phase II is informed by the accident progression timeline and fire response timeline but is determined by first identifying how much time is available in Phase III and then how much time is available to complete the required actions following abandonment to take the plant to a safe, stable condition. See Section 7.3.3 for additional discussion.
	Time to perform any required actions just before leaving the MCR	Operator response timeline	
	Time margin, if operators delay abandonment	Decision to abandon timeline	This time must be greater than or equal to zero in order for the scenario to be feasible. The more time margin in Phase II, the less time available to perform actions in Phase III.
Phase III	Time to perform any required actions just before leaving the MCR	Operator response timeline	
	Time at which operators leave the MCR	Decision to abandon timeline	The time at which the operators leave the MCR will be used to determine how much time the operators have to perform actions once outside the MCR.
	Time each action within the MCRA procedure is started	Operator response timeline	T_{delay} for the individual HFEs depends upon the time required for the decision to abandon and take actions required to leave the MCR. In some cases, the MCRA procedure is linear. In these cases, one action cannot be performed until the preceding action is completed.

Table 7-6 (continued)
Integration of timing sources into MCRA timeline

MCRA Timing Phase	Timing Parameter	Timing Sources	Notes
	Time required to complete each action listed in MCRA procedure, including travel times to action locations	Operator response timeline	The time required for response depends on what procedures are being used, including the time to transition through different procedures, as well as the time needed to implement the procedures.
	Timing of possible 'hold points' required by operators who are not co-located	Operator response timeline	In some cases, the procedure may have a 'hold point' (i.e., a note or a caution), calling for an operator to wait for communication that prerequisite actions have been completed.
	Timing of key communications required by operators who are not co-located	Operator response timeline	In some cases, communications between operators can delay an action from being performed due to the need to confirm one action's completion before another can be started.
	Time available to complete each MCRA action	Accident progression timeline	The time available to complete each action will be dependent on the accident progression model and the scenario-specific timing of when the action is no longer useful to prevent core damage. The time available for each action directly feeds into quantification.

7.6 Examples of MCRA Timeline and Individual HFE Timelines

7.6.1 Example of Timeline for LOH Scenario

Table 7-7 and Figures 7-7 and 7-8 present an example of an MCRA timeline for a LOH scenario. Table 7-7 shows the timeline as a running list of events starting with ignition. Figure 7-7 presents the timeline as a Gantt chart following MCRA, while Figure 7-8 displays the relative timing of the individual HFEs used to model the LOH MCRA scenario.

Table 7-7
Example MCRA timeline for LOH

Time Phase	Clock time	Description
Phase I	T =0	Start of fire in the MCR
	T =0	Reactor trip. Operators enter EOP-0 due to reactor trip.
	T =0	Control room crew is aware of the fire in the MCR.
	T =0	Fire brigade summoned.
	T = 5 minutes	First four steps of EOP-0 are completed. No safe shutdown (SSD) equipment is damaged by the fire.
	T = 5 minutes	Fire brigade continues to fight fire unsuccessfully. Operators open fire procedure, but fire has not yet progressed to consider abandonment.
	T = 5-17 minutes	Operators work in ES-01 and assess damage caused by fire. The fire brigade continues unsuccessfully to suppress fire. Operators notice the buildup of smoke in the MCR environment.
Phase II	T = 18 minutes	Fire modeling calculations show the evacuation criteria are met at 18 minutes and the crew will abandon at this time.
Phase III	T = 19-20 minutes	Operators perform the first eight steps of MCRA procedure. Most of the actions have already been performed since the operating crew has been progressing through EOP-0 since the start of the fire. Although the fire is causing smoke and hot gas, it has damaged only components associated with the panel where the fire has started. Upon completion of the first 8 steps of the MCRA procedure, AFW and RCPs are stopped as directed by the procedure and the electrical power feed from offsite power is tripped. Operators leave the MCR and go to the RSDP. The aux building operator leaves the ready room to start aligning AFW.
	T= 22 minutes	RO arrives at RSDP
	T = 24 minutes	RSDP instrumentation is established.
	T = 28 minutes	Aux building operator reaches the location and begins to restore AFW. The aux building operator must verify valve alignment and then start pump at RSDP.
	T = 30 minutes	AFW is established and Aux Building operator must radio back to RO at the RSDP that AFW flow has been established. Once started, AFW can be controlled at RSDP by a single operator. As soon as AFW is started the Aux building operator will travel to the charging pump location and begin to establish charging.
	T = 38 minutes	Aux Building operator radios to operator at RSDP to determine charging flow. The flow indicators are not available locally. This is a key communication; if not completed the action will fail.
	T = 42 minutes	Charging is re-established.
	T = 42 minutes – 24 hours	Long-term control of plant established. **Note:** The timeline should consider what is required for long-term control and when key inventories are depleted. In this example, the CST inventory is greater than 36 hours and the EDG tank inventory is greater than 30 hours. Both of these inventories are greater than 24-hour PRA mission time.

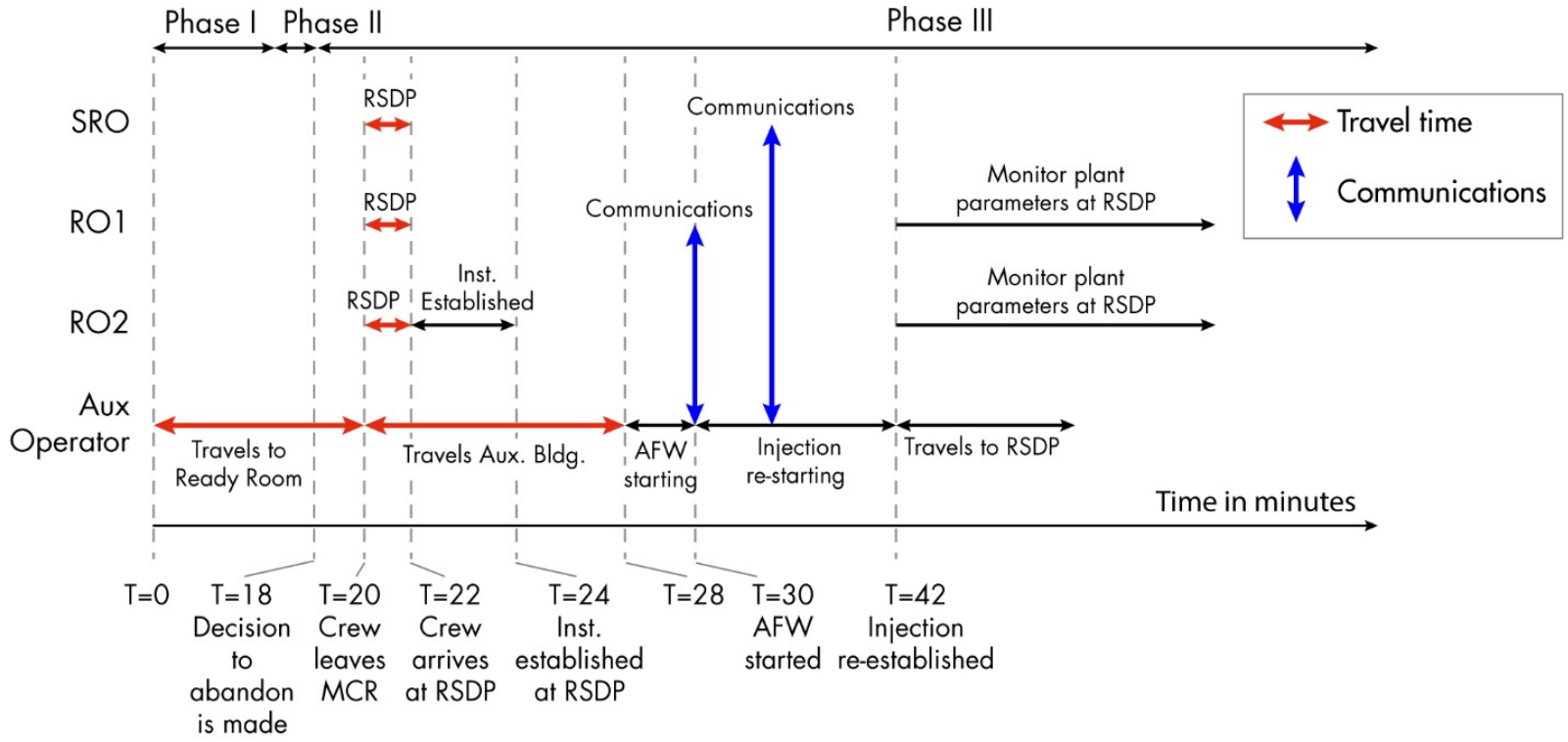


Figure 7-7
MCRA timeline after the decision to abandon has been made

In this example, an individual timeline was developed for the three unique operator actions:

1. Establishing control at the RSDP
2. Establishing and controlling AFW
3. Establishing and controlling charging

Since the decision to abandon will occur due to environmental conditions in the MCR (LOH), the decision to abandon was not included as a required operator action.

The individual timelines consider the following plant conditions; reactor trip with a loss of feedwater followed by no recovery of MFW or AFW, no sprays/fans, and no bleed and feed. AFW and charging fail at T=0 due to fire damage.

HFE 1: Operators fail to establish control at RSDP

T_{sw} = 40 minutes (Based on the most limiting/bounding T-H analysis)

T_{delay} = 22 minutes

T_{cog} = 1 minute

T_{exe} = 1 minute (T_{exe} includes travel time)

HFE 2: Operators fail to establish AFW

T_{sw} = 1 hr. and 8 minutes

T_{delay} = 20 minutes

T_{cog} = 1 minute

T_{exe} = 9 minutes (T_{exe} includes travel time)

HFE 3: Operators fail to establish charging

T_{sw} = 1 hr. and 38 minutes

T_{delay} = 30 minutes (Starting charging is delayed until AFW is established. T_{delay} is the time it takes for the aux building operator to reach the step in the abandonment procedure which directs the start of the charging pumps. The abandonment procedure prioritizes the order of actions based on the success criteria timing.)

T_{cog} = 1 minute

T_{exe} = 11 minutes (T_{exe} includes travel time)

For HFE 2 and HFE 3, the timing requirements start once the pumps are switched off by the operators before leaving the MCR. If pumps are running at the beginning of fire and continue to run throughout the scenario, then the operator actions to recover pumps would not be required. For HFE 2, AFW must be recovered within 50 minutes to prevent steam generator dry out. The time at which AFW runs successfully needs to be included in T_{sw}. T_{SW} = 18 minutes + 50 minutes = 1 hr. and 8 minutes.

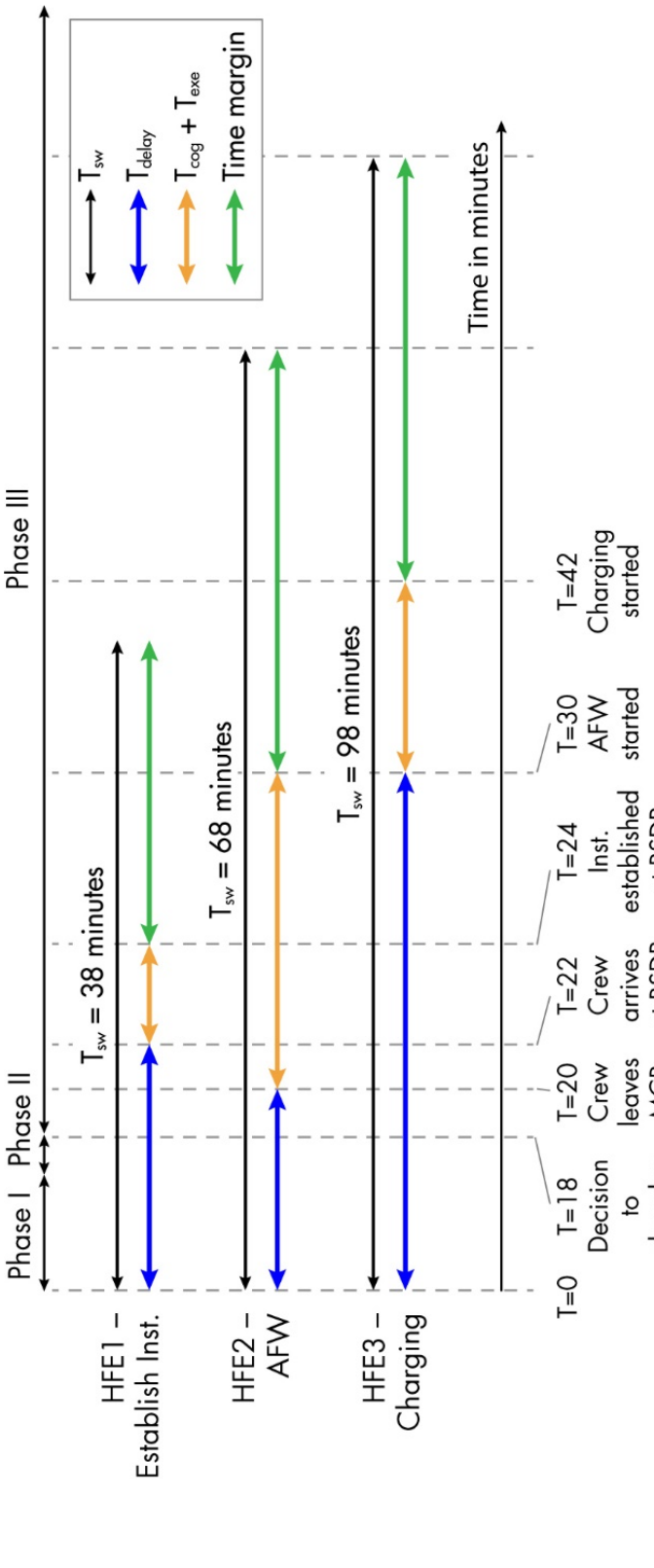


Figure 7-8
Timing of individual HFEs with respect to the same time origin

7.6.2 Examples of Timeline for LOC Scenario

Table 7-8 shows an example of an MCRA timeline for a LOC scenario.

Table 7-8
MCRA timeline example for LOC

Time Phase	Clock time	Description
Phase I	T = 0	Start of fire in the CSR.
	T = 0	Reactor trip. Operators enter EOP-0 following reactor trip.
	T = 0	Control room crew is aware of a severe fire in the CSR.
	T = 0	Fire brigade summoned.
	T = 5 minutes	The first four steps of EOP-0 are completed.
		There is major SSC equipment damage, including AFW failures, charging/safety injection failures, and MSIVs spuriously open.
Phase II	T = 6 minutes	Fire brigade continues to fight fire unsuccessfully. Operators open MCRA procedure and read the following criteria for abandonment: No decay heat removal systems are available from the MCR.
	T = 6-14 minutes	Operators work in EOP-0, EOP-1, and FR-H.1 to determine the status of the failed systems.
	T = 15 minutes	Operators make the decision to abandon MCR.
Phase III	T = 16 minutes	Operators perform the first eight steps of the MCRA procedure. Most actions have already been performed since the operating crew has been progressing through EOP-0 since the start of the fire. Upon completion of the first 8 steps of the MCRA procedure, AFW is secured and RCPs are stopped as directed by the procedure and the electrical power feed from offsite power is tripped. Most of these components are already failed due to fire damage.
	T = 17 minutes	Operators leave the MCR and go to the RSDP. The aux building operator leaves the ready room to start aligning AFW.
	T = 20 minutes	Operations team arrives at RSDP; SRO distributes MCRA procedure attachments to ROs.
	T = 22 minutes	Control is established at RSDP by SRO.
	T = 25 minutes	The aux building operator must verify valve alignment and then start pump.
	T = 28 minutes	AFW is established and aux. building operator must radio back to RO at the RSDP that AFW flow has been established. Once started, AFW can be controlled at RSDP by a single operator. As soon as AFW is started the Aux building operator will travel to the charging pump location and begin to establish charging.

Table 7-8 (continued)
MCRA timeline example for LOC

Time Phase	Clock time	Description
	T = 29 - 34 minutes	RO2 closes breaker to close spuriously open MSIVs.
	T = 35 minutes	Aux Building operator radios to operator at RSDP to determine charging flow. The flow indicators are not available locally. This is a key communication; if not completed the action will fail.
	T = 37 minutes	Charging is re-established.
	T = 37 minutes to 24 hours	Long-term control of plant established. **Note:** The timeline should consider what is required for long-term control and when key inventories are depleted. In this example, the CST inventory is greater than 36 hours and the EDG tank inventory is greater than 30 hours. Both of these inventories are greater than the 24-hour PRA mission time.

Timing associated with individual actions

The time available for each action following abandonment is determined by subtracting T_{delay} from T_{SW} in this example. In some cases, T_{delay} is defined as the time of abandonment.

HFE 1: Operators fail to establish instrumentation at RSDP

T_{sw} = 38 minutes

T_{delay} = 20 minutes (Based on time at which operators reach the RSDP.)

T_{cog} = 1 minute

T_{exe} = 1 minute

HFE 2: Operators fail to establish AFW

T_{sw} = 50 minutes

T_{delay} = 17 minutes

T_{cog} = 1 minute

T_{exe} = 10 minutes (T_{exe} includes travel time)

HFE 3: Operators fail to establish charging

T_{sw} = 1.5 hours

T_{delay} = 28 minutes (In this example, initiation of charging is delayed until AFW is established. T_{delay} is the time it takes for the aux building operator to reach the step in the abandonment procedure which directs the start of the charging pumps. For this example, the abandonment procedure prioritizes the order of actions based on the success criteria timing.)

T_{cog} = 1 minute

T_{exe} = 8 minutes (T_{exe} includes travel time)

HFE 4: Operators fail to close spurious MSIVs

T_{SW} = 1.15 hours

T_{delay} = 29 minutes

T_{cog} = 1 minute

T_{exe} = 4 minutes including travel time

7.6.3 Dual Unit Abandonment Timeline Example

Figure 7-9 shows an example timeline for a dual unit abandonment. The purpose of this example timeline is to show the timing relationships between the actions for a plant with a shared control room. The top portion of Figure 7-9 shows the actions required for Unit 1 and the bottom portion shows the actions required for Unit 2. Following abandonment, the STA (shared between units) will go to the technical support center (TSC) and start monitoring available parameters on both units from the plant computer system. All other operators will report to the designated RSDP. The fire PRA does not credit the plant computer system, therefore the STA's role in establishing a safe, stable state is not credited in the analysis. The abandonment strategy is designed such that once abandonment occurs, Unit 1 and Unit 2 crews function independently.

In Figure 7-9, the green lines show when the operator will be located at the RSDP, the red lines show when the operators will be away from the RSDP. The blue lines indicate when key communication and/or coordination will be required among operators located at different locations. All of the actions credited in the MCRA scenario are shown for completeness and not all actions would be required if the preceeding actions are successful. For example, if depressurization and starting LPCI are only needed in the MCRA scenario if operators fail to start RCIC before -125 is reached.

In this example, the exact times have been replaced by variable names. (T=0, T=EDG, T=RCIC, etc.). This is done to show that the timeline can first be represented graphically and then the analyst can work to establish the timing values. It can be useful to first establish the relative timing relationships, before calculating the specific times. So, when the actions are walked down or discussed, the analyst is aware of the key coordination and communication points among operators that need to be considered. It is also helpful to understand this relationship, since often a range of times is provided instead of a single point estimate.

This example involves a LOOP. Starting of the EDGs is the only action shown on the timeline in Phase I, because the action to locally start the EDGs is the only action credited in the fire PRA before MCRA occurs. In Phase I, the operators will enter the EOPs and the fire procedures. The fire procedures do not direct any actions until after the decision to abandon has been made. While in the MCR, the EOPs are followed, but due to extensive fire damage, none of the EOPs are effective. In Phase I, one local operator for each unit will be dispatched to start the EDGs for their respective unit. The time that these operators are dispatched is named T=EDG in Figure 7-9. The action to locally start the EDGs may not be completed by the time that abandonment occurs. If either of the EDG operators needs to communicate with the MCR staff following MCRA, additional challanges would be presented since command and control has moved outside the MCR.

Phase II is designated as a point estimate at time T= ABANDON. When the LOH conditions are reached, there is no hesistation among the operators to leave the MCR. The time between when the criteria are met and when the operators leave is less than a minute. Since this is a shared MCR, both units are modeled as leaving at the same time.

Phase III starts onces the decision to abandon has been made. At that point, the operators are expected to ensure the reactor is tripped and transfer control to the RSDP. Once complete, the staff in the control room will travel to their specified destinations. Once at the RSDP, or designated location, the shift supervisor for each unit begins to direct and coordinate required actions. Once outside the MCR, both operating crews function independently; however, the same types of actions are required for both units.

Summary of Key Events On Dual Unit Example Timeline

There is a fire inside the MCR and, at T=0, the fire starts and a LOOP occurs. The EDGs on both units fail to start and a local operator will locally start the EDGs at time T= EDG. This will occur before MCRA. At time T = ABANDON, the LOH criteria are met and the shift superviors make the decision to leave the MCR. Once the decision to abandon is made, the crew for both units will leave the MCR at the same time and proceed to the appropriate RSDP.

At time T= RSDP, all operators (expect for the ones starting the EDGs) are given an attachment which outlines their required tasks. The first task is to establish instrumentation and control at the RSDP. Unit 2 has only one RSDP and establishing control and instrumentation is performed at a single location. Unit 1 has two RSDPs and coordination is required between operators at multiple locations.

Once instrumentation is established, RCIC is started (T= RCIC). For Unit 1, this requires one operator to locally operate the RCIC valves and a second operator at the RSDP to start the RCIC pump. For Unit 2, control of the RCIC pump and valve manipulations are both performed at the RSDP.

At time T= MSIV, the operators who were directed to start the EDGs are now directed to close the spuriously open MSIVs. The abandonment procedure directs the operators to close the spuriously open MSIVs regardless of known status. In this scenario, power is lost so the MSIVs are closed but the expected plant response is that the operators will follow all procedures steps in the MCRA procedure. This action has been added to the timeline to show who is doing what when. This action would make the operators unavailable to assist with other actions if needed.

At time T= DEPRESS, the RPV level reaches -185 inches if RCIC cannot be started. T = DEPRESS represents the end of the system time window to start RCIC. If RCIC is started before this time, then the plant can remain in hot standby and the actions associated with times T=DEPRESS and T=LPCI would not be required. T = DEPRESS also represents the time at which instrumentation must be established at the RSDP; without instrumentation, the operators will not know RPV level and, therefore, would not know they had to depressurize. If RCIC is not started before T= DEPRESS, then the crew is expected to initiate an emergency depressurization. For both units, depressurization is performed by opening SRVs from the RSDP.

T= LPCI represents the time at which depressurization must occur in order to enable low-pressure coolant injection (LPCI) and prevent core damage, if RCIC was not successful. Unit 1 requires an operator to open the LPCI valves locally and then start and control the pumps at the RSDP. This action requires coordination between two operators in two different locations. For Unit 2, the RSDP contains both the valve and pump controls and only requires a single operator.

T= SDU2 is the time at which the cue to establish shutdown cooling occurs for Unit 2. T = SDU1 is the time at which the same cue would occur for Unit 1. Due to differences in plant design, the time for Unit 1 and Unit 2 are different. For Unit 1, establishing shutdown cooling requires four operators at three different locations. For Unit 2, three operators in three different locations are required. Both units require the use of chemistry personnel. The time required to establish shutdown cooling includes the time needed for communication and coordination of multiple personnel. Following abandonment, all support staff such as health physics, chemistry, electrical personnel are co-located at the TSC and awaiting futher instructions. The travel time for the chemist is included in the time required for shutdown cooling.

T = 1.5 hrs and T= 2 hrs are the times at which shutdown cooling is expected to be established. It should be noted that the completion times between Unit 1 and Unit 2 will be different due to differences in plant design.

After shutdown cooling has been established, the MCRA procedure directs the crew to maintain long-term control until the MCR can be re-entered. There are no specific actions listed in the procedures. During the PRA mission time of 24 hours, the anticipated control actions include:

- Refilling the EDG fuel tanks
- Maintaining RPV level
- Refilling of the CST

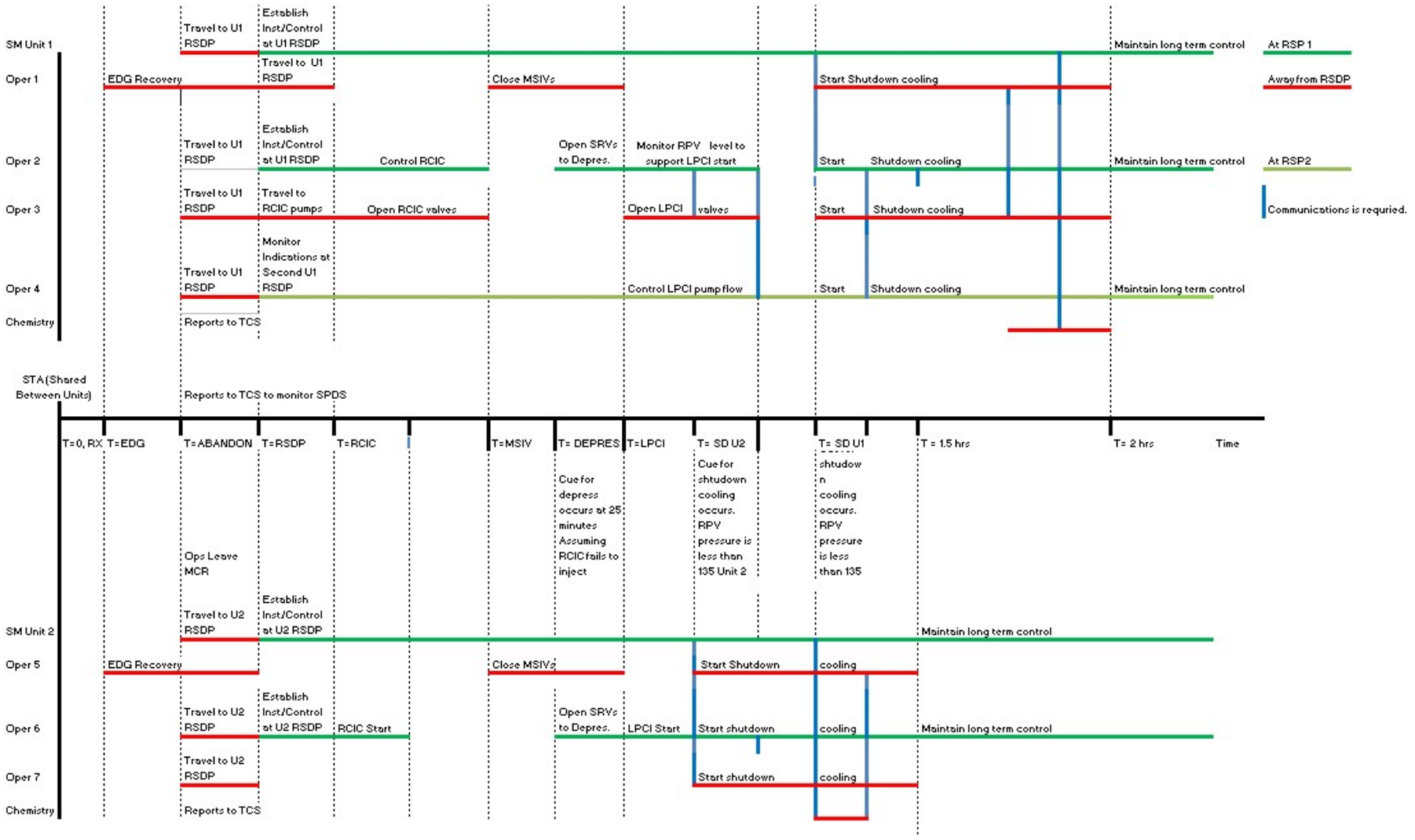


Figure 7-9
Timeline for dual unit abandonment

7.7 Uncertainty Associated with Timing

Section 9.4 provides a discussion of uncertainty analysis that is relevant to MCRA scenarios. This section provides some additional discussion that is specifically related to the development of timing inputs for MCRA scenarios.

Both the MCRA timeline and the individual HFE timelines should be based on best estimates, to the extent possible. Ideally, each scenario should be talked-through and walked-through with operators in order to determine $T_{Required}$ for each action (i.e., the time it takes to perform the actions, including travel time). In addition, most timing parameters in the MCRA timeline are presented as point estimates for convenience of understanding the scenario. However, each point estimate could be replaced with a range of values that is determined to be more appropriate. The time ranges for $T_{Required}$ can also be collected as part of data collection in talk-throughs and walk-throughs. The upper bound of the response time ranges can be used initially and then refined as needed, depending upon the impact on the HEP, and the degree to which a conservative HEP impacts the fire PRA results.

In general, there will likely be greater uncertainty associated with timing information based on assumptions as opposed to uncertainty associated with the timing data that is simulated or observed via a JPM or walk-through. Examples based on assumption include:

- Time to abandon
- Timing associated with coordination of multiple, concurrent actions
- Timing associated with key communications

It is recognized that MCRA scenarios are complex and there is more subjectivity associated with these scenarios than with internal events scenarios. Once a base MCRA scenario has been constructed, the HRA analyst can perform sensitivity studies on individual time parameters to determine the overall impact on the timeline.

7.8 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. 1023001/NUREG-1921.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,* U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
3. U.S. Nuclear Regulatory Commission. NUREG-1852*, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,* Washington, D.C. October 2007.

8
PERFORMANCE SHAPING FACTORS FOR MCRA SCENARIOS

8.1 Introduction

This section provides guidance for evaluating PSFs in the HRA task for MCRA scenarios. The guidance provided herein is not meant to duplicate material that was already given in NUREG-1921 [1], but to provide those items and issues specific to the evaluation of PSFs that are particularly relevant for MCRA. Typically, the evaluation of the PSF impacts are evaluated following the definition of the HFE and the feasibility assessment; however, the qualitative analysis should be considered an iterative process. The process of reviewing timing and PSFs also provide an initial qualitative analysis for input to the HFE quantification.

The guidance for evaluating PSFs is primarily derived from the list of PSFs developed in NUREG-1921 [1] and the experience of PRA analysts in identifying the kinds of MCRA sequences modeled in fire PRAs. The impact of the PSFs on MCRA operator actions is based on several sources: 1) the literature review of the bases for human performance assessment (which started with NUREG-2114 [2]), 2) interviews with current and former operators and trainers, 3) the experience of analysts in using various HRA methods, what these methods indicate about the effects of different PSFs and the contexts in which they are influential, and 4) the experience of analysts in performing fire and MCRA HRAs and PRAs.

A proper foundation of information gathered through, for example, talk-throughs or walk-throughs, is crucial for an accurate portrayal of the MCRA scenario and context and is necessary for understanding PSF impacts. Therefore, Appendix C, which describes the information gathering process, should be reviewed prior to applying the guidance described in this section. Appendix C also offers guidance on how to conduct the operator interviews, plant walk-throughs, and talk-throughs.

8.2 PSFs Relevant to MCRA

Although the core list of PSFs relevant for MCRA is similar to that focused on in NUREG-1921 [1], there are special considerations for each of these PSFs as well as overarching themes that must be considered.

Command and control has been identified as a process of unique importance to MCRA and is, therefore, not discussed in NUREG-1921. Command and control describes the need for a central body of authority to make decisions but have them carried out by a distributed group. A discussion of this topic is provided in Appendix B, but certain command and control elements are discussed below under individual PSFs.

NUREG-1921 identifies the following PSFs as relevant for fire HRA:

- Complexity
- Crew dynamics
- Crew communications
- Cues and indications
- Procedures
- Training
- Timing
- Workload, pressure, and stress
- Human-machine interface
- Environment
- Staffing and Availability
- Special equipment
- Special fitness needs

NUREG-1921 provides guidance on each of these PSFs that generally applies equally to the MCRA scenarios as well as the non-abandonment scenarios. Guidance specific to MCRA is identified below for each PSF. In some cases, NUREG-1921 included guidance for abandonment cases, and that is included below as a reminder, along with additional guidance where relevant.

In general, assessment of the PSFs for MCRA needs to consider: 1) the decision to abandon the MCR, 2) actions at the RSDP, 3) local actions in the plant, and 4) command and control issues. These topics are discussed for each PSF category.

8.2.1 Complexity

There are several possible sources of complexity associated with MCRA scenarios beyond those that apply for the non-abandonment situations. Two of the most obvious sources are the challenge of deciding to leave the MCR (discussed in Section 4), and, after leaving the MCR, the complexity of controlling the plant from multiple local positions coordinated via a distributed communication system. In addition, the concurrent use of multiple types of procedures (e.g., AOPs and EOPs usually prior to MCRA) may make the response more complex.

The issue of complexity arises with the combined effects of multiple PSFs. In general, operations in the event of a fire involving MCRA will be more complex than for a non-abandonment event and will involve additional PSF influences not normally considered in the case of non -abandonment. These are mostly because of the change in the command and control environment caused by the operating crew being dispersed to multiple locations rather than being co-located in the MCR. As a result, additional PSF characteristics need to be considered, not only individually but also in combination, to understand how the reliability of the operations will be affected. Appendix B goes into more depth on the issue of command and control and how to consider the effects of PSFs.

Issues that need to be addressed in evaluating the degree of complexity are:

- While in the MCR:
  - The extent of guidance provided in the procedures or training on the decision to abandon and when to abandon the MCR (for LOH and LOC)
  - The potential for spurious (false) cues and indications that may occur in the MCR because of fire-related damage and that may cause a delay in deciding that abandonment is necessary
  - The degree to which the AOPs associated with abandoning the MCR are coordinated with the EOPs directing the response to the plant shutdown (e.g., do the AOPs direct the MCR crew to take copies of the EOPs with them during abandonment? Do they provide guidance on how the procedures interact in terms of priorities?)
- After abandoning the MCR:
  - The number of different locations that require manual positioning for taking plant readings and local control actions; also the number of movements of plant personnel between different locations during implementation of the MCRA procedure
  - The degree to which required control actions:
    - Involve challenging calculations
    - Have indirect effects (e.g., controlling a rapidly changing level by means of a manual flow-restricting valve)
    - Involve physical challenges (e.g., accessing equipment in cramped spaces, using ladders, or operating a valve requiring multiple turns of a difficult/large handwheel)
  - The degree to which control of more than one parameter may require coordination as a result of the impacts one action may have on another action (e.g., AFW/decay heat may influence RCS volume/inventory/the need for charging flow/injection)

Complexity may lead to errors of omission as well as errors of commission. Complexity also feeds into timing considerations in the HRA, since more complex and challenging cognitive or execution actions are expected to require more time to perform. Reflecting complexity in the timing can become an important factor in the assessment of MCRA feasibility assessment given the time constraints for when the actions need to be completed. These issues are discussed further in Section 7 regarding MCRA timing and timelines.

8.2.2 Crew Dynamics

Because command and control is different for MCRA than for actions in the MCR, crew dynamics are considered to be even more influential. As has been discussed with the impact of other PSFs (e.g., complexity), further guidance on the special consideration of the impact of crew dynamics should be considered within the overarching theme of command and control covered in Appendix B.

For scenarios when the operators are in the MCR, the STA is responsible for maintaining the “big picture” of the situation and often assists with monitoring parameters and following the procedure(s). At some NPPs, the SS, who provides command and control at the RSDP in

MCRA scenarios, may be assisted by the STA. At other NPPs, the STA may be deployed as a field operator to take actions as directed by the SS. This use of the STA as an additional resource is plant-specific and needs to be determined based on interviews and simulator exercise observation.

The analyst also should consider that, following MCRA, crew members are distributed throughout the plant to perform the steps of separate MCRA procedure attachments independently (i.e., without direct oversight or peer checks from other crew members, as would be the case for actions performed in the MCR).

8.2.3 Crew Communications

Section 4.6.10.3 of NUREG-1921 [1] discusses the issues of communications related to operations at local panels and at the RSDP. For local actions, communication may be much more important because of the possibility of a less-than-ideal environment or situation. The way in which fire-induced equipment failures could affect the ability of operators to communicate as necessary to perform the desired action(s) should be understood. For instance, having to set up equipment, talk over significant background noise, and possibly having to repeat oneself multiple times should be considerations, even if only as possible “time sinks” for the time to perform the action. In addition, the analyst should assess the operators’ level of familiarity and training with any special communication devices.

Following MCRA, operators will be at the RSDP and other plant locations where actions are required. Therefore, the ability to communicate from different places should be addressed. Furthermore, if an SCBA is required to be worn, the apparatus might interfere with clarity in communications among team members. The ability of operators to communicate with one another during the initiation and execution of the tasks and after their completion is critical. The role and significance of communications in command and control is discussed in Appendix B.

Specific considerations when evaluating crew communications should include:

- The command and control structure for MCRA and how communication is proceduralized, trained upon, and implemented during simulator exercises
- Whether field operators are required to simply report back what has been done or if more complicated communication and coordination is required
- Whether or not the operators are using 3-way communication
- The type of equipment that is being used, the number of redundant and backup systems available, and related issues for ensuring that the equipment can operate when required (e.g., the need for extra batteries for the radio, or paging systems that are not functional in certain areas or during LOOP events)
- The assignment of radio frequencies or other methods for avoiding cross talk

8.2.4 Cues and Indications

NUREG-1921 [1] provides a comprehensive description of issues associated with indications and cues for ex-control room actions including those taken at the RSDP. This material should be reviewed when addressing this PSF.

However, it should be recognized that each plant and each RSDP is different, so the guidance below needs to be considered within that context and plant-specific cues, displays and annunciators (or the lack of them) need to be analyzed.

Prior to abandonment, the primary cue for diagnosis of a fire (aside from fires originating in the MCR) is the fire alarm. Analysts should note the location of the fire alarm panel(s) in the MCR, whether they are on the front or back panels, and how easy or difficult it is to determine the fire location and severity. Often an operator is sent out to locally verify the location and severity of the fire. Another important cue for the decision to abandon the MCR due to LOC is the plant parameter indications in the MCR, which may display conflicting and nonsensical readings due to fire damage.

The analyst may decide to identify a separate HFE for the actions associated with transferring control from the MCR to the RSDP; this HFE would include the case where “pre-staging” activities are taken prior to leaving the MCR altogether. If cues and indications inside the MCR are impacted by the fire, but abandonment is not yet required, then some plants may implement a strategy where they can send an operator to the RSDP and communicate plant information back to the MCR as necessary. If this strategy is implemented, the HRA should consider instrumentation fidelity at the RSDP compared to that in the MCR.

Analysts should also check whether the system parameter indications are easy to locate on the RSDP and whether these indication and/or displays present any human-machine interface deficiencies.

The RSDP may only have a small annunciator panel or no alarms at all, and there may or may not be a safety parameter display system (SPDS) available there. This reduction in alarms and display capability can impact awareness of parameters and plant conditions and should be analyzed as part of the limitations of command and control at the RSDP versus the MCR. The intent here is to understand the difference between how the crew can access and integrate information from the RSDP compared to doing the same in the MCR. This is accomplished by asking the following two questions:

1. How is the range of indications different from what the operators are accustomed to seeing?
2. How do the available resources (e.g., STA and TSC) change the ability of SS to integrate the available information into a “big picture”?

Another important task for the analyst is to conduct a comparison of the cues and indications presented at the RSDP with the information that the MCRA procedure or other procedures direct the operators to monitor. These additional procedures may be identified during operator interviews as being used at the direction of the SS. The availability of the TSC and the resources of the STA should be assessed for their ability to provide the “big picture” guidance that is usually available in the MCR but may not be available at the RSDP.

Operator interviews of the MCRA strategy usually determine that operators would be sent to check local equipment and indications when necessary. NUREG-1921 [1] points out that the crew may have less or even limited familiarity with the local panels and the way in which cues for actions are presented there (in terms of layout, demarcation, and labeling). These issues must be considered during walk-throughs and interviews in evaluating the adequacy of relevant cues for post-MCRA actions. As with the RSDP, analysts need to ensure that there are cues on the

local panels consistent with those required by the procedures. In addition, the potential effect of crews no longer having access to all of the information in the MCR (such as the full set of annunciators/indicators, plant process computer and associated alarms, plant drawings and other documentation) needs to be evaluated.

As a result of this evaluation, the analyst should be able to assess:

- The availability of information required by the procedures and the tasks
- The fidelity of this information for various fire scenarios (as determined by circuit analysis)
- The information that is available at the RSDP versus the information available at local stations

In addition, from the perspective of command and control, the limited information available at the RSDP may leave the SS concerned that there are conditions in the plant that he/she cannot observe and may act to distract him/her. During interviews, the analyst can inquire as to whether there are any plant conditions that the SS or plant staff may not be able to observe and that might act as a distraction or source of stress.

8.2.5 Procedures

Unlike EOPs that are by-and-large standardized for each of the vendor groups, the procedures that govern the evacuation of the MCR are written on a plant-by-plant basis, and, therefore, do not necessarily meet the same stringent criteria (e.g., the formatting) associated with EOPs and other similar procedures. As a result, the individual plant MCRA procedures need to be reviewed for:

- **Identification of the location of the fire.** Some plants have detailed procedures indicating actions required given a fire in a particular area based on the fire alarm panel identifiers and stipulate that local verification of the fire location and severity must be made. The analyst must ask: will the operators have enough time to confirm the location and severity of fire given the MCRA scenario timeline(s)? (See Section 7 for more discussion of timelines and timing.)
- **Identification of appropriate and actionable criteria to guide the decision to evacuate the MCR because of a fire event.** (See Section 4 for additional discussion of the decision to abandon.)
- **Identification of actions to be taken before leaving the MCR during MCRA.** Examples of such actions include: control actions (such as tripping the reactor), plant announcement of change in control status to plant areas, isolation of controls in MCR, etc.
- **Relevance to the fire PRA scenarios for MCRA and the associated scenario feasibility criteria.** Historically, U.S. fire procedures were written to address the 10 CFR Part 50, Appendix R criteria [3], which may or may not match the PRA success criteria.
- **Inclusion of the collective set of MCRA actions for all operators in all locations.** For example, are communication points clearly identified in the procedures? Are multiple attachments or appendices supposed to be performed at the same time? What is the structure of the MCRA procedure and its relation to and application with EOPs, AOPs, and

annunciator response procedures (ARPs)? How will the procedures be implemented by operators (e.g., are there separate attachments for individual operators to use in separate locations)? Is the procedure structured by fire area, equipment impacted, or equipment required?

- **Inclusion of clear "kick outs" from the MCRA procedure.** For example, are there transitions from the MCRA procedure to other procedures that are required to reach a safe, stable condition?
- **Specification of who goes where and what to take.** Examples of items that might need to be collected in the MCR (before leaving) and taken to the RSDP are: EOP notebooks, radios, and keys.
- **Description of how the command and control is implemented for MCRA scenarios.** Examples of command and control issues that need to be addressed are: 1) indication of what proceduralized actions will be carried out, and 2) who is responsible for performing these actions. The MCRA procedure may address such issues or, the command and control and/or communications plan(s) for MCRA scenarios may address such issues. (See Section 6.4.1 for more discussion on the requirements for feasibility with respect to command and control, and communications plans for MCRA.)

The review of the MCRA procedure(s) should ensure that they contain sufficient information in a clearly laid out format and written in a readily understandable language that facilitates their use during the high stress conditions of the event. Interviews, tabletop discussions or talk-throughs, and walk-throughs can inform how the procedure(s) would be implemented by the operators and can reveal any disconnects in how the procedure is written versus how it would be implemented by the operators.

8.2.6 Training

Training on fire, especially MCRA scenarios, is typically given on a less frequent basis than for other accident scenarios that require the use of EOPs and in a less realistic simulator setting. Often, training on MCRA scenarios is provided once per year and consists of talk-throughs, with some visits to plant areas. Few plants have a simulated RSDP for training. Plants that do simulate the RSDP have a range of training capabilities ranging from a cabinet (or perhaps a computer terminal) to the use of a full mockup of the RSDP.

Consistent with discussions in Section 8.2.5, training should be reviewed to verify inclusion of the collective set of MCRA actions for all operators in all locations. The interview template provided in Appendix C may be useful when interviewing the operators to understand how the integrated training on MCRA and the use of the RSDP is accomplished.

Given the wide variability in training, the following issues need to be reviewed to assess the plant-specific PSF for training:

- The frequency and comprehensiveness of training for MCRA, including training on making the actual decision to abandon the MCR, and ensuring that the necessary tools, procedures, knowledge of work locations, etc., have been preplanned
- The use of any kind of learning aid(s), such as a simulator or mock-up of the RSDP

- Whether the training involves visits to plant areas to:
  - Become familiar with access routes and any limitations, including consideration of locked doors security barriers, radiation, and other environmental access controls
  - Identify the location of local controls and indications
  - Evaluate communications tools (radio signals, sound-powered telephones, etc.)
- Donning and wearing of SCBA or other PPE

The HRA analyst should attend a simulator training session for MCRA to see how it is conducted, what the operator response is like, how the decision for MCRA is made, and how actions at the RSDP and local panels are trained upon. Some sense for the timing of the scenario can also be gained, as well as insights on procedure use and other PSFs. Attending the post-training exercise briefing is also important to obtain insights on what went well or not so well, in the trainers' eyes.

A separate walkthrough of the MCRA strategy should also be conducted to access local areas where actions take place.

8.2.7 Timing

Timing is discussed extensively in Section 7 of this report and is also covered in NUREG-1921. When considering timing, the HRA task needs to consider (particularly for the LOC events) the three phases of abandonment described in Figure 7-1 as well as the actions taken following abandonment. Also, Section 4.2.2 of NUREG-1852 [4] mentions equipment access, different travel paths resulting from the fire location, and expected variability among individuals and crews as other contributors to timing uncertainty.

8.2.8 Workload, Pressure, and Stress

This combination of workload, pressure, and stress is treated as a single discussion because they are so integral to each other; it makes little sense to separate them. Interviews of operations and training staff at various plants have confirmed that MCRA will be a stressful situation for the operators. Timing of actions and how quickly the operators must respond may also increase the pressure and stress felt; however, the impacts will be different for long-term versus short-term actions.

The issues associated with this PSF for MCRA are:

- Level of discomfort leaving MCR (e.g., quality of indications and controls available at the RSDP, MCRA training)
- The amount of work that is required by each plant operator involved in implementing the MCRA procedure(s), especially where travel to plant areas beyond the RSDP (either initially or during the response) is involved

- The effort required to reach the areas where operators perform actions, including the physical and administrative demands, coupled together with the time urgency and requirement for the actions to be taken
  - This includes the need to identify an alternate travel path to avoid any areas that the operators recognize as potentially hazardous
- The experience of having to don SCBA or other PPE seldom used
  - Narratives from non-nuclear settings indicates that some fraction of people become panicked when using SCBA due to claustrophobia or similar afflictions[35]
- The effects of possible distractions on the cognitive tasks of the SS, including:
  - Interruptions and calls from staff not directly related to immediate plant responses
  - The need to perform proceduralized tasks that are not essential to the PRA-modeled tasks
  - Physical layout of space (e.g., at the RSDP) and administrative protocols that may be in place to prevent access and limit distractions

8.2.9 Human-Machine Interface

The issues with respect to HMI can be quite varied depending on whether the particular plant has a RSDP or whether all or most actions must be taken at local controls distributed in plant areas. It is possible to evaluate the design of the interface and layout at the RSDP in terms of the kinds of human-factors criteria used for MCR designs, such as the use and layout of mimics, readability of indications, provision of feedback to confirm control actions taken have been effective (e.g., valve positions and motor states) and so on. In some cases, the panel's design is similar to the layout of related panels in the MCR, which should simplify the operators' understanding of the panel. For actions in plant areas separate from the RSDP, the concerns include whether the indications can be read with sufficient accuracy and the controlling devices (including manual valves) can be operated sufficiently easily and promptly to accomplish the requirements of the procedure steps within the time available. For both locations (i.e., actions at RSDP and at local panels), the feasibility and reliability of executing long-term control actions should be also be considered.

[35] Anecdotal information from military fire training, for example.

A walkthrough of the MCRA strategy should be conducted to see the RSDP, access local areas where actions will be taking place, and to note the key parameter indicators and interface points at each location to see whether they appear clear or confusing. It is recommended that this walk-through be done after the HRA analyst has reviewed the MCRA procedures and has become familiar with the MCRA scenarios identified in the PRA to know which parameters and controls are of particular significance. The items to be evaluated for this PSF are:

1. *For plants with remote shutdown panels*:
   - Are the parameters cited in the MCRA procedures provided at the RSDP and do they present the information in a way that facilitates operator understanding of the conditions? For example, are parameters that must remain below a particular level displayed digitally or are parameters that involve a trend shown as a graph?
   - Are controls for necessary equipment provided at the RSDP or must they be manipulated locally?
   - How well does the layout of indications and controls on the panel comply with the human-factors guidance for MCR panels? Section 12.2 of NUREG-0700 [5] presents guidelines for the design of local control stations (including RSDPs) in terms of HMI design requirements.
   - Is there sufficient space at the panel to place procedures and other documents to allow the operators to consult the documents when taking actions or directing others via communications?
2. *For plants without remote shutdown panels or where actions must be taken at locations other than the shutdown panel*:
   - Is local feedback to field operators provided for local actions?
   - For each indication credited in the MCRA response, is the display clearly identified, adequately clear, and sufficiently readable from where the operator will be to make the judgments of the value compared with the EOP requirements? The requirements of Section 12.2 of NUREG-0700 [5] for the HMI design of local control stations provide a set of standards for indications and controls.
   - For each control manipulated during the MCRA response, is the location of the control device (e.g., switch, breaker, valve, etc.) clearly labeled, accessible, and visible to allow the operator to take the necessary action without the use of access aids that are not permanently installed (e.g., a portable ladder or portable lighting)?

8.2.10 Environment

Section 4.6.7 of NUREG-1921 [1] identifies the issues associated with actions required outside the MCR. Of special consideration for MCRA are long-term actions. Specifically, would heat or radiation have an impact on how long someone could remain in a particular area (i.e., can operators continue to remain at the location for the PRA mission time given the environmental changes at that location)?

8.2.11 Staffing and Availability

Issues related to sufficiency of staffing and the availability of operators to respond to events may be of concern for MCRA scenarios. More operators than are normally in the MCR may be needed to take actions close in time in multiple plant areas, and the time needed to travel between locations may prevent operators from being able to accomplish all of the actions. Additionally, operators may be required to coordinate the actions performed in multiple locations. The possibility of using staff from another unit may be considered. This will not be practical, however, for plants that have a shared MCR for multiple units, or in the event of a multi-unit fire.

8.2.12 Special Equipment

As described in Section 4.6.8 of NUREG-1921 [1], operators will likely need to be prepared with portable equipment and tools for locally accessing and operating equipment. In addition, a means for accessing secure areas (e.g., keys, any special badges, etc.) may be required. These items must be taken to the RSDP from the MCR upon abandonment (if they are not provided at the RSDP). Beyond these considerations, there are no significant issues apparent for MCRA that were not already discussed in NUREG-1921.

8.2.13 Special Fitness Needs

In order to implement actions outside the MCR, the operators will need to be capable of reaching the equipment to be operated and taking actions in areas that may be difficult to access, especially if PPE such as SCBA is required. This capability may require the operators to be suitably fit to accomplish these actions. NUREG-1921 explains that the HRA analyst should verify that unique fitness needs are not introduced due to the fire and its effects (e.g., the need to move and connect equipment, especially if using a heavy or awkward tool).

8.3 Special Considerations for Decision to Abandon on LOC

While the PSFs related to the decision to abandon the MCR on LOC have been highlighted in the previous sections for the individual PSFs, the issues and factors important for the cognitive decision to abandon the MCR in LOC scenarios are summarized here. Modeling of the decision to abandon is discussed in detail in Section 4.

Timing estimates during LOC situations will be more difficult to ascertain, because the decision to abandon will be based on: 1) cues of system and function loss due to the severity of the fire, 2) procedure direction clarity on how these cues translate into abandonment criteria, and 3) training on the decision process itself. Ultimately, the decision to abandon is typically made at the discretion of the operating crew. Section 7 describes the calculation of the timing elements and considers that, for most U.S. NPPs, the criteria for abandonment can vary widely, from simply abandoning upon confirmation of an MCR fire to not being clearly defined (which may not allow a timely abandonment decision).

In addition to the uncertainty in estimating the timing, the decision to abandon during a LOC scenario also has increased complexity. In particular, when assessing the complexity of the diagnosis, the HRA analyst needs to consider that the diagnosis (and associated actions)

directed by the SS may be based on general guidance and interpretation of (potentially non-specific) cues, rather than based on prescriptive procedure guidance. Therefore, the complexity should be described in terms of the effect of the diagnosis and decision strategy, and whether it has a nominal or negative impact.

Finally, crew communications, staffing, and crew dynamics may be unusually impacted during LOC situations. While the procedures will state who makes the decision, the HRA analyst may not be able to clearly identify how the decision is reached, since the decision is a function of the culture of the operating crew and how they interpret the level of damage to key plant systems and functions that render the MCR ineffective. Interviews and simulator exercises play a significant role in revealing the crew dynamics of the decision process (e.g., the extent to which it is based on consensus versus declarative decision).

8.4 Guidance for Evaluating PSF Impacts

This section provides preliminary guidance on how to assess the reliability of operator actions in a qualitative manner. While the ultimate goal is to provide the means for quantifying the failure probabilities of HFEs, assessing the reliability qualitatively will provide a basis for identifying: 1) which kinds of accident sequences are most affected by which PSFs and scenario characteristics, and 2) the kinds of PSFs that need to be incorporated in an HRA quantification model to be used for these sequences. This guidance has been developed using the authors' experience with HRA modeling of MCRA scenarios, as well as the types of inputs already considered in existing HRA methods (e.g., cause-based decision tree (CBDT) [6], ATHEANA [7,8]), and more general understanding of influences on human performance (e.g., the cognitive mechanism tables provided in Appendix A of NUREG-2114 [2]). This guidance is expected to be updated, as needed, when separate quantification guidance is developed and when the understanding of command and control issues has further matured.

This guidance was developed by first considering how different kinds of scenarios that are modeled in the MCRA PRAs will affect the various types of PSFs. Second, the guidance considered what effects these PSFs will have on the reliability of the operator actions in these scenarios. For example, the likelihood of success in a scenario that requires actions at many plant locations could be challenged by inadequate staffing (which would be assessed as a negative PSF). The HFE representing these operator actions should therefore be assessed with a higher than "nominal" HEP in order to appropriately represent the staffing situation. In contrast, the effect of this PSF may not be important for scenarios that are primarily controlled from the RSDP and do not require as many local actions at various plant areas.

In some cases, the interaction of the scenario and one or more of the PSFs may be adverse, resulting in a lower likelihood of success, and in other cases it may be beneficial. For example, a well-designed RSDP that mimics the MCR will benefit from the training the crew has received on the instruments and cues in the MCR.

The assessment guidance provided here was influenced by the list of PSFs developed in NUREG-1921 and expanded upon in the above sections. In addition, the guidance was heavily influenced by interviews of current and former operators and trainers conducted by the authors of this report. The ex-operators interviewed had experience at BWRs and PWRs, and several also had experience as operator trainers. Several themes arose during these interviews, helping the

authors to better understand the context surrounding MCRA as well as better define the situations and PSFs that may have the biggest impact. Feedback was received on various issues such as: 1) how a two-unit shutdown is handled, 2) what parameters might be difficult to control locally, 3) how training is conducted, 4) if the determination of timing used during training is realistic, and 5) differences in the distribution of RSDP capabilities at a sampling of plants.

Tables 8-1 and 8-2 provide preliminary tools for the PSF assessment. Table 8-1 provides examples of the type of PSF impacts (detracting and compensating) that an analyst might see for certain scenario characteristics. These PSF impacts were identified as distinguishing factors from the HRA perspective for MCRA scenarios. While it is possible that a PSF can be better than optimal (and this can be noted in the documentation), these positive PSF influences typically (but depends on HRA quantification method used) influence the HRA as compensatory factors for other detracting PSFs. For this reason, Table 8-1 lists the potential detracting PSFs for a given scenario and their associated compensating PSFs. For example, the degree of capability of the RSDP has a significant impact on the HRA evaluation of an MCRA scenario. When the analyst is assessing the capability of the RSDP, one of the key attributes the analyst must evaluate is whether the RSDP provides the indications for the parameters that need to be monitored and controlled by the operators during MCRA scenarios, as defined by the MCRA procedure. Therefore, Table 8-1 advises the analyst that the HMI for the RSDP or local stations could differ significantly from the MCR, providing a detracting PSF (negative impact upon the analysis). However, the analyst also needs to assess whether the procedures and training provide an adequate compensating PSF to counterbalance the detracting HMI PSF. These evaluations will be based upon procedure reviews as well as operator and training staff interviews/walk-throughs/talk-throughs. In this sense, Table 8-1 provides ‘things to look for’ both in terms of MCRA scenario characteristics and PSF issues that matter most to the qualitative analysis of these scenarios. The intent of Table 8-1 is to provide a bridge between the qualitative analysis of PSFs discussed in this section and the quantification process to come.

Table 8-2 is intended to assist the analyst in determining which PSFs are the most significant contributors to the qualitative analysis of a particular MCRA scenario. For each of the PSF categories, the table identifies the issues that make a PSF consequential and why. For example, if a procedure is poorly worded, then it may not be executed when needed. Table 8-2 also indicates scenario-specific elements that should be considered for the PSF categories. Continuing the poorly-worded procedure example, if the scenario is risk-significant, then a procedure modification may be recommended to address the issue and improve the PSF assessment. Finally, Table 8-2 offers a selection of offsetting factors that may exist in the scenario to compensate for the negative effects of the consequential elements for each PSF category. Offsetting factors for poorly worded procedures could include the demonstration during walk-throughs that the action is simple enough not to require strong procedural direction, the shift supervisor clearly directs the action anyway, or skill-of-the-craft is evident in performing the action. These offsetting factors would, therefore, soften the negative impact of that PSF’s contribution to the qualitative analysis of the HFE/scenario.

The suggested application process is for the HRA analyst to identify the characteristics of the particular accident sequence being analyzed and see how they compare with the scenario characteristics presented in the first column of Table 8-1. It may be that more than one characteristic in Table 8-1 matches the sequence being analyzed. The analyst then uses the examples in Table 8-1 for each PSF category as triggers for the type of considerations needed to qualitatively evaluate each PSF. This approach assists the analyst in identifying which PSFs may be important influences for the reliability of operator actions based on the entries for the most closely-matching scenario description.

Table 8-2 then helps the analyst evaluate the degree of each PSF's influence on a scenario or HFE, to either drive it to a greater or lesser concern from a risk perspective. Offsetting factors that might mitigate the PSF's influence should be noted and documented. Particularly dominant adverse PSFs might even be candidates for modification (such as procedure changes or physical modifications to add capability the RSDP) to better ensure reliability.

If more than one set of characteristics in Table 8-1 matches, the HRA analyst must select either the most closely-matching description or consider more than one set of characteristics and then evaluate the overall result. If the differences warrant separating into multiple scenarios or HFEs, this should be coordinated with the fire PRA model development discussed in Section 3.

Table 8-1
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
Time constrained scenario or scenario involving rapid response Examples BWR: Fire causes multiple stuck-open relief valves (SORVs). Operators must locally remove power to the valve solenoids to close SORVs before uncovery of top of active fuel (TAF) occurs (~6 to 30 minutes depending on how many SRVs are open). PWR: Fire causes loss of RCP seal cooling. Operators must trip RCPs within 13 minutes on loss of seal cooling to avoid RCP seal LOCA.	Timing: The less time available for recovery, the lower the reliability.	Procedures and Training: • Clear (unambiguous) direction in procedure to reduce variability in diagnosis and execution time • Timed training runs (e.g., JPMs) with emphasis on key actions Crew Dynamics/Command and Control: • Clear plan in place for communicating priorities and coordinating operator actions and ensuring time critical actions are addressed when needed, despite distractions
	Procedures and Training: Actions in the MCRA procedure that are not deemed critical in the fire PRA could delay time-critical fire PRA actions and reduce the time margin.	Procedures and Training: • Timed training runs (e.g., JPMs) with emphasis on key actions • Re-shuffling of procedure steps to move non-risk significant steps after the risk-significant steps in the procedure
	Complexity: Challenging cognitive or difficult physical task to perform in time to prevent core damage	Procedures and Training: • Training, either in classroom or simulator exercises, that specifically address the challenging cognitive diagnosis and decision-making rather than just telling the crew what the scenario is • Timed training runs (e.g., JPMs) that include actual physical manipulations
	Environment: Conditions that could make actions more difficult and require more time, such as: • Emergency or portable lighting • Heat • Cramped spaces or difficult access to locations	Procedures and Training: • Timed training runs (e.g., JPMs) that include actual physical manipulations at location with discussion of possible lighting/heat issues

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
	Special Equipment: Equipment that could make actions more difficult and require more time to access and implement, such as: • Donning and working in SCBA • Acquiring and using special tools (location of lockers; have they been replaced/maintained) • Acquiring and using keys or key cards for secured areas	Procedures and Training: • Timed training runs (e.g., JPMs) that include actual physical manipulations at location using PPE gear Special Equipment: • Pre-staging required tools and PPE gear to ensure they are readily available when needed
	Staffing: Staff may be allocated to fire brigade or other tasks so that insufficient staff remains available to perform the required actions	Procedures and Training: • Plan for MCRA covers allocation of staff and appropriate prioritization to ensure operators are available to perform all required actions
Long timeframe or delayed action <u>Examples</u> BWR: Any fire scenario that requires containment venting. PWR: Fire causes transient. AFW runs for several hours until the CST depletes and operator must then refill the CST.	Cues and Indications: Cue presented earlier in scenario but not repeated at time when action is required (and could be forgotten)	Procedures and Training: • Procedure includes clear reminder step • Training highlights need for Shift Manager/Supervisor to provide cue reminder
	Procedures and Training: Numerous actions in the procedures can take attention away from the essential actions identified in the fire PRA.	Cues and Indications: • An additional cue presented when parameter reaches action point can be credited as a reminder to the crew to perform the required action Procedures and Training: • Procedure includes clear reminder step • Training highlights need for Shift Manager/Supervisor to provide cue reminder

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
	Workload, Pressure and Stress: Interim complacency or lack of vigilance until action is suddenly needed	Cues and Indications: • A relevant second cue presented (again) when parameter reaches action point can compensate for complacency Procedures and Training: • Procedure includes clear reminder step after interim procedure steps can compensate for lack of vigilance • Training highlights need for Shift Manager/Supervisor to provide cue reminder later in scenario and also compensate for complacency
	Staffing: Staff delegated to perform other tasks before the long-term action is required and is occupied with other tasks when required for the action	Command and Control: • Plan in place for supervisory monitoring and control of staffing
Includes actions to maintain control (initiate, actuate, stop) of a system or function (rather than a one-time action) <u>Examples</u> BWR: Maintain long-term RCIC control (vs. start RCIC).	Cues and Indications: Not all cues required for the control action are co-located at the action location(s) Complexity: Control action is distributed among various plant locations Timing/Workload, Pressure and Stress: The longer the time between each control iteration, the greater the chance that the operator will become distracted	Crew Dynamics/Command and Control: • Plan exists for coordinating control actions and for providing verbal cues for control steps Communications: • Supervisor (in charge of command and control) communicates with staff performing distributed control actions to ensure and verify that actions are taken Procedures and Training: • Procedural reminders are provided for control actions to reduce distraction • All steps of control actions are covered in JPMs/simulator training

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
Examples (continued) PWR: Maintain long-term AFW control (vs. start AFW).	HMI: Parameters to be controlled are presented poorly or poorly annunciated (if at all)	Procedures and Training: • Procedure steps include specific parameter indications for reminders and actions • Training includes time at mockup or actual RSDP or local stations with highlighting of parameter presentation
Capability of RSDP (whether or not indications or controls needed are on the RSDP or whether operators need to access multiple plant areas, instead) Examples BWR: For starting the RHR pumps in shutdown cooling, the procedures direct the operators to flush the system to prevent voiding. The system is flushed by listening for water flow through pipes at multiple locations. The RHR pumps can be started at the RSDP. PWR: Starting Charging vs. another low pressure injection (LPI) system	HMI: Layout and/or controls/annunciators on RSDP differ significantly from MCR	Procedures and Training: • Procedural direction and/or training notes that prepare operators for the differences between the RSDP and MCR capabilities and highlight the need to access local stations for information
	Complexity: • Not all functions can be performed at the RSDP and therefore operators must travel to and perform actions away from the RSDP • Multiple actions required in parallel at multiple locations	Timing: • With enough time, any number of actions can be completed. A greater time margin can offset the multiple actions at multiple locations Crew Dynamics/Command and Control: • Clear coordination plan is in place that involves communication of action completion OR • Actions are independent and do not require significant coordination or associated communication for successful performance Cues and Indications, HMI: • Action locations have all of the necessary cues/indications and controls needed for successful performance

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
LOC, especially the decision to abandon	Cues and Indications: "Soft cues" such as spurious cycling of plant equipment due to fire damage or unreliable indications may not be sufficient to trigger the need to abandon	Procedures and Training: • Guidance related to the inability to operate equipment from the MCB, visible MCB panel damage, loss of indications, or spurious equipment operation and a fire of such a nature that there is concern about maintaining the ability to safely control the plant
	Timing: The less time available for recovery, the lower the reliability	Procedures and Training: • Clear (unambiguous) direction in procedure Timed training runs (e.g., JPMs) with emphasis on when the decision to abandon needs to be made
	Procedures: Fire-damage-related conditions that would result in the Shift Manager/Shift Supervisor calling for MCRA are not well specified in the procedure	Training: • Guidance is provided during training (as identified through operator interviews) that gives operators a basis for determining how the procedures are interpreted and implemented in making the decision to abandon (e.g., loss of certain equipment, indications, or some combination thereof)
	Staffing: Culture of the operating crew may impact the decision to abandon (e.g., would such a decision be made in an "executive" fashion by the Shift Manager, would they consult with one or more senior operations staff or managers, or would the decision be more of a consensus process)	Procedures and Training: • The person who has the authority to make the decision to abandon is clearly identified in procedures and training

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
Reliance of skill-of-craft actions	Procedures and Training: Procedural direction limited, requiring reliance on skill-of-craft actions.	Procedures and Training: • Lack of detailed procedure steps may be offset by skill-of-the-craft if (a) cue for action is prioritized through procedures and training and (b) training quality and frequency and/or experience exists and has been demonstrated Cues and Indications: • Cue for action is clear and distinct
Multi-unit site	HMI: Different RSDP and local interfaces for the different unit(s)	Procedures and Training: • For sharing of staff across units, training involves time at the other unit's RSDP
	Staffing: More personnel to coordinate for an already complex scenario can lead to confusion about roles and tasks	Procedures and Training: • Procedures and/or plans include clear direction of the unit in charge given the impacted unit and staff responsibilities • Multi-unit staffing and responsibilities are clearly covered in training (as indicated by operations and training responses to interview questions)
Other concurrent effects/ special conditions in addition to fire, e.g., SBO resulting in additional Phase III actions for EDG start and associated bus load stripping <u>Examples</u> BWR and PWR:	Workload, Pressure and Stress: Concurrent effects typically result in high workload for the operators because these scenarios usually require the use of multiple procedures Cues and Indications: SBO impacts instrumentation availability	Procedures and Training: • Procedure provides alternative indications and warnings of indication impacts in case of SBO • Training includes time at mockup or actual RSDP or local stations highlighting parameter fidelity in case of SBO
	Workload, Pressure and Stress: Multiple actions need to be performed within a specific timeframe	Procedures and Training: • Procedural reminders for control actions • All steps of control actions are covered in JPMs/simulator training

Table 8-1 (continued)
Potential PSF impacts given specific scenario characteristics

Scenario Characteristics	Detracting PSFs	Potential Compensating PSFs
Examples (continued) Fire causes MCRA with SBO, Transient, LOCA, LOOP, or RCP seal LOCA (PWR only)	HMI: These scenarios could require manipulation of equipment that is not frequently trained upon or not manipulated frequently. The HMI for components may not be ideal. For example, breaker cabinet labeling could be similar for all breakers and could cause confusion about which breakers to manipulate	Procedures and Training: • All steps of control actions are covered in JPMs/simulator training to provide familiarity with tasks • Actions are similar to non-MCRA SBO actions that are trained upon more frequently
	Environment: These scenarios may result in less than ideal environmental conditions such as lack of normal lighting, high radiation areas, or high temperatures	Special Equipment: • Emergency and portable lighting is available at specified locations • Procedures and Training: High radiation or temperature environmental conditions may be addressed in procedural warnings or during training
	Staffing: Staff may have multiple tasks to perform, may not be available to perform required actions concurrently, and may need to sequence/prioritize actions	Procedures and Training: • Plan for MCRA covers allocation of staff to ensure requirements are met
	Communications: Operators must relay information on status of task(s) from additional field locations	Crew Dynamics/Command and Control: • Plan in place for supervisory monitoring and control of communication and coordination

Table 8-2
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Potential Offsetting Factors
Procedures and Training	Do not exist	Potentially insufficient guidance for required action(s)	If risk significant, consider procedure modification	Training/experience/ procedure modification
	Do not match situation	Inappropriate guidance for required action(s)		Training/experience/ procedure modification
	Take too long to execute versus time constraints	• Nice to have vs. must do actions	Depends on scenario timing	See Timing
	Insufficient or inadequate training	• Classroom vs. realistic training (communications) • Integrated training (field operators and communications included) • Security drills	If scenario involves coordination of multiple operators and communications, training should cover it	• Simplicity of action • Strong supervision • Skill-of-the-craft • General training
	Poorly worded	• Procedure not entered • Procedure not executed • Insufficient level of detail • Confusing path to/ through attachments	If risk significant, consider procedure modification	• Simplicity of action • Strong supervision • Skill-of-the-craft • General training

Table 8-2 (continued)
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Potential Offsetting Factors
Cues and Indications	Ambiguous	Event parameters inconsistent with designof indications		• Simplicity of action • Strong supervision • Skill-of-the-craft • General training • Clear procedural directions
	Spurious indications	Fire-induced effects		• General training • Specific training • Clear procedural direction of indications impacted or not impacted by fire
	Located in hard-to-see locations (also HMI)	HMI issues at plant area or RSDP		• Strong supervision • Skill-of-the-craft • General training • Specific training
	Absent	HMI issues at plant area or RSDP		• Strong supervision • Skill-of-the-craft • General training • Specific training • Clear procedural directions

Table 8-2 (continued)
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Potential Offsetting Factors
Complexity	Need for challenging calculations or complex control actions	• Coordination between fire procedures, AOPs and EOPs • Exacerbated by high workload		• Strong supervision • Skill-of-the-craft • General training • Specific training • Clear procedural directions
	Coordination and communications at multiple work locations			• Strong supervision • Skill-of-the-craft • General training • Specific training • Clear procedural directions
Workload, Pressure, and Stress	Number of tasks is inconsistent with time available	Cannot complete actions in time	Should have been evaluated via JPMs and simulator exercises for MCRA training, but these may not have included time required for LOC cognitive portion	• Nice to do" actions that can be removed • Procedure modifications that can be made • Physical modifications that can be installed
HMI	Capabilities of RSDP do not match MCRA tasks required	Requires local checking or manipulation	Should have been evaluated during MCRA training sessions	• Physical plant modification of alternate cable routing to make action feasible on RSDP • Alternative local action(s)

Table 8-2 (continued)
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Potential Offsetting Factors
Environment	Fire is in work area itself		Not usually an issue for MCRA, but should be checked; if so, HEP is set to 1.0 for that fire area	• Physical plant modification of alternate cable runs to make action feasible • Alternative action in accessible area
	Heat or high radiation conditions exist			Limit time the worker can be in the area (per health physics determination)
	Poor lighting			• Emergency lights available where needed • Use of flashlights or headlamps
	High noise	Interferes with communications and attention to alarms		• Ear protection for the worker • Alternate forms of communication
Special Equipment	SCBA required	Limitations on visibility, movement, time to implement task		Additional staff available to take over task
	Tools required	Stored in lockers and regularly maintained/put back (usually a process/procedure for this)		Communicate need for tool
	Keys required	Security access requirements and location of keys (if not on belt)		Notify supervisor who in turn calls security to obtain access
Special Fitness Needs	Climbing ladders; difficult access to equipment	Impacts timing of task and reliability		Sufficient/extra time available

Table 8-2 (continued)
PSF effects explained and potential offsetting factors

PSF	Consequential When…	Reasons Why	Scenario-Specific Influences	Potential Offsetting Factors
Crew Staffing/Availability	Crew diverted to fire brigade	Not usually an issue for MCRA, but should be checked		• Emergency planning (prior preparation for number of staff needed) • Sufficient/extra time available
Communications	Radios do not function properly in task areas	No diversity or functionality of communication systems (should be a procedure for this)		Emergency planning (prior preparation for communication needed)
	Protocols for communication are not used	Procedural direction/confirmation or other instructions not clear/verified		Strong supervision
Timing	Time required > time available	Could be infeasible	Look at JPMs and simulator exercises for MCRA training	• "Nice to do" actions that can be removed or moved to end of procedure • Procedure modifications that can be made • Physical modifications that can be installed
	No clear cues for abandonment	Requires additional diagnosis and decision-making time		LOH cues are clear; LOC can be identified through discussions with operations and insights from fire PRA and fed into procedure

8.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. U.S. Nuclear Regulatory Commission. NUREG-2114, *Cognitive Basis for Human Reliability Analysis.* Washington, D.C.: January 2016.
3. 10 CFR Part 50, Appendix R, Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979.
4. U.S. Nuclear Regulatory Commission. NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, Washington, D.C. October 2007.
5. U.S. Nuclear Regulatory Commission. NUREG-0700, Revision 2, *Human-System Interface Design Review Guidelines*, Rockville, MD: 2002.
6. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment.* EPRI. Palo Alto, CA: 1992. TR-100259.
7. U.S. Nuclear Regulatory Commission. NUREG-1624, Rev. 1, *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA*), Washington, D.C. May 2000.
8. U.S. Nuclear Regulatory Commission. NUREG-1880, *ATHEANA User's Guide,* Washington, D.C. June 2007.

9
RECOVERY, DEPENDENCY, AND UNCERTAINTY

9.1 Introduction

This section provides guidance on recovery, dependency, and uncertainty for MCRA scenarios. The fundamentals of each of these steps in the HRA process are not unique to fire HRA or MCRA HRA.

9.2 Recovery

This section re-states the definition of recovery provided in NUREG-1921 [1], shows how that definition applies to MCRA, and then summarizes changes since NUREG-1921.

NUREG-1921 cites the following definition for a *recovery human failure event*: “the failure to restore failed equipment or find alternative equipment or configurations within the time period required” [1].[36] NUREG-1921 also states, “After the initial fire PRA model quantification, recovery actions may be identified to restore or reconfigure a function, system, or component initially unavailable in the scenario. Accounting for such a recovery would reduce the frequency of the scenario.” Therefore, the recovery actions considered in NUREG-1921 are typically those that were not initially incorporated to the PRA model as part of the initial, planned plant response. Instead, these actions are added to the PRA model logic at the sequence or cutset level to realign the affected system or to provide an alternative system, such that success of these actions would have prevented core damage and/or large early release. This may be done by adding additional logic to the PRA model or by applying post-processing rules.

For MCRA, recovery opportunities within an HFE (i.e., not the traditionally defined 'PRA recovery') need additional consideration. Recovery opportunities of this type following MCRA are often limited to self-check or peer check by others directly involved in the action; for example, when operators are distributed between multiple locations (rather than co-located in the MCR). This will depend upon the structure of the procedure and the capabilities of the remote shutdown command and control location. When an action takes place at this command and control location, additional co-located staff would have the ability to provide a peer check just as they would in the MCR, and the peer check could be credited in a similar fashion. When an action takes place in another location, the availability of a peer check would be the same as a local action when command and control remains in the MCR. A remote action could be confirmed by local indication or through communication from the local operator to the RSDP based on the indications there. Such opportunities for HRA recovery though peer checking are generally treated with considerations for dependencies. This is addressed further in Section 9.3.

[36] This definition of recovery, which has been in common use in PRA for many years, is ***not*** to be confused with the definition of “recovery action” used in NFPA 805.

During MCRA, the “initial, planned plant response” is the alternate shutdown procedure (the MCRA procedure). Typically, this procedure was developed assuming one train of equipment was failed by the fire. Since many of the U.S. plants only have two electrical trains, this means the alternate shutdown procedure is using the one remaining train - such that there are typically no options for recovery. However, some of the MCRA scenarios may have long time windows that could allow consideration of additional staff and additional recovery options that may be available for use during MCRA, such as actions in the Extensive Damage Mitigation Guidelines (EDMG) procedures.

For example, since publication of NUREG-1921, consideration of FLEX and Severe Accident Management Guidelines (SAMG[37]) in PRA models is being discussed. Historically, actions proceduralized in FLEX and SAMG (or EDGMs) have not been credited as recovery actions in internal events PRAs due to the lack of proceduralized links to these procedures (as well as potentially poor or insufficient cues, training, procedure quality). The scope of this project did not include consideration of actions located in FLEX, SAMG, and/or EDGM procedures. Recovery actions based on FLEX and SAMG procedures has been left to future evaluation and consideration.

9.3 Dependency Analysis

The ASME/ANS PRA Standard [2] requires that multiple operator actions in the same accident sequence or cutset be identified, an assessment of the degree of dependency performed, and a joint HEP be calculated, if a dependency exists. This requirement focuses upon the quantitative aspects of dependency, but the underlying qualitative dependency must also be evaluated.

One way in which dependency is qualitatively addressed for MCRA is through the development of the MCRA timeline, as discussed in Section 7. This process ensures that the timing of individual MCRA operator actions that model the critical MCRA tasks are correlated to each other and that the combined set of actions is feasible within the total timeframe available to bring the plant to a safe, stable condition.

The dependency analysis should consider all three phases of the timeline. Generally, there are only a few actions in Phase I that are feasible so the dependency among Phase I actions is limited. Typically, Phase II is modeled as a single operator action that, if failed, would lead to core damage. There is potential for the Phase II action to be highly, if not completely, dependent on Phase I actions. Phase III actions are only required given that the decision to abandon was successful. The time for the decision to abandon should account for the time required to perform Phase III actions and therefore no additional dependency considerations between Phase II and Phase III are required. Any failed action in Phase I can be considered independent of any Phase III action because the crew has successfully abandoned in time. For Phase III actions, all dependency considerations described in NUREG-1921 are applicable, as well as consideration of coordination and communication.

[37] Note that SAMG actions will not actually result in an alternate success path for MCRA since they do not prevent core damage. However, they may be effective in reducing the risk of a large early release.

Another facet of dependency is the treatment of recovery opportunities within an action, as mentioned in Section 9.2. Self-checking and peer checking recovery actions reflect an implicit amount of dependence between the initial cognition or execution failure and the checking action(s) that can reduce the likelihood of the initial error. The dependency level between the initial and recovery actions is assessed qualitatively according to a scale from zero to complete dependency (see discussion above Figure 9-1) and is ultimately translated into quantitative dependence that modifies the substep probabilities within an HFE. There are unique considerations for the MCRA case in this type of dependency, for example, the extent to which self-check and extra crew checking apply to cognitive decisions that occur after leaving the MCR and to the degree to which peer checking can be credited when everything is occurring through communications between local stations. Some specific considerations are:

- Where is the action being performed? Is it within the capability of the panels at the command and control (C&C) location? The dependency model for recovery within a HFE taken solely at this location would be similar to one taken in the MCR, while one taken elsewhere would be modeled like actions taken outside the MCR.
- How many people (and who) are at the C&C location? This goes to whether credit can be given to extra staff and/or STA.
- What indications are available at the C&C location to achieve recovery? This relates the extent of credit (dependency level to assign) for self-check, extra staff, and/or STA. The ability to check the success of the action may be less at the C&C location than in the MCR because of fewer parameters being available.
- For actions that take place away from the C&C location, the direct indications of success may only be at the location where the action takes place, thus limiting initial recovery to self-check. Whether a subsequent recovery is possible within the available timeframe would depend on whether a secondary indication is available and whether it is timely.[38]

Another way in which dependency analysis is evaluated for MCRA is through the decision-making by the HRA analyst on the definition of HFEs, as discussed in Section 5 on Identification and Definition. The HFE definition for MCRA depends, in large part, upon how the procedures are organized and implemented as well as the overall modeling strategy in the fire PRA.

If the HEPs for individual operator actions, including the decision to abandon, are combined together into a single MCRA HFE/HEP to be included in the fire PRA model (as described in Section 3.7), then the dependency between the individual actions should be appropriately accounted for in the logic and data associated with that single HFE/HEP.

[38] For example, take the case when of an AFW pump that needs to be started at a local station. Flow indication is only available at the local station. The C&C location only has SG level. Initially only a self-check would be possible to confirm flow. If an error is made, eventually the lack of flow would be checked at the C&C location because the SG level would not be coming up. This may provide a second opportunity for recovery, if this conclusion could be reached soon enough. The analyst would then need to assign an appropriate dependency level.

However, if separate HFEs are defined for the MCRA actions, then the interdependencies between the MCRA HFEs may need to be assessed as described in NUREG-1921. In many cases of MCRA modeling in the PRA, each of the defined HFEs will lead to a failure of MCRA (i.e., all the modeled actions must be successful in order for MCRA to be successful). This is because the limited set of equipment used in the MCRA procedures provides only one path to success. In this case, there will be at most one MCRA HFE in a cutset and so there would be no dependencies to be addressed.

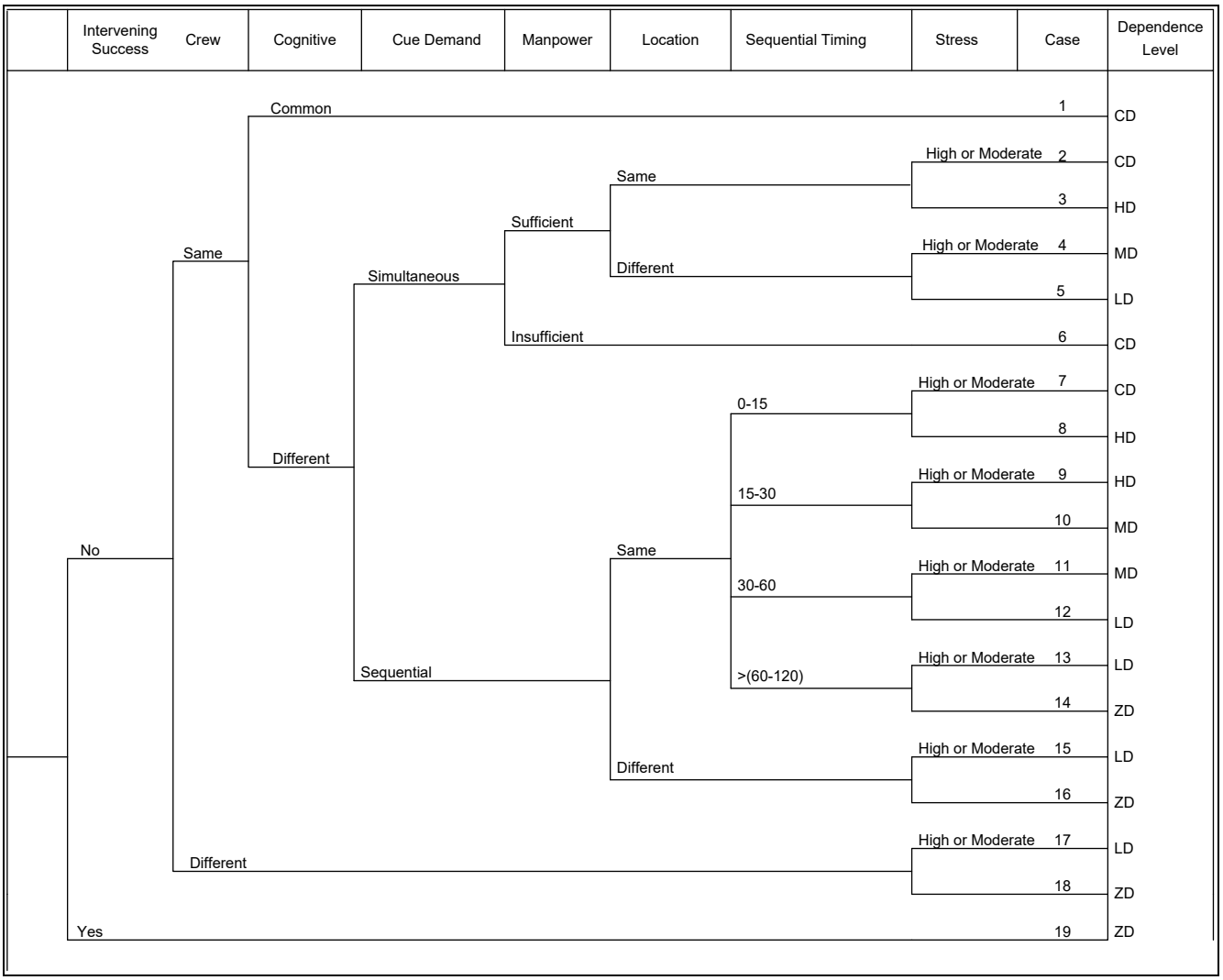
There are, however, some examples where cutsets contain multiple HFEs that will need to be considered. Once such example is for a BWR: operator failure to start RCIC and failure to emergency depressurize to enable low pressure injection. In this scenario, the analyst will need to account for dependencies since the shift supervisor may want to delay depressurization as long as possible because he believes RCIC is about to be started.

The individual HFEs can be defined from a functional or an operator action standpoint. In the functional case, multiple operators can be working together to restore a function and the relevant tasks performed by the various operators may be embedded in a single HFE. The HRA analyst must determine whether the timing of the single functional HFE covers the time required to perform all of the embedded tasks necessary to restore the function. This is a similar evaluation as for the MCRA timeline, but it is done on an individual HFE basis. Timing for these evaluations generally comes from thermal-hydraulic analyses for the overall time available (T_{SW}) and from simulator data or training walk-throughs for the task performance timing. This is a form of dependency analysis since it addresses dependency within an HFE, but does not address the interdependencies between the various MCRA HFEs that collectively restore all the necessary functions.

In the operator action case, individual HFEs are defined for different operator actions, such as when Operator A takes Attachment A of the MCRA procedure and performs those actions independently and Operator B does the same with Attachment B. The MCRA timeline is used to evaluate whether all the operator actions can be performed in time, but again, does not address other interdependencies between the operator actions.

The various ways in which MCRA is modeled in the fire PRA are discussed in Section 3 and the identification and definition of HFEs for MCRA is discussed in Section 5. In general, when individual HFEs, whether defined by function or operator action, are included in the MCRA portion of the model, the solution of the PRA model may result in cutsets or accident sequences that depend on multiple HFEs. The dependency between these multiple HFEs must be reviewed and assessed, consistent with the process followed for internal events or fire HRA, as discussed in NUREG-1921 and demonstrated in Figure 9-1. Additionally, Chapter 3 of EPRI 3002003150 [3] provides additional detailed guidance on the EPRI dependency approach and Figure 9-1. The dependence levels shown in the far right column (ZD for zero dependency, LD for low dependency, MD for medium or moderate dependency, HD for high dependency and CD for complete dependency) ultimately correlate to a quantitative process to ensure that the multiplication of multiple HFEs in a cutset does not result in a lower than credible combined human error probability.

The dependency decision tree shown in Figure 9-1 was designed to be a conservative first approach to assessing the dependency levels. Since MCRA scenarios involve significant communication and simultaneous actions, using the tree may result in an initial assessment of complete dependency. In many cases, however, scenario specific inputs can be used to justify a level of dependency lower than what is explicitly given by the dependency tree.



*Note: The units of the “Sequential Timing” branch are in minutes.

Figure 9-1
Dependency rules for post-initiator HFEs

9.4 Uncertainty

The ASME/ANS PRA Standard [2] supporting requirement HR-G8 directs the analyst to use mean values for quantification of HEPs and their associated uncertainty in the risk analysis. However, this does not provide much insight into the evaluation of the uncertainty of qualitative analyses for HRA.

Since the publication of NUREG-1921 in July 2012, subsequent technical reports have been issued by the U.S. NRC and EPRI that provide guidance for evaluating uncertainty in PRA. NUREG-1855, Revision 1 [4], provides guidance on how to treat uncertainties associated with PRAs used by a licensee or applicant to support a risk-informed application to the NRC. EPRI 1016737 [5] and EPRI 1026511 [6] provide guidance on identifying and characterizing sources of model uncertainty in PRA models, the former for internal events and internal flood hazards, and the latter for the internal fire hazard, seismic hazard, low-power and shutdown operational modes, and Level 2 PRA.

These documents first define the various types of uncertainty and then provide guidance for addressing them.

9.4.1 Types of Uncertainty

NUREG-1855, Revision 1 [4] provides the following overview of the types of uncertainty that are examined in PRA:

> "Generally speaking, there are two main types of uncertainty; aleatory and epistemic.
>
> - Aleatory uncertainty is based on the randomness of the nature of the events or phenomena and cannot be reduced by increasing the analyst's knowledge of the systems being modeled. Therefore, it is also known as random uncertainty or stochastic uncertainty.
> - Epistemic uncertainty is the uncertainty related to the lack of knowledge about or confidence in the system or model and is also known as state-of-knowledge uncertainty.
>
> PRA models explicitly address aleatory uncertainty, which results from the randomness associated with the events in the model logic structure. The random occurrence of different initiating events with subsequent failure of components to operate and human errors lead to a large number of possible accident sequences that are accounted for in the event and fault trees used in a PRA model. The results of the PRA model evaluation (accident sequences and cut sets) represent aleatory uncertainty.
>
> Note that the exclusion of initiating events, hazards, accident sequences, systems, components, or cutsets from the PRA model results in epistemic uncertainty (i.e., in model uncertainty), and is not a contributor to the aleatory uncertainty.
>
> The different types of epistemic uncertainty are completeness, parameter, and model uncertainty."

These three types of epistemic were defined as follows in the original version of NUREG-1855 [7]:

- **Completeness Uncertainty** – "relates to contributions to risk that have been excluded from the PRA model. This class of uncertainties may have a significant impact on the predictions of the PRA model and must be addressed. Examples of sources of incompleteness include the following:
  - The scope of the PRA does not include some class of initiating events, hazards, or modes of operation.
  - There is no agreement on how the PRA should address certain elements, such as the effects on risk resulting from aging or organizational factors.
  - The analysis may have omitted phenomena, failure mechanisms, or other factors because their relative contribution is believed to be negligible."
- **Parameter Uncertainty** – "relates to the uncertainty in the computation of the parameter values for initiating event frequencies, component failure probabilities, and human error probabilities that are used in the quantification process of the PRA model."
- **Model Uncertainty** – "relates to the uncertainty in the assumptions made in the analysis and the models used…In general, model uncertainties are addressed by studies to determine the sensitivity of the results of the analysis if different assumptions are made or different models are used."

9.4.2 Relationship of Uncertainty Types to MCRA Qualitative Analysis

Each of the three types of epistemic uncertainty are discussed below in terms of their relevance to this report's mission of addressing qualitative analysis for MCRA. Input to this section was provided from presentations and discussions at the joint NRC – EPRI workshop on the treatment of uncertainty in risk-informed decision-making [8, 9] held in November 2015.

Completeness Uncertainty

This category of uncertainty refers to items not included in the PRA model, which can be defined as [9]:

- Those known not to be in the model, e.g., excluded systems or equipment
- Those not in the model because they are not known, e.g., effects of unknown failure mechanisms

For those items that are known to not be included in the model, the guidance from NUREG-1855, Rev. 1 [3] states that it is the responsibility of the analyst to determine the risk significance of a missing scope or PRA item by performing a screening analysis to demonstrate that the non-modeled item can be eliminated from further consideration.

Since this report focuses on the qualitative analysis of MCRA, the screening discussed here is based on the qualitative assessment of relevance.

The qualitative criteria for identifying MCRA relevant HRA scenarios will be consistent with the scope of the fire modeling and PRA modeling tasks, as discussed in Section 3. In particular, Figure 3-1 shows where the guidance for the MCRA fire scenario selection/plant response modeling and HRA fits within Task 11 of NUREG/CR-6850 [10], NUREG-1921 and this report.

Regarding the “unknown unknowns,” these are beyond the capability of the qualitative analysis and are assumed to be addressed via other principles of risk-informed decision-making [9]:

- Defense-in-depth
- Safety margins
- Performance monitoring

Parameter Uncertainty

Since this category is concerned with uncertainty in the computation of the parameter values used in quantification, such as the HEPs used to quantify individual HFEs in an MCRA scenario, it is beyond the scope of this report. However, the assumptions involved in evaluating and estimating the inputs to the calculation of these parameter values, such as timing and PSFs, are part of the qualitative analysis described in other sections of this report. These assumptions should therefore be clearly documented and may be challenged once quantitative results are obtained.

Table 9-1 lists potential sources of parameter uncertainty related to MCRA.

Model Uncertainty

The PRA standard defines a source of model uncertainty as:

> “a source is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event). A source of model uncertainty is labeled “key” when it could impact the PRA results that are being used in a decision, and consequently, may influence the decision being made. Therefore, a key source of model uncertainty is identified in the context of an application.”

Appendix A of EPRI 1016737 [5] provides tables of potential generic sources of model uncertainty for internal events, while Appendix B, Table B-1 of EPRI 1026511 [6] provides a table of potential sources of model uncertainty for fire HRA.

Table 9-1 lists the generic potential sources of MCRA HRA uncertainty. The sources of parameter uncertainty are MCRA-specific based on the experience of the team. Table 6-2 of NUREG-1921 [1] lists potential sources of fire HRA uncertainty based on fire HRA experience and results. This table should be reviewed for relevancy to MCRA.

Table 9-1
Potential sources of uncertainty for MCRA HRA

Category	Potential Sources of MCRA HRA Uncertainty
Parameter Uncertainty	
Timing[39]	Operator action modeling such as timing for decision-making or execution (e.g., limited input from operators).
	Impact of timing variability on short or constrained timeframe events.
	Degree of difficulty and complexity in performing ex-control room actions.
	What to do with varying or conflicting operator input.
Communications	Availability and effectiveness of back-up communication systems.
	Command and control related communication.
Training	Effectiveness for the collective set of MCRA actions.
Procedures	Impact of unclear cues or direction in procedures.
	MCRA procedures not in an industry standard format (like EOPs).
Cues	Impact on cues such that the indications may not be accurate.
	Compelling indications or cues that may distract the operator from the modeled task.
Model Uncertainty	
Generic HRA (from Table A-4 of EPRI 1016737 [5])	
HFE Delineation	The discrimination of those HFEs that are to be modeled and the conditions under which they are characterized. There are hundreds of individual HFEs that could be modeled. Of these, there are HFEs that are screened or subsumed into larger groups. The larger group of HFEs is then represented by a single set of limiting conditions. MCRA relevance: definition of individual HFEs in a scenario.
HFE Applicability	The HFE application to specific circumstances within the accident sequence may be constrained in different ways for different applications. MCRA relevance: applicability of individual HFEs to different scenarios and the definition of scenario bins.

[39] Section 7.7 provides additional discussion of uncertainties associated with the timing inputs used in MCRA HRA.

Table 9-1 (continued)
Potential sources of uncertainty for MCRA HRA

Category	Potential Sources of MCRA HRA Uncertainty
Model Uncertainty (continued)	
Scenario-dependent recovery and repair	The accident sequence level of discrimination with regard to plant conditions, timing, operator interface, and use of non-safety systems. The finite nature of the level of delineation collapses the continuum of possible sequences to a limited set. Repair and recovery of failures is an area of significant judgment in the PRA model. It involves the designation of sufficient time, access, personnel, and guidance to either recovery (manual action) or repair of a failed SSC. MCRA relevance: definition of individual HFEs in a scenario based on procedure steps and equipment interfaces.
Organizational interfaces	The plant-specific organization during an event may be difficult to capture in the HRA and may strongly depend on the personalities involved, including: • Operations-Maintenance • Staff-Management • Control Room-TSC • Ex-Plant (for example, grid operator) MCRA relevance: command and control
Errors of commission	MCRA relevance: • Failure to make decision to abandon in time • Failure to implement necessary systems and functions in time to prevent core damage
Procedural changes (permanent and temporary)	MCRA relevance: consideration of re-ordering or further clarification of MCRA procedure steps to improve operator action feasibility.
Human performance impact of beyond-design-basis conditions and environments (for example, steam generator tube rupture (SGTR), SBO, and ATWS)	The characterization of human performance for beyond design basis events is critical to the successful realism in a PRA. The simulator training and results from that training can support the HEP characterization. MCRA relevance: consideration of fire PRA success criteria and fire PRA scenarios applicable to MCRA.
Instrumentation response resulting in degraded information flow to crew	The crew's window on the plant comes primarily from instrumentation. Failures of instrument or degraded conditions of instrumentation may significantly alter the way the crew responds to an accident, but the level of redundancy in the instrumentation should be considered as part of the PSFs utilized in the HRA development. MCRA relevance: instrumentation issues in MCR prior to abandonment; limited instrumentation available at RSDP or local control stations.

Table 9-1 (continued)
Potential sources of uncertainty for MCRA HRA

Category	Potential Sources of MCRA HRA Uncertainty
Model Uncertainty (continued)	
Human-machine interface	There may be unique components, instruments, or controls that make plant operation, accident response, and recoveries significantly better or worse than the typical plant. These shaping factors are difficult to fully integrate into the HRA. MCRA relevance: Deficient HMI or lack of controls available at RSDP or local control stations.
Training and procedures	Training and procedures form the basis for the HRA. MCRA relevance: clarity of procedure cues for action and degree of preparation provided by training.
Multi-unit events	Multiple units may provide both significant benefit—by virtue of the sharing of equipment and personnel—and significant challenges if all units require accident mitigation simultaneously. MCRA relevance: coordination of personnel between units and staffing availability.
Crew response times	The simulator, crew input, and JPM response times are sources of information for crew response times. All sources are not consistent and can be either optimistic or pessimistic. MCRA relevance: realism of timeline(s) constructed for MCRA scenarios.
Distractions (for example, tired, problems outside of work, and so on)	The crew work schedule and individual crew member conditions are not generally included as part of the shaping factors of the HRA.
Crew turnover	Period of crew turnover and the information transmittal at crew turnover is not modeled.
Crew awareness to conditions	Training can alter crew awareness. The awareness of the crew to specific accident conditions varies with the training cycle and current industry experiences that are promulgated to the crews. MCRA relevance: training on the decision to abandon.
Circadian clock	Time of day is not generally included in the HRA despite evidence that the most serious crew errors occur between 12 midnight and 6 a.m.
Training cycle emphasis	Training can alter crew awareness. The awareness of the crew to specific accident conditions varies with the training cycle and current industry experiences that are promulgated to the crews.
	Fire HRA (from Table B-1 of EPRI 1026511 [6])
Impact of fire on HEP evaluation	The impacts of the fire need to be factored into the HFE analysis for the fire PRA model (e.g., added stress or limited accessibility for ex-control room actions). MCRA relevance: PSFs of stress, location

Table 9-1 (continued)
Potential sources of uncertainty for MCRA HRA

Category	Potential Sources of MCRA HRA Uncertainty
Model Uncertainty (continued)	
HEP Methodology	The basis for the HEP methodology utilized needs to be consistent with the internal events PRA standard requirements for HRA. MCRA relevance: quantification method selection (not in scope of current report)
Fire impacts on recovery actions	Recovery actions in the plant response model are subject to the same requirements as the internal events recovery actions. MCRA relevance: ANS/ASME PRA Standard [2] requirements for recovery actions per SR HR-H1 and HRA-E1.
Modeling of any existing or new FPRA actions including accident sequence-specific factors	Inclusion of the HFEs into the model may include modification to an accident sequence, system model, or recovery of an event. Failure to properly model the HFE impact can result in either conservatism or non-conservatism. MCRA relevance: definition of MCRA HFEs; coordination with Fire PRA PRM task (as defined by the ANS/ASME PRA Standard [2]) on how to incorporate into the fire PRA model.

9.4.3 Specific Uncertainty Issues in MCRA Qualitative Analysis

Uncertainty in the input information to HRA is generally characterized in the qualitative analysis in the form of assumptions.

Assumption is defined in the ASME/ANS PRA Standard [2] as a decision or judgment that is made in the development of the PRA model. An assumption is labeled “key” when it may influence (i.e., have the potential to change) the decision being made.

Assumptions need to be clearly stated in the documentation and can form the basis for follow-on operator interviews or modeling of fire response or thermal-hydraulics. Some examples of uncertainty-driven assumptions related to MCRA are provided in this section.

As discussed in Section 4, the conditions that lead to a LOC involve significant uncertainty, including fire-damaged cables and equipment. As a result, the timing of those fire-induced effects complicates the plant and operator response and may require assumptions on the part of the HRA analyst. An example of such an assumption that is a significant source of uncertainty is the case where the fire scenario, although eventually requiring abandonment to reach safe shutdown, is mild enough that the overall time window for the decision to abandon and subsequently perform the post-abandonment actions is relatively long. The source of uncertainty in that case is the time window for the decision to abandon, which can be interpreted as a time margin to recover from a failure to decide to abandon the MCR. If the analyst selects a relatively long time (effectively giving the operators additional time margin from the decision not to abandon), this shortens the time available in Phase III actions and may result in a higher probability of failure of those actions. Conversely, if the analyst selects a relatively short time window for the decision to abandon, there would be more time available to perform the post-abandonment actions, but the cognitive failure to abandon would have a higher probability.

The MCRA procedures themselves can be a source of uncertainty and assumptions. Section 4 has already cited the lack of specific cues for MCRA as a source of uncertainty related to the cognitive HFE for the decision to abandon. The HRA analyst must often take the lead in defining these cues, but the time required for the abandonment decision based upon these cues is still an assumption. Some NPPs choose to perform an initial MCRA analysis to gain information on the key actions and time constraints, incorporating this information in the MCRA model and decide to formally update their procedures later, stating as an assumption of the preliminary analysis that these procedure changes will have to be made at a later date.

9.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, The American Society of Mechanical Engineers, New York, NY, February 2009.
3. *A Process for HRA Dependency Analysis and Use of Minimum Values for Joint Human Error Probabilities.* EPRI, Palo Alto, CA: 2016. 3002003150.
4. U.S. Nuclear Regulatory Commission. NUREG-1855 Revision 1, *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,* Washington, D.C.: March 2017.
5. *Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessment.* EPRI, Palo Alto, CA: 2008. 1016737.
6. *Practical Guidance on the Use of PRA in Risk-Informed Applications with a Focus on the Treatment of Uncertainty.* EPRI, Palo Alto, CA: 2012. 1026511.
7. U.S. Nuclear Regulatory Commission. NUREG-1855 Revision 0, *Guidelines on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,* Washington, D.C.: March 2009.
8. Memo from A. Gilbertson to J. Nakoski, December 23, 2015, “Summary of the U.S. Nuclear Regulatory Commission and Electric Power Research Institute Co-Sponsored Workshop on the Treatment of Uncertainty in Risk-Informed Decisionmaking.” ADAMS Accession Number: ML15355A540.
9. Presentation slides, U.S. NRC and EPRI Workshop on the Treatment of Uncertainties in Risk-Informed Decision-Making, November 18-19th, 2015. ADAMS Accession Number: ML15327A182.
10. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities: Volume 2: Detailed Methodology*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.

10
CONCLUDING REMARKS

10.1 Introduction

This section highlights lessons learned and experience gained from the development of qualitative analysis guidance to support fire scenarios that may result in MCRA. This section also describes good practices for MCRA modeling and HRA, and the type of interface that should be conducted with plant operations personnel during the MCRA HRA qualitative analysis process.

Within this section, discussion is provided on the requirements for MCRA HRA from the ASME/ANS PRA Standard [1], with particular emphasis on documentation of the analysis. Finally, it presents a summary of the high-level conclusions from the development, and lists areas identified for future development.

10.2 Properties of a Good Qualitative Analysis

As noted throughout this report, MCRA is a unique case of fire HRA. The definition of fire-related damage criteria leading to abandonment, crew structure outside the MCR, and the coordination of many overlapping timeframes and actions necessitate a solid qualitative analysis to ultimately support quantification of HFEs. The facets of a good qualitative analysis include:

- Collection and review of plant-specific information for MCRA including:
  - MCRA procedure
  - Fire-induced risk model (fire PRA)
  - Fire PRA success criteria
  - Fire modeling
  - Available feasibility studies (such as from Appendix R evaluations)
- Coordination with the fire modeling task to define the criteria for MCRA on LOH
- Defining the criteria for MCRA on LOC
  - What are the key safety functions that will determine whether the operators need to abandon the MCR due to LOC?
  - Which systems provide or backup the key safety functions lost during a fire that leads to MCRA?
  - Which systems need to be enabled or recovered to provide or restore the key safety functions?

- Coordination with the fire PRA analysts to identify relevant MCRA scenarios, including consideration of the decision to abandon and proper treatment within those scenarios based on different functional requirements
- Review of each MCRA procedure step to determine critical tasks required to meet the fire PRA success criteria
- Conducting plant-specific walk-throughs and talk-throughs of the MCRA procedure at the plant locations where the actions occur and observation of simulator exercises of the MCRA strategy (if possible)
- Development of a timeline for the MCRA strategy based on walk/talk-throughs, simulator exercises of the MCRA strategy, timed training materials, and thermal-hydraulics analyses
- Identifying and defining HFEs based on the relevant MCRA procedure steps and the context of the fire PRA scenarios for MCRA
- Feasibility assessment for MCRA scenarios as well as individual operator actions
- Evaluation of HFE-specific PSFs based on the context of the fire scenarios for MCRA and other influences on operator performance observed during walk/talk-throughs and simulator exercises of the MCRA strategy
- Assessment of C&C in terms of existing plans, training, and communication requirements
- Dependency analysis –consideration of HFEs that occur in the same cutsets
- Assessment of uncertainty
- Documenting the analysis in sufficient detail to allow the basis for the qualitative analysis to be understood and the input parameters to quantification to be clearly identified

Further discussion on documentation is provided in Section 10.6.

10.3 MCRA Modeling and HRA Checklists

Earlier guidance provided in NUREG/CR-6850 [2] and even NUREG-1921 [3] may not have provided an adequate level of detail in order to consistently and properly model the relationships and elements commonly found in MCRA. The checklists in this section serve as a high level reminder of the elements to consider in the MCRA PRA modeling and the HRA process.

10.3.1 MCRA Modeling Checklist

1. Based on fire-induced damage, HRA operator interviews, and procedure review, the analyst should define the plant conditions that would constitute a LOC for the plant and include appropriate logic in the model to credit abandonment only when those conditions occur.
2. Based on the fire modeling for fires that may cause visibility or temperature concerns in the MCR, the analyst should determine the scenarios that would result in a LOH.
3. The analyst should include random failures of equipment required for remote shutdown (including the controls located at the remote shutdown panel) in the PRA model.

4. The analyst should include recoverable fire-induced failures of equipment required for remote shutdown (including the controls located at the RSDP) in the PRA model. This requires analyzing the circuits[40] of the RSDP and control circuits to determine if any abandonment scenarios can cause failure of this equipment.
5. The analyst should include non-recoverable fire-induced failures of equipment required for remote shutdown in the model. These would include MSOs that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed, etc.).
6. For scenarios modeled with detailed fire modeling, the analyst should account for detection and suppression.

10.3.2 MCRA HRA Checklist

1. **Perform feasibility assessment for each MCRA scenario modeled in the fire PRA.** This assessment includes showing that the hardware needed to establish a safe, stable state is available and that the operators can perform all required actions within the available time.
2. **Identify HFEs.** This task starts with the current abandonment procedure(s) to identify the shutdown strategy following the decision to abandon. This procedure review should be done in conjunction with the review of the fire modeling for MCRA scenarios. It should be recognized early on in the MCRA analysis that the shutdown strategy may need to be revised. If possible, the analyst should involve the procedure writer.

   The HRA should identify and define three sets of actions:

   a. Actions required before the decision to abandon has been made,
   b. Actions related to the decision to abandon for LOC scenarios, and
   c. Actions taken after the decision to abandon has been made. This includes any long-term control actions.
3. **Perform operator interviews and walk-throughs.** To start the MCRA HRA, walk-throughs and talk-throughs should be performed so that all parties involved can develop an understanding of the plant-specific RSDP displays, capabilities, and limitations. This should include physically walking down the RSDP and the locations of other local actions. Additional interviews and walk-throughs should be conducted throughout the MCRA process as further clarification is needed to refine the analysis. For example, interviews provide input to the following aspects of the qualitative analysis:

   a. Timeline development
   b. Modeling the decision to abandon for LOC scenarios
   c. Verification of feasibility

[40] In a manner that meets the supporting requirements of the ASME/ANS PRA Standard.

   d. Discussions on how command and control is maintained following MCRA
   e. Discussions on the coordination and communications conducted between operators for the three MCR time phases, including addressing how requests and communications from personnel not involved with key safety functions are managed

4. **Feasibility assessment of HFEs.** The analyst should perform a feasibility assessment of individual HFEs and the collective set of operator actions. In addition, the analyst should review the feasibility items in NUREG-1921 [3] and NUREG-1852 [4] and ensure that these issues have been addressed in the HRA, both qualitatively and quantitatively, such as emergency or normal lighting, keys and tools needed (and the time required to acquire them), and SCBA usage.
5. **Timeline development.** The analyst should develop a timeline for each MCRA scenario and individual actions. The timeline should include timing associated with the decision to abandon.
6. **Documentation.** The analyst should thoroughly document in the HRA notebook/report on MCRA the interview findings, cues, assumptions, and timing. In addition, the analyst should augment this documentation, as necessary, with interview notes and photos.
7. **Maintain coordination among different organizations, including PRA, HRA, and plant operations.** In particular, the analyst should:
   a. Work closely with operations and training to walk- and talk-through the MCRA procedure to identify the actions that are essential for safe, stable end state rather than those that are just “nice to do if you have time.” It is important to get “buy-in” from operations regarding the MCRA modeling strategy (this has sometimes been met with resistance and may require some discussion about the PRA perspective).
   b. Consistent with items above, plant operations staff and the fire PRA analysts need to agree on the fire-damage-related conditions that would result in the Shift Manager/Shift Supervisor calling for MCRA. This is often not well specified in the procedure but is needed to model the scenario(s) properly, identify relevant fire compartments and equipment impacted, and to determine the crux of the cognitive abandonment decision. (Note these conditions can be incorporated into the MCRA procedure to provide more distinct entry criteria.)

10.4 Interface with Operations

The success of an MCRA HRA is, in large part, dependent upon gathering plant-specific information from operations and training staff. These plant personnel are the ones who are directly informed of and involved with the structure and implementation of the MCRA procedure, the associated training process, and the capabilities of the RSDP(s). The HRA analyst needs to have a good knowledge base and understanding prior to meeting with operations to make the most effective use of their time. Appendix C provides guidance and tips for the MCRA-related information collection and the preparation process for the analyst.

The information sharing is a two-way street, however, since the findings from the analysis can be fed back into operations, training, or even design to enhance the feasibility and improve the reliability of the MCRA strategy. The following subsections discuss the various forms this interface with operations can take.

10.4.1 PRA Perspective

Nuclear plant operations staff have extensive knowledge of systems, training, and procedures, as well as a discipline that enables them to tackle situations that others, who are not in that field, would consider overly challenging and stressful. As such, their ability to provide information on response to accident scenarios is of great value to an HRA. The impacts due to fire effects postulated in MCRA scenarios are unique and severe. This can lead to specific challenges, to both the operators and the HRA analysts, in understanding and communicating the MCRA scenarios and actions, given the differences in perspectives between operators and PRA. Operators are trained to think in “success space” while PRA/HRA analysts focus on “failure space.” In addition, PRA/HRA analysts are accustomed to evaluating rare and unlikely scenarios with high consequences, while the experience base of operators may lead them to consider these scenarios incredible. Understanding these differences is important for PRA/HRA analysts to aid in communication and information gathering from operations and training.

Given their familiarity and comfort with the MCR, operators are likely to express reluctance to abandon the MCR, since it provides the scope and range of controls and indications they are accustomed to having during a transient or other plant upset. Consistent with this mindset, it may be difficult for operators to conceive of a fire that is large or severe enough that abandonment would be necessary. The analysts will have to assist in providing the PRA perspective regarding the severity of the fire, such as with the following explanations:

- The type of fire resulting in MCRA is severe. The fire modeling may show that certain large fires may affect multiple cable trays leading to damaging enough cables and/or equipment to cause LOC from the MCR.
- Risk insights from fire PRA indicate that fires large enough to result in significant effects on the availability and reliability of instrumentation will also be large enough to impact systems capable of providing sufficient cooling water flow to the reactor vessel (both high and low pressure systems). In such cases, the operators will not be able to determine plant status from the MCR and the vessel water injection systems may not be operating and attempts to actuate those systems from the control room with the abnormal operating procedures may fail. Therefore, transfer of command and control to the RSDP(s), which are unlikely to have affected instrumentation, provides backup capabilities for those scenarios that would have otherwise led directly to core damage.
- Providing the operators with the list of equipment and indications that have failed for the most risk-significant, plant-specific scenarios that would trigger a MCRA can help break the “barrier of conception” of the fire severity that they may face. These scenarios can even be set up as simulator exercises so that they can see what they would be dealing with.

10.4.2 Plant Modifications

When time is particularly constrained and the action is essential, plant modifications may be appropriate to provide a rapid response mechanism or an improved human-machine interface.

One of the more common modifications is the installation of a MCR “disconnect switch” (or several switches) to address spurious operation of valves (e.g., mitigates spurious opening by causing the valve to re-close). This protects the plant from spurious operations due to hot shorts and allows reactor or secondary coolant system boundary integrity to be maintained.

NRC IN 92-18 [5] describes a situation discovered by a licensee where “…a fire in the control room could cause hot shorts (i.e., short circuits between control wiring and power sources) for certain motor-operated valves (MOVs) needed to shut the reactor down and to maintain it in a safe shutdown condition. If a fire in the control room forces reactor operators to leave the control room, these MOVs can be operated from the remote/alternate shutdown panel. However, hot shorts, combined with the absence of thermal overload protection, could cause valve damage before the operator shifted control of the valves to the remote/alternate shutdown panel.” The IN further states, “Moreover, because thermal overload protection had been bypassed at some facilities, the potential existed for fire-induced spurious valve actuations to result in sufficient mechanical damage to prevent the reactor operators from manually operating the affected valves.” Some plants, therefore, choose to conduct plant modifications of MOVs susceptible to this type of overload damage to ensure they are available for manual operation when de-energized.

Other examples of plant modifications that facilitate or eliminate the need for operator manual actions related to MCRA are shown in the right-hand column of Table 10-1. The left-hand column of Table 10-1discusses the challenges for operator actions, including how the existing design and/or fire damage may prevent operator actions from being successful.

Table 10-1
Example plant modifications for MCRA

Challenge to MCRA Effectiveness	Description of Suggested Plant Modification
Following MCRA, the fire PRA cannot credit alignment of the fire water system as a backup injection source because hook-up requires collecting and gathering several pieces of equipment and currently there is insufficient time and procedure guidance to coordinate the movement of the required equipment.	Permanently install a fire water cross-tie spool piece and additional valves necessary to provide the ability to inject fire water into the feedwater system.
Following MCRA, the operators must travel to several different locations to depressurize RPV by opening Electromatic Relief Valves (ERVs) and there is insufficient time to perform all the required manipulations.	Modify the valve control circuits for the ERVs by providing an additional local selector/control switch that will allow an operator to turn power off/close the ERVs or to open the ERVs using a new alternate power source. The selector/control switches will have three positions for 1) normal power, 2) removal of power to close the ERV, and 3) emergency power to open the ERV. All required manipulations will be performed from a single location in the reactor building. This will ensure the operators have sufficient time to open ERVs.
If the control circuits for the diesel-driven cooling water pump are impacted by the fire, then the fire PRA requires a single operator to travel to two locations and coordinate with a second operator at the RSDP. This action is highly risk significant due to the complexity of the communication and coordination between the operators.	Protecting the control circuits to the diesel driven cooling water pumps would eliminate the current required manual action of sending an operator to two separate locations.
Following MCRA, there is insufficient time to de-energize a spuriously open PORV.	Install a kill switch from inside the MCR. This switch will de-energize equipment from the MCR and the operators will then need to re-start required equipment once outside the MCR. Procedure and training changes are necessary to ensure the decision to abandon is made within 5 minutes of the start of the event.

As the last entry in the table indicates, procedure changes and training updates for the physical plant modifications, as discussed in Section 10.4.3, are needed to ensure that operators have the direction and practice necessary to make the modifications effective.

10.4.3 Procedure and Training Updates

Some plants may already be in the process of updating their MCRA procedures and training. But as discussed in Section 10.4.2, discussion between the plant operations and training team and the PRA/HRA analyst can assist in re-ordering or emphasizing certain steps to ensure they are performed in a sufficiently timely manner.

An alternative is to perform the MCRA analysis first to gain information on the key actions and time constraints, then update the procedures later, stating as an assumption of the preliminary analysis that these procedure changes will be made.

There could be situations where evacuation is not immediately required but is anticipated, and the procedure could be modified to include steps to "pre-stage" the transfer of command and control to the RSDP. In such a case (as discussed in Section 4), one operator is dispatched to the RSDP as soon as it is determined that an active fire is occurring in an area that may require an MCRA. This "pre-staging" allows: 1) additional support to the diagnosis of LOC, since indications of system status and plant parameters on the RSDP can be compared with those observed in the control room, 2) additional time for making the decision to abandon the control room by shortening the amount of time required to make the transfer, and 3) initial actions to be immediately implemented at the RSDP by the operator stationed there once the decision to abandon is made.

Other examples of procedure changes related to MCRA are listed in Table 10-2.

Table 10-2
Example procedure changes for MCRA

HFE Description	Description of Suggested Procedure Change
Operators fail to cross tie Bus 15 and Bus 25	Add guidance to locally close bus-tie breakers if necessary to repower Train A 4kV bus from opposite unit.
Failure to make decision to leave MCR due to fire that causes LOC	Revise Shift Supervisor guidance for decision to abandon MCR.
Failure to manually isolate letdown	Add steps to determine whether letdown LOCA is in progress, and if so, close letdown valve switches on MCB prior to abandonment; re-establish using local controls if feasible.
Operators fail to de-energize source of fire-induced LOCA using MCR switch	Add steps to operate isolation switches prior to MCRA.
Operators fail to verify containment isolation	Add steps to require the operators to perform manual containment isolation prior to exiting the MCR, and to locally verify isolation after abandonment. Procedure changes should be optimized to improve the speed of the local isolation verification.

10.5 MCRA Requirements from the PRA Standard

The fire HRA section of the ASME/ANS PRA Standard [1] does not specifically discuss requirements for MCRA HRA. However, the requirements for fire HRA in the PRA Standard refer back to the internal events HRA standard requirements. Supporting Requirements (SRs) that are particularly relevant to MCRA actions are:

- HR-E3 (HRA-A1) on conducting talk-throughs of procedures
- HR-E4 on using simulator observations or talk-throughs to confirm the response models used for scenarios
- HR-G5 on basing the required time to complete actions for significant HFEs on action time measurements from either procedure walk-throughs or talk-throughs, or simulator observations

- HR-H2 on requirements for crediting operator recovery actions only if:
  a. A procedure is available and operator training has included the action as part of crew's training, or justification for the omission for one or both is provided
  b. There are "cues" (e.g., alarms) to alert the operator to the recovery action provided procedure, training, or skill-of-the-craft exist
  c. Attention is given to the relevant PSFs listed in HR-G3
  d. There is sufficient manpower to perform the action

The Fire Scenario Selection (FSS) section of the PRA Standard contains two SRs (FSS-B1 and FSS-B2) related to analysis of potential fire scenarios leading to MCRA. The guidance provided in Section 3 assists the analyst in meeting these SRs from a modeling perspective. In addition, the decision to abandon discussion provided in Section 4 addresses the need to define LOC criteria based on the distinction between LOH and LOC scenarios.

10.6 Documentation

Documentation of the MCRA HRA qualitative analysis should follow the basic concepts from NUREG/CR-6850 [2] and the ASME/ANS PRA Standard [1] outlined in Section 7 of NUREG-1921 [3] for the development of a calculation package or notebook. Generally, MCRA HRA is documented as a subsection of the overall fire HRA calculation, but can be done as a stand-alone document so long as any changes to the fire HRA that might impact MCRA are updated as well.

The following outline identifies the typical set of information that should be included in the MCRA HRA documentation:

- Introduction
- Assumptions
- Fire scenarios modeled for MCRA
- Abandonment criteria
  - LOH abandonment criteria
  - LOC abandonment criteria
- Timeline development for MCRA scenarios
- Operator interviews
- Identification and definition of HFEs associated with MCRA –including discussion on which HFEs are associated with which MCRA scenarios.
- Feasibility assessment
- Qualitative and quantitative analysis associated with HFEs (Note that the quantification of HFEs is not covered in this report.)

- Dependency analysis
- Uncertainty and sensitivity
- Feedback to operations and future plant improvements

10.7 Conclusions and Areas for Future Development

MCRA is a unique case of fire HRA that necessitates the development of a solid, qualitative analysis that accounts for fire-related damage criteria leading to abandonment, crew structure outside the MCR, and the coordination of many overlapping timeframes and actions.

The aspects of a good qualitative MCRA analysis include:

- Collection and review of plant-specific information and fire PRA insights
- Identification of MCRA scenarios including consideration of the decision to abandon and proper treatment within those scenarios based on different functional requirements
- Review of MCRA procedure steps and assessment of why each step is or is not relevant to the analysis
- Plant-specific walk-throughs and talk-throughs of the MCRA procedure
- Development of timeline based on walk/talk-throughs, simulator exercises, training material and thermal-hydraulic analyses
- Identification and definition of HFEs based on the MCRA procedure and context of MCRA scenarios
- Evaluation of HFE-specific timing and PSFs based on the context of MCRA scenarios
- Assessment of command and control in terms of existing plans, training, and communication strategies
- Documentation of analysis, including input parameters

The following areas have been identified as areas for future development as a result of the compilation of this report.

- Guidance for MCRA HRA quantification
- Ways to model command and control

Appendix B and the discussion of aspects of C&C in the Section 8 identify what C&C is and how some facets are addressed through PSFs. However, there is not, yet, an agreed-upon approach for modeling C&C. This is an area for further research and development.

10.8 References

1. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, The American Society of Mechanical Engineers, New York, NY, February 2009.
2. *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, U.S. Nuclear Regulatory Commission, Rockville, MD and EPRI, Palo Alto, CA: September 2005. NUREG/CR-6850, EPRI 1011989.
3. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
4. U.S. Nuclear Regulatory Commission. NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*, Washington, D.C. October 2007.
5. Information Notice No. 92-18: *Potential for Loss of Remote Shutdown Capability During a Control Room Fire*, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, DC: February 28, 1992.

APPENDIX A
MAIN CONTROL ROOM ABANDONMENT REGULATORY BACKGROUND, HISTORICAL EVENTS, AND REMOTE SHUTDOWN PANEL VARIATIONS

This appendix provides summaries relevant to MCRA on the topics of: 1) U.S. regulatory background, 2) historical events, and 3) alternative and remote shutdown panel variations.

A.1 Regulatory Background for MCRA

Although fires are the most frequently occurring event that could require MCRA, fires are not the only type of event addressed in regulatory requirements for NPPs that may require MCRA. Requirements for MCRA are rooted in the Code of Federal Regulations (10 CFR 50), both Criterion 19 in Appendix A [1] (which relates to control room habitability) and Appendix R [2] (e.g., Sections III.G.3 and III.L) which relates to fire protection.

A.1.1 10 CFR Part 50, Appendix A and Related Guidance

The MCR is the area of a NPP defined in the facility licensing basis from which actions are taken to operate the plant safely under normal conditions and to maintain the reactor in a safe condition during accident situations. For most plants, the criteria defined in General Design Criterion 19 (GDC 19) in 10 CFR Part 50, Appendix A [1], “General Design Criteria for Nuclear Power Plants,” apply to this area.

NRC Generic Letter 2003-01 [3]: Control Room Habitability, issued in 2003 further defines issues related to the requirement to maintain control room habitability. The control room envelope (CRE) is the plant area defined in the facility licensing basis that encompasses the control room and may encompass other plant areas. Structures that make up the CRE are designed to limit the in-leakage of radioactive and hazardous materials from areas external to the CRE. Control room habitability systems (CRHSs) typically provide shielding, isolation, pressurization, heating, ventilation, air conditioning and filtration, monitoring, and the sustenance and sanitation necessary to ensure that the control room operators can remain in the control room and take actions to operate the plant under normal and accident conditions. Plant design bases and severe accident risk analyses both assume that the control room operators can remain safely within the control room to monitor plant performance and take appropriate mitigation actions. NRC Generic Letter 81-12 [4] outlines the equipment that is required to be operational so that the plant can achieve hot standby and cold shutdown for both a PWR and a BWR. Generic Letter 81-12 also outlines the requirements for alternative or dedicated shutdown capabilities.

A.1.2 10 CFR Part 50, Appendix R and Related Guidance

The regulations do not specify criteria for when operators must abandon the MCR. The criteria for MCRA are procedurally outlined by each plant and therefore may vary widely from plant to plant. For example, no regulatory limit exists on the amount of smoke allowed in the control room. The plant's ability to manage smoke infiltration is assessed qualitatively. Licensees should perform a qualitative assessment to ensure that the plant can safely be shut down from either the control room or the alternate shutdown panel during an internal or external smoke event [5]. The MCR evacuation procedure's entry conditions may include criteria such as a fire in certain critical plant areas (e.g., the control room, CSR, HVAC equipment room, etc.), loss of or unreliable operation of controls and indicators, spurious operation of plant circuitry exposed to a fire, or personnel safety concerns due to smoke, toxic gas, radiation, bomb threat, etc.

A.2 Historical Events Involving MCRA

Evacuation of the MCR is an extremely rare and unusual occurrence. The regulations require that the control room be maintained in a habitable condition such that critical functions can be safely performed even under accident conditions. 10 CFR 50, Appendix A, General Design Criterion 19 [1] states that, "A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents." Thus the occurrence of conditions that lead to the evacuation of the control room should, by design, be extremely uncommon.

As part of this project, relevant operating experience was reviewed. In particular, NUREG/CR-6738 [6], *Risk Methods Insights Gained From Fire Incidents,* and licensee event report (LER) searches were performed. Searches of both LER abstracts and full-text LERs were performed using the following key words:

- Control room
- Main control room fire
- Control room evacuation

These searches revealed that, to date, there have been no evacuations of the control room of any operating nuclear power plant in the United States. One evacuation occurred at Haddam Neck Nuclear Power Plant due to toxic gas (see Section A.2.1), which was permanently defueled at the time of the event.

The only known evacuation of an operating NPP MCR occurred at the Narora Atomic Power Station, a non-U.S. NPP, in Uttar Pradesh, India.[41]

Sections A.2.1 and A.2.2 briefly summarizes the two events that resulted in MCRA. Section A.2.3 summarizes some other incidents that involved challenging fires, but did not result in MCRA.

[41] Table 4-1 in NUREG/CR-6738 [6] identifies a control room evacuation for the December 31, 1978 event at Beloyarsk Unit 2. However, the detailed description of this event in Section A.5 in NUGREG/CR-6738 does not support that this event resulted in an evacuation.

A.2.1 Haddam Neck– Non-Fire Event with MCRA of Defueled US NPP [7]

In August of 1997, the only evacuation of a control room to date in a U.S. nuclear power facility took place at the Connecticut Yankee Nuclear Power Plant in Haddam Neck, Connecticut. At the time of the evacuation the plant was in a permanently defueled condition. At approximately 9:47 a.m. the control room Halon system was inadvertently discharged while a training instructor was taking flash camera pictures of the inside of a Halon control panel located in the control room. Because prolonged exposure to Halon, a chemical used to extinguish fires, can result in nausea and dizziness, the control room and adjacent security central alarm station were evacuated as a precautionary measure. Upon exiting the control room, operators continuously monitored the control board through a window in the viewing area located immediately outside the control room. The control room ventilation system was used to remove the Halon, the air was sampled, and operators were able to reoccupy the control room in approximately 45 minutes.

A.2.2 Narora Atomic Station – Fire with MCRA of Non-U.S. NPP [6]

The only occurrence of a MCRA at an operating nuclear power facility took place in March of 1993 at the Narora Atomic Power Station in Uttar Pradesh, India. Narora is a two-unit 220 MWe PHWR (Pressurized Heavy Water Reactor). With Unit 2 shutdown (but containment still pressurized), the Unit 1 turbine generator tripped from 84% power followed immediately by the sound of an explosion and the report of a large fire under the main generator. A gust of hot dusty air was felt in the MCR and, after observing the extent of the fire, 38 seconds after the turbine trip, operators manually tripped the reactor and commenced an emergency cooldown. In just under eight minutes, the fire station was called. At about eight minutes following the turbine trip, there was a complete loss of all electric power in Unit 1 and a plant emergency was declared. The fire spread quickly through a cable penetration fire barrier into the control equipment room adjacent to the control room, leading to such extensive smoke in the MCR that operators were forced to evacuate. Operators were not able to re-enter the control room for about 13 hours. An attempt was made to control the plant from the emergency control room. This effort was successful for Unit 2, but there was no power available to the Unit 1 side (so there were no functioning indications for Unit 1). The fire was brought under control in about 1.5 hours and, after an additional 4 hours, power was restored to one emergency bus via diesel generator. The fire was not completely extinguished until 9 hours after it began and the plant emergency was ended at 19 hours.

The root cause of the fire was identified in follow-up investigations to be a fatigue failure of the last stage low-pressure turbine blades. This caused a severe imbalance on the rotor, leading to failure of the turbine bearing and the generator hydrogen seals. Escaping hydrogen was ignited by generator slip rings. The effects of the ensuing explosion ruptured turbine generator oil pipes, which fed the fire and helped to ignite electrical cable insulation. In addition, the fire spread from the turbine building to the adjacent control equipment room via cable trays, and was assisted by the lack of proper fire barrier penetration seals.

The Narora incident illustrates that a large plant fire can cause control room habitability issues significant enough to necessitate abandonment of the control room even if the fire is outside of the MCR. The Narora fire also illustrated that turbine building fires, which are often screened out as being risk insignificant, can under certain circumstances present a severe challenge to nuclear safety.

A.2.3 Challenging Fire Events That Did Not Result in MCRA

A sample of fire events history must include the Browns Ferry event that resulted in some dramatic changes in U.S. fire protection requirements. This event is summarized below, followed by brief descriptions of a few other U.S. and non-U.S. fires where smoke was observed in the control room.

Browns Ferry [6, 8, 9]

Though no evacuation took place, there has been one challenging fire in an operating U.S. NPP that, had it occurred today may have led to the evacuation of the control room. This event took place at the Browns Ferry NPP in Athens, Alabama in 1975. The fire event at Browns Ferry forever changed how the NRC and the nuclear power industry view the threat of fire to nuclear power plant safety and prompted a new series of fire protection regulations.

Using a small lit candle to search for air leaks in temporary polyurethane penetration seals between the reactor containment building and the Unit 1 reactor building of the plant, a technician inadvertently ignited insulation around electrical cables that supplied power to the plant's MCR and safety systems. The fire started around 12:20 p.m. and advanced from the CSR into the reactor building through the cable-tray penetration and burned for over 7 hours before water was used to extinguish the fire. Initially hand-held dry chemical and CO_2 had been used to fight the fire, but the fire continued to smolder and re-ignite. Activation of the plant's permanently installed CO_2 fire-extinguishing system was initially delayed due to the fact that the power had been shut off as a safety measure during the leak testing and because manual activation was prevented by metal plates that had been installed under the breakout glass to prevent inadvertent activation during plant construction. The fire in the CSR was eventually extinguished using the CO_2 system and chemical extinguishers, but the fire continued to burn in the reactor building, requiring use of ladders to apply the contents of hand held extinguishers. By 12:35 p.m., the smoke had become so dense that breathing apparatus was required. Problems in fighting the fire were compounded by reluctance to use water (e.g., hose streams) on energized electrical cables, the loss of the ventilation system and the reactor building lighting, along with a shortage of air-breathing equipment.

During the seven hours the fire was burning, operators faced several unusual situations. Around 12:40 p.m., alarms associated with the emergency core cooling system (ECCS) initiated but were inconsistent with the systems' status. The residual heat removal (RHR) core spray (CS) system, the high-pressure coolant injection (HPCI) system, and RCIC had initiated and were running. The operators stopped the pumps, but the alarms would not reset. Over the next few minutes there was other anomalous behavior of controls and instrumentation including other starts and stops of RHR, CS, and HPCI and brightening and dimming of panel lights. At one point smoke infiltrated the MCR to the extent that some operators put on breathing apparatus for a brief period. All of Unit 1, and many of Unit 2, reactor emergency core cooling systems were rendered inoperable due to fire damage.

Though the operators were successful in maintaining core cooling and the fire was eventually extinguished, this event challenged nuclear safety and lead to changes in fire protection for all U.S. NPPs.

Other Fires Resulting in Smoke in the Control Room

There have been a number of other incidents where varying quantities of smoke entered the control room from other areas of the plant. In all of these incidents the operators remained in the control room.

One such incident occurred at the Vandellos NPP [6], a graphite moderated reactor in Barcelona, Spain in 1989. In this incident, a turbine blade ejection caused a rupture in several oil lines and a large oil and hydrogen fire. Smoke from the turbine building fire entered the control room and several other parts of the plant. Automatic fire suppression systems were activated in areas remote from the actual fire due to smoke and plant personnel had to wear SCBA to enter certain areas of the reactor building. Control room operators were issued SCBA but they were never used. Portable fans were brought in to clear the smoke and provide fresh air into the control room.

Another incident occurred at the Oconee NPP [6] in Seneca, South Carolina in 1989. In this incident a switchgear failed explosively and caught fire. At some point in this incident smoke entered the control room, but the extent of the smoke and the path by which it found its way into the control room are not described in available sources.

In 1978, a fire in the turbine building at the Beloyarsk [6], a 146 MWe light-water-cooled, graphite-moderated reactor (LWGR) 1000 type nuclear power plant in Ekaterinburg, Russia resulted in fire propagation into the adjacent control building via cable penetrations and other openings. The fire also propagated into the control panels of the MCR and caused damage. Operators had to work in heavy smoke conditions with some operators reported as being “half-conscious” due to smoke inhalation. Despite these difficulties, operators worked under extremely difficult conditions and managed to start one train of reactor emergency cooling system while remaining in the control room.

A large cable gallery fire occurred at Armenia Nuclear Power Plant, Units 1 and 2 on October 15, 1982, resulting in a SBO. This fire mainly affected Unit 1, but both units were tripped. Unit 1 lost all safety related systems, including active core cooling capability, but was able to use natural circulation. Dense smoke entered the control room making habitability difficult, however operators remained in the control room. Fire propagation spread through non-existent or open fire doors and unsealed cable penetrations. There were a number of unexplained failures (as noted in Reference 6) in addition to the lack of cable separation which resulted in numerous common cause failures.

A.3 Alternative and Remote Shutdown Panel Variations

Per fire protection requirements defined in 10 CFR 50.48 and 10 CFR Appendix R, plants are required to have an alternative means to bring the plant into safe shutdown in the event that redundant trains of shutdown equipment are located in the same fire area and not adequately protected or separated. The MCR is a plant location where cables for redundant trains are located. Therefore, alternative or dedicated shutdown capability must be provided. Alternative or dedicated shutdown capability may be in the form of alternative/dedicated shutdown systems or

remote shutdown systems. Remote shutdown systems are needed to meet GDC 19 and must be redundant and physically independent of the control room. Alternative or dedicated shutdown capability required by Appendix R need not be redundant but must be both physically and electrically independent of the control room. [10].

In the event of a fire that requires evacuation of the control room, safe shutdown is accomplished by the use of controls and instrumentation that are isolated or independent from the fire area, in addition to operator manual actions for select components. There is no requirement to have all of the required controls and instrumentation in one central location. Such devices may be located in numerous areas of the plant provided it can be demonstrated that there is adequate manpower available to accomplish the required tasks within an acceptable timeframe.

Common alternative shutdown design approaches include:

- Installation of a dedicated RSDP containing the majority of the controls and indications for the systems required to achieve and maintain shutdown, located in a separate plant fire area
- Upgrading and backfitting of an existing panel (installed as part of meeting GDC 19) to meet the criteria of Section III.L of Appendix R
- Use of multiple panels and local control stations to meet the criteria of Section III.L

The safe shutdown analysis should demonstrate that alternative or dedicated shutdown systems and equipment are capable of performing their required safe shutdown functions and that fire damage to other systems and equipment will not cause perturbations that can prevent the accomplishment of required safe shutdown conditions.

Specific criteria include:

1. The alternative or dedicated shutdown capability should be capable of accomplishing required shutdown functions where offsite power remains available and where offsite power is not available.
2. The control systems used for alternate shutdown outside of the control room must be separate from the fire area, and redundant fusing should be installed to protect against the occurrence of fire-induced circuit failures in the fire area that might affect transfer to the local or remote panel and subsequent equipment operation (IN 85-09 [11]).
3. Where alternative or dedicated shutdown capability is required, the licensee shall provide fixed fire suppression and detection for the fire area or zone containing the redundant success paths (detection and suppression are not necessarily required for the area or zone containing the alternative or dedicated shutdown system except where required by the fire hazards analysis).
4. The licensee should provide procedures to implement the alternative or dedicated shutdown capability, as described in Regulatory Position 5.5 of RG 1.189 [12].

5. The licensee should consider the occurrence of one spurious operation or signal before control of the plant is achieved through the alternative or dedicated shutdown system. After the operators transfer control from the control room to the alternative or dedicated shutdown system, single or multiple spurious operations that could occur in the fire-affected area should be considered, in accordance with the plant's approved fire protection plan.
6. For a fire requiring control room evacuation, the only operator action in the control room before evacuation for which credit is usually given is reactor trip. For any additional control room actions deemed necessary before evacuation, a licensee should be able to demonstrate that such actions can be performed. Additionally, the licensee should ensure that such actions cannot be negated by subsequent spurious operation signals resulting from the postulated fire. The design basis for the control room fire should consider one spurious operation or signal to occur before control of the plant is achieved through the alternative or dedicated shutdown system. After control of the plant is achieved by the alternative or dedicated shutdown system, single or multiple spurious operations that could occur in the fire-affected area should be considered, in accordance with the plant's approved fire protection program[42] (RG 1.189 [12]).
7. Procedures should be in effect that describe the tasks to implement alternative or dedicated shutdown capability when offsite power is available and when offsite power is not available for 72 hours. These procedures should also address necessary actions to compensate for spurious operations and high-impedance faults, if such actions are necessary to affect safe shutdown.
8. Procedures governing the return to the control room should consider the following conditions:
    a. The fire has been extinguished and so verified by appropriate fire protection personnel.
    b. Appropriate fire protection personnel and the shift supervisor have deemed the control room to be habitable.
    c. Damage has been assessed and, if necessary, corrective action has been taken to ensure that necessary safety, control, and information systems are functional (some operators may assist with these tasks), and the shift supervisor has authorized the return of plant control to the control room.
    d. Turnover procedures that ensure an orderly transfer of control from the alternative or dedicated shutdown panel to the control room have been completed.
9. Repair procedures should be in effect to accomplish repairs necessary to achieve and maintain cold shutdown within 72 hours. For plants that must proceed to cold shutdown within 72 hours, the procedures should support the required time for initiation of cold shutdown.
10. The performance of repair procedures should not adversely affect operating systems needed to maintain hot shutdown.

[42] Most licensees have a Safety Evaluation Report (SER) for their alternate and dedicated shutdown strategies outlining the specific considerations needed in response to a control room fire scenario. These SERs are referenced in each plant's fire protection license condition.

Given that plants can meet the requirements for alternative shutdown capability in a number of ways, there is significant variability in the approaches that different plants use to meet alternative shutdown requirements when the MCR must be abandoned. Some plants have panels that look like smaller versions of the control panels in the MCR while others may only have a simple panel with a few essential indications and controls while other plants do not have a centralized panels but must go to several locations to perform the required functions.

The U.S. commercial industry operates licensed PWR and BWRs. Due to the different reactor type, vintage, and plant-specific design features in the United States, each reactor can be considered to be unique with respect to ensuring that safe shutdown can be maintained outside the control room. Table A-1 and A-2 list various plant designs to illustrate the differences in panels utilized for alternative or dedicated shutdown capability, as well their functionality of critical systems.

Table A-1
Examples of PWR RSDP variations

Plant Identifier	# of RSDPs	Functions available at RSDP										
		Reactor Subcriticality		**Primary Integrity**		**Primary Inventory**		**Core Heat Removal, Early**		**Core/Containment Heat Removal, Late**		**Support Systems**
		Examples: Rx trip, Emergency Boration, Rod insertion		**Examples:** PORV control Block valve control		**Examples:** Safety Injection Charging		**Examples:** AFW Condensate Feed and Bleed Make up to the CST		**Examples:** RHR/ High pressure recirculation		**Examples:** Component Cooling Water (CCW)/ Emergency Service Water (ESW)/ Service Water (SW) Instrument Air (IA) DC power AC power
		Instrumentation	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Hardware/ control**
PWR A (W 4 loop)	1	None	None	RCS pressure; RCS temperature; Reactor water level	None	Charging pump flow; Reactor water level	Charging pump	SG level	AFW (1 train)	RCS pressure; RCS temperature	None	None – All local actions taken away from the RSDP
PWR B (W 4 loop, 2 unit)	2 (shared between units; one primary RSDP, 2nd very limited)	Emergency Boration Flow; Gamma metrics; Source range neutron flux	Boric acid pumps; Emergency borate valve	PZR pressure; PZR liquid temperature; PZR level	PZR Heater groups; PORV emergency close; PZR aux spray [secondary RSDP]	Charging header flow; Charging pump discharge pressure; Volume Control Tank (VCT) level	Charging pump; Flow control valve	SG pressure; SG wide range level; AFW pump discharge pressure; AFW flow; CST level; Raw water reservoir levels	10% steam dumps; AFW pumps (2 of 3); level control valves (motor and electro-hydraulic driven)	[located on secondary RSDP] RCS pressure; RCS loop temps	None	CCW & ASW pump control; Containment fan cooler unit (CFCU) control; Voltmeters for busses
PWR C (W 3 loop)	Panel A			RCS hot leg wide range temp; RCS cold leg temp; Percent Power	PZR Heater	Charging flow; Charging pressure; Charging flow control valve status	Charging flow control valve transfer (remote/local)	Turbine-driven emergency feed pump valve flow	TD EFP flow valve to SG	Low pressure Letdown flow	Letdown orifice isolation control; Letdown line isolation level control valve	SW pump control
	Panel B	Emergency Boration Flow	Emergency Boration Flow control	RCS pressure; RCS cold leg temp; PZR pressure; PZR wide range level; PZR Heater BU group 2 status	PZR Heater BU group 2 status	VCT level; PRT level		SG pressure; SG wide range level; Condensate tank level; Motor-driven emergency feed pump valve flow	MD EFP flow valve to SG control			SW pump control

Table A-2
Examples of BWR RSDP Variations

Plant Identifier	# of RSDPs	Functions available at RSDP										
		Reactor Subcriticality		**High Pressure Injection**		**Depressurization**		**Low Pressure Injection**		**Long Term Decay Heat Removal**		**Support Systems**
		Examples: Rx trip, Emergency Boration, Rod insertion, SLC		**Examples: HPCI RCIC**		**Example: SRVs**		**Examples: LPCI RHR SW**		**Examples: Torus Cooling Shutdown Cooling/RHR**		**Examples: SW IA DC power AC power**
		Instrumentation	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/ control**	**Instrumentation**	**Hardware/control**	**Hardware/control**
BWR A, Unit 1	3	Reactor power	None	RPV level	None	Primary pressure and temp.	SRV control	Primary pressure and temp.	LPCI start and control	Torus temp.	RHR pump start	None
BWR A, Unit 2	1	Reactor power	None	RPV level	RCIC	Primary pressure and temp.	SRV control	Primary pressure and temp.	LPCI start and control	Torus temp.	RHR pump start	None
BWR B	1	Reactor power	None	RPV level; RPV pressure	None (RCIC controlled locally)	MSIV close	SRV control	Primary pressure and temp.	RHR SW pump start RHR pump start; RHR pump min flow valve control;	Torus temp; RHR flow; Drywell pressure	RHR pump start; RHR pump min flow valve control; Containment vent/ purge valve control; Hard pipe vent valve control	Emergency SW pump; DG transfer switch; Transformer to Bus switch; Standby EDG control; Primary and secondary load center control; Diesel oil transfer pump start; SW equipment room HVAC control

A.4 References

1. Code of Federal Regulation (CFR), Title 10, Appendix A to Part 50, “General Design Criteria for Nuclear Power Plants,” U.S. Government Printing Office, Washington, D.C.
2. Code of Federal Regulation (CFR), Title 10, Appendix R to Part 50, “Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979,” U.S. Government Printing Office, Washington, D.C.
3. U.S. Nuclear Regulatory Commission, Generic Letter (GL) 2003-01: “Control Room Habitability,” Washington, D.C.: June 12, 2003.
4. U.S. Nuclear Regulatory Commission, Generic Letter (GL) 81-12: “Fire Protection Rule (45 FR 76602, November 19, 1980),” Washington, D.C.: February 20, 1981.
5. *Control Room Habitability at Light-Water Nuclear Power Reactors*, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, D.C.: January 2007. Regulatory Guide (RG) 1.196 Revision 1.
6. U.S. Nuclear Regulatory Commission, NUREG/CR-6738, *Risk Methods Insights Gained From Fire Incidents,* Washington, D.C.: September 2001.
7. Licensee Event Report, LER 50-213/97-013-00, “Inadvertent Halon Discharge in Control Room Due to Camera Flash Results in Precautionary Control Room Evacuation”: August 1997.
8. A.J. Pryor, *The Browns Ferry Nuclear Plant Fire,* Society of Fire Protection Engineers Technology Report 77-2, Boston, MA: 1977.
9. U.S. Nuclear Regulatory Commission, NUREG/KM-0002, Rev. 1, *The Browns Ferry Nuclear Plant Fire of 1975 Knowledge Management Digest,* Washington, D.C.: February 2014.
10. U.S. Nuclear Regulatory Commission, Generic Letter (GL) 1986-10, “Implementation of Fire Protection Requirements,” Washington D.C.: April 1986.
11. U.S. Nuclear Regulatory Commission, Information Notice (IN) 1985-09: “Isolation Transfer Switches and Post-fire Shutdown Capability,” Washington, D.C.: January 31, 1985.
12. U.S. Nuclear Regulatory Commission, Regulatory Guide (RG) 1.189: “Fire Protection for Nuclear Power Plants,” Washington, D.C.: October 2009.

APPENDIX B
COMMAND AND CONTROL

B.1 Introduction

This appendix concerning command and control (C&C) represents the current status of development, as related to operator responses in the MCR of U.S. NPPs and, more specifically, to MCRA scenarios. The reader should note that this research is ongoing, including:

- Finalization of the definition of command and control (and related terminology) in the context of U.S. NPPs
- Reviews of relevant operational experience
- Identification and understanding of explanatory psychological and behavioral models
- Understanding the differences between C&C in the MCR versus following MCRA
- Identification of relevant PSFs and their potential dependencies, connections, and/or overlaps
- Understanding how C&C should be represented in HRA (such as a separate function and HFE, a meta-PSF for multiple HFEs, or a set of dependent PSFs imposed on individual HFEs)
- Identification of similarities, overlaps, or gaps with factors or inputs used in existing HRA methods.

In addition, while the project team has reached consensus on the importance of C&C in MCRA HRA scenarios, the work presented below is considered interim guidance on an understanding of C&C issues and how these issues can be incorporated in PRA and HRA modeling for MCRA events. Section B.5 of this appendix provides interim guidance on aspects of HRA for C&C, and a list of the areas for intended development.

While this work is still in development, the area of C&C is an important one when considering the reliability of operator actions where the center of control is no longer the MCR and the MCR crew may no longer function as an integrated team. C&C is important for MCRA scenarios and may well be true for other NPP accident scenarios where effective control is distributed as, for example, control actions are being directed from the TSC.

This appendix is organized in the following way:

- Section B.2 provides a background discussion on C&C for NPP accident response from the MCR and for MCRA scenarios
- Section B.3 provides a working definition of C&C and describes how it relates to the current understanding of macrocognition, especially the contrast between operator tasks for in-MCR and abandonment scenarios

- Section B.4 summarizes lessons learned from operational experience relevant to C&C
- Section B.5 provides the interim guidance for analysts to begin incorporating C&C issues in MCRA scenarios

B.2 Background

B.2.1 A Summary of Command and Control

Command and control is a term that has evolved from military applications to common usage in systems where there is need for a central body of authority to make decisions but have them carried out by a distributed group [1]. The abbreviation “C2” is often used in military applications for command and control, and is sometimes extended to “C3” to designate the addition of communications. As these abbreviations are used in specialist ways in military settings, the abbreviation “C&C” is used in this report to indicate that it is a general term that does not correspond exactly to the military usage, though there is a significant overlap in the concepts.

Searches for a relevant definition for command and control have so far identified military sources, such as the U.S. Army Field Manual [1]:

> “*Command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission. Commanders perform command and control functions through a command and control system.”

Along with this definition, Figure B-1 illustrates what is meant by "command and control" in the military perspective in which “the focus of Command and Control (C2) is the commander. Commanders assess the situation, make decisions, direct action and continuously assess whether operations are being successful. To implement their decision, commanders direct coordinated actions by their forces that together accomplish the mission” [1].

Stanton, et al., [2] describe the North Atlantic Treaty Organization’s (NATO’s) definition as separating command and control in the following way:

> “‘command’ is ‘…the authority vested in an individual…for the direction, coordination and control of military forces’. This implies that an individual will be given the role of Commander, that this individual will (through this role) be imbued with sufficient authority to exercise command, and (by implication) this command will involve defining the goal (intent, effect) that Forces under the individual’s command will achieve.”

Further, Stanton, et al., believe that C&C can be summarized as having the following three features [2]:

- "A common overall goal (this may, however, be comprised of different but interacting sub-goals).
  - Corollary: Systems of command and control are goal-oriented systems.
- Individuals and teams acting individually or in unison.
  - Corollary: There is the need to coordinate activity.
- Teams and sometimes individuals are often dispersed geographically.
  - Corollary: There is the need to communicate and share 'views' on the situation"

In summary, the attributes of a military C&C system are:

- Focus to assess the situation, make decisions, and direct actions
- Goal is mission accomplishment
- Commanders exercise authority and direction over forces by establishing command or support relationships
- Commanders must dedicate and organize resources. Commanders use these resources to plan and continuously assess operations that the force prepares for and executes
- Command/control system manages information to produce and disseminate a common operational picture (COP) to the commander, staff, and subordinate forces
- Direct forces by transmitting execution information

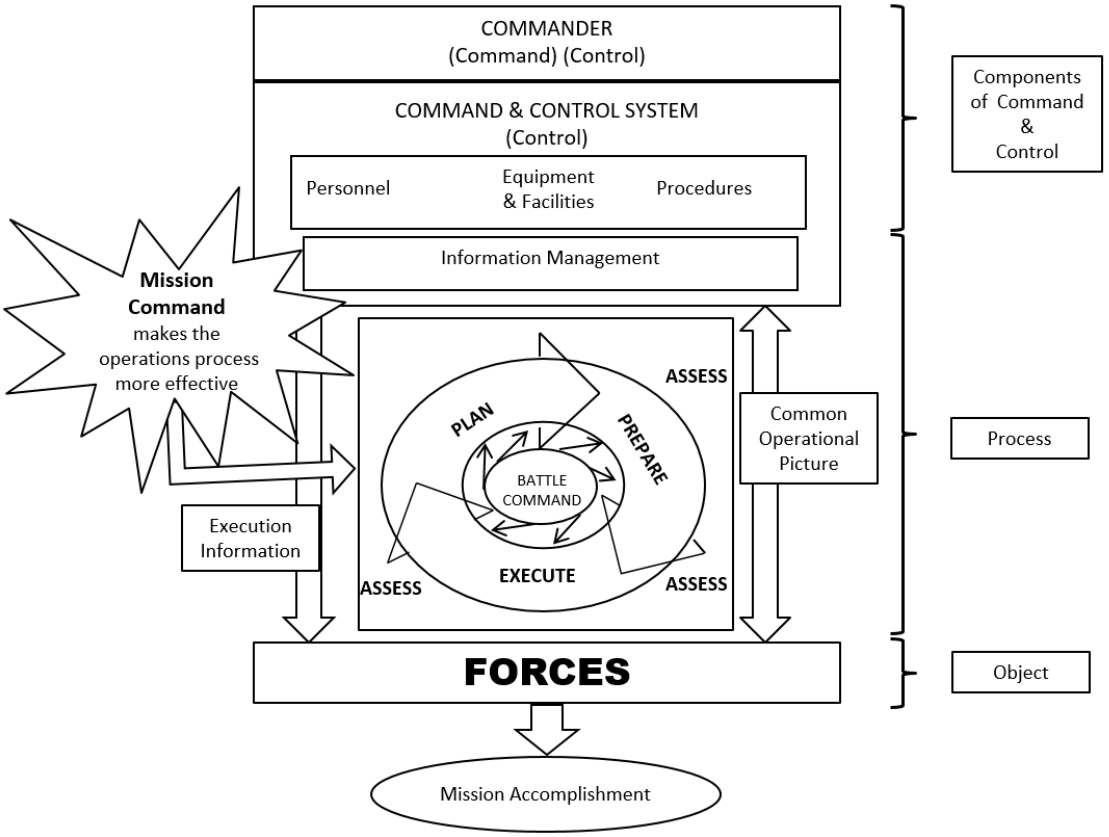


Figure B-1
Military representation of command and control [1]

In a more general view, Smalley [3] proposed a functional flow diagram to describe the activities that make up C&C in a general setting; this is shown in Figure B-2. As described by Stanton, et al., [2]:

> "Smalley proposes a functional socio-technical model of command and control, comprising some seven operational and decision support functions (six in the ovals and one in the box) and ten information processing activities (appended to the input and output arrows). These include several 'unobservable processes'. The ten information processing activities are: primary situation awareness, planning, information exchange, tactical situation reports, current situation awareness, directing plan of execution, system operation, system monitoring, system status, and internal co-ordination and communications."

Figure B-2 shows how Smalley represented the relationship between the operation and decision support functions, as well as information processing activities. The figure is intended to show the following:

- Information is collected based on the operators' situational awareness to form the basis for overall command tasks and planning
- Following the development of the planning activities, these are communicated to external groups and those involved in the command and control activities
- Tactical decision-making (how to respond) is based on the current situation, determined from monitoring the state of the plant and knowledge of the systems operation
- The tactical decision-making leads to requirements for systems operations
- System monitoring is performed to see if expected outcomes are achieved
- Both internal and external coordination and communication keep the command and control system functioning

B.2.2 Behavioral and Cognitive Models Related to C&C in NPP Operations

This project performed a psychological literature review in order to identify any relevant models that might shed light on how command and control is represented within NPP operations. The literature review was first done generally, then specifically in terms of relevance to NPP operations. This review was aided by the interviews of NRC staff with operational experience, and is ongoing while the authors begin preparing HRA quantification guidance for MCRA scenarios. Existing resources (e.g., psychological bases for existing methods, reports, and papers on behavioral and cognitive models) were initially reviewed and the scope was then expanded to include personal communications with various experts in psychology, behavioral and cognitive science, and related fields. This section represents our knowledge and understanding to-date.

The text below briefly describes the human information processing models that either have been used in NPP operational contexts before or appear to be useful specifically to MCRA scenarios. At present, the authors have not found any model that is directly relevant to command and control in MCRA scenarios. Consequently, later discussions include consideration of issues not represented in the models that are relevant to command and control within MCRA scenarios.

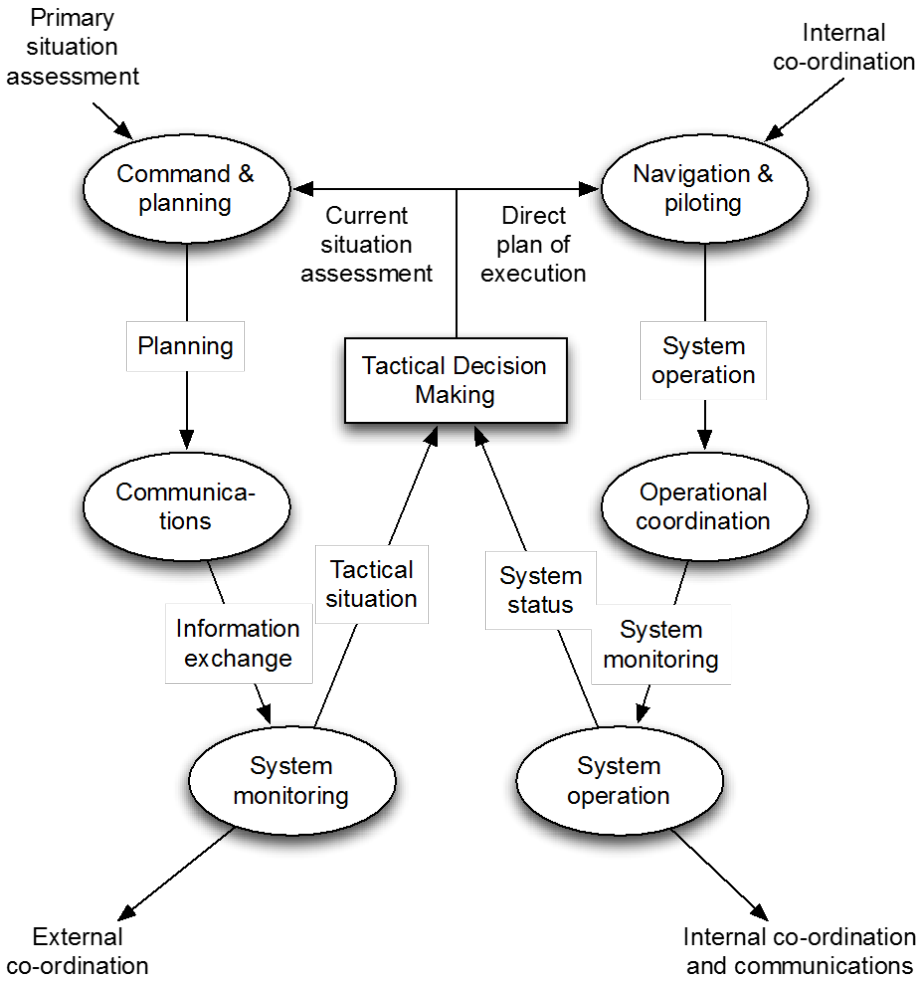


Figure B-2
Functional process diagram for C&C developed by Smalley [3]

Command and control represents the essential functions of the operating crew in a post-initiator response as described in HRA methods like ATHEANA [4, 5]. One framework that has been developed for describing the performance of humans in process control (including the response to initiating events in NPPs) is based on an understanding of macrocognition [6, 7]. Macrocognition refers to the process in real-world settings by which individuals and teams detect situations, make sense of those situations, and formulate response plans.

NUREG-2114 [8] adopted the macrocognitive model to describe the high-level functions through which an operator's task within a nuclear power plant is accomplished. The model described in NUREG-2114 assumes that cognitive tasks are achieved through five macrocognitive functions: 1) detecting and noticing, 2) understanding and sensemaking, 3) decision-making, 4) action, and 5) teamwork. These macrocognitive functions are further refined by identifying possible causes of failures (labeled proximate causes), the cognitive mechanisms for these failures, and the relevant PSFs.

As the NUREG-2114 explains [8]:

> "The purpose of the cognitive framework is to identify and provide explicit connections between plausible causes, mechanism, and influences for failure of a macrocognitive function".

This framework was developed to address human cognition within and outside the MCR.

In earlier work similar to NUREG-2114, Roth, Mosleh, et al., [9] describe macrocognition for nuclear plant operating crews as being comprised of the following activities:

- Detecting/noticing
- Directing attention/managing workload
- Sense-making/understanding
- Planning/deciding
- Communicating/coordinating (teamwork functions)
- Supervising/directing personnel
- Executing actions

Figure B-3 presents a summary of these activities based on Roth, Mosleh, et al. [9]. The following description is taken from Roth, Mosleh et al.:

> "At the core of this model is the concept that people actively work to construct a coherent understanding of the situation they are in – this is referred to as '*sensemaking*' [c.f., 10]. The output of sensemaking is a *situation model* that represents a person's understanding of a situation. This understanding draws on both real-time information obtained from the world via perceptual processes (i.e., the macrocognitive function of *'detecting/noticing'*), as well as background knowledge stored in long-term memory (e.g., mental models). The situational model is closely related to (and subsumes) theoretical concepts such as *situation awareness* and *diagnosis*. A person's situation model may or may not be an accurate representation of the true state of the world. Another core concept of the model is that people have limited attention, short-term memory, and information processing capability. This places a premium on '*directing attention and managing workload'* functions. Attention/workload management refers to determining where to direct attention and focus activity under high workload/ high attention demand conditions. People form expectations as to what should happen next and what is highest priority to deal with based on their situation model. These expectations influence where people will direct their attention and how they will manage their workload (e.g., how they will prioritize activities under high workload conditions). These in turn will influence what people will pay attention to and therefore what they will detect/notice [11, 12]. People's understanding of a situation also influences *planning and deciding* functions. Based on their situation model people will prioritize goals, make decisions, and plan actions. *Communicating and coordinating* and other related teamwork activities, including supervising/directing personnel, are also central macrocognitive functions [13]. These functions enable the team to operate as a cohesive macrocognitive unit. The output of all these macrocognitive processes is the execution of observable physical actions."

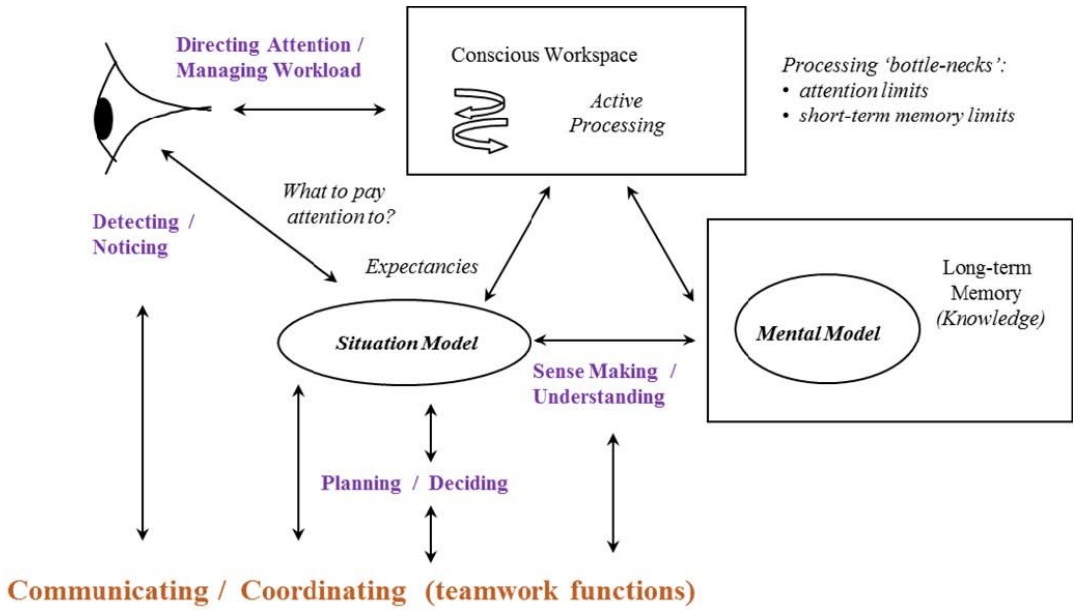


Figure B-3
A simplified model of macrocognition (based on Roth, Mosleh et al. [9])

Using this model, Roth, Mosleh et al. developed sets of situational factors (SFs). SFs are those factors (or contextual elements) that are considered to make successful completion of the activities in macrocognition less likely. Compared with the more typically used PSFs in human reliability and performance models, situational factors are more finely grained and are connected with the particulars of the context in which the action is taking place. Table B-1 lists the sets of SFs associated with the activities identified by Roth, Mosleh et al. [9].

Figure B-4 is an adaptation of Figure B-3, showing the application of the macrocognitive functions to power plant operations. (This figure is an update of the model used in the ATHEANA HRA method [4]).

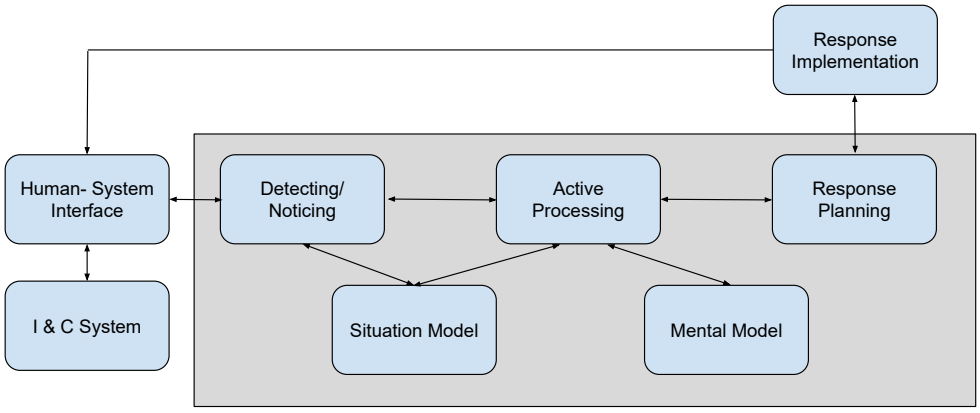


Figure B-4
Basic macrocognitive steps in post-event responses for non-abandonment scenarios

Table B-1
List of situational factors identified in Roth, Mosleh, et al. [9]

Detecting/ Noticing	Sense making/ Understanding	Planning/Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/Directing Personnel	Directing Attention/ Managing Workload
• Large number of simultaneous alarms (that make the key alarm(s) difficult to detect) • Missing information (e.g., failed alarm) • Degraded information (i.e., the primary info is not available and requiring use of the secondary info) • Misleading information (e.g., valve indicates closed when actually partially open)	• Ambiguous cues • Unreliable cues (e.g., indicator has a high false alarm rate) • Multiple malfunctions • High information load (e.g., large number of incoming reports) • Relevant information is distributed over time or space. • Masked cues (e.g., a safety injection masks a small LOCA) • Garden path (initial cues focus operators in wrong direction)	• Mismatch of event evolution with procedures (e.g., plant conditions arise after relevant steps are passed) • Incomplete procedural guidance/ ambiguous or conflicting guidance • Multiple competing goals to balance • Mismatch with expectations based on prior training or experience (regarding appropriate response) • Choice under risk and uncertainty • Workarounds routinely expected	• Complex system dynamics (e.g., shrinks or swells) • Stimulus-response incompatibility (e.g., two controls are spatially crossed with their corresponding displays; moving lever down to increase value) • Multi-mode displays/controls • Inadequate system feedback (feedback about control state is missing or too slow) • Negative transfer - mismatch with required response based on prior training or experience population stereotype violations (e.g., red for normal, green for abnormal)	• Close/frequent communication demands within MCR • Close/frequent communication demands between MCR and outside (e.g., field operators) • Close/frequent coordination demands within MCR • Close/frequent coordination demands between MCR and outside (e.g., field operators) • Other	• Need to supervise and coordinate multiple independent activities in parallel • Unclear lines of authority • Key personnel missing, unavailable or delayed in arrival • Other	• Multiple concurrent demands for operator attention and action • High tempo, time-pressured tasks • Multiple distractions and interruptions • Demands on memory/Need for mental calculation • Need for sustained attention/ continuous monitoring • Psychological stressors; and physical stressors • Other

Table B-1 (continued)
List of situational factors identified in Roth, Mosleh, et al. [9]

Detecting/ Noticing	Sense making/ Understanding	Planning/Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/Directing Personnel	Directing Attention/ Managing Workload
• Small or gradual change • No reason to check • Status of automatic control system/ automatic control actions not clearly indicated (e.g., complex interlocks) • Unfamiliar/ unrecognizable alarm pattern • Other	• Mismatch with expectations based on prior training or experience (wrong mental model) • Other	• Decision has foreseeable grave damage to plant properties, staff safety, and/or society • Other	• Confusable controls/poor control coding (multiple controllers that look alike and are next to each other) • Less than adequate in work space design (e.g., size, orientation, and nominal lighting) • Hazardous, harsh or uncomfortable work environment • Specific tool (not including procedures) required for the action is not available or condition is less than adequate • Other			

In terms of plant operations from the MCR (including during non-abandonment fires), much of the macrocognitive activity is the responsibility of the SS, aided by the ROs providing monitoring and detecting functions and implementing actions. The STA is typically providing support to the SS in assessing the situation and adding knowledge. The MCR team is co-located allowing a level of redundancy (e.g., the SS monitoring the reactor status in addition to the ROs, and the ROs discussing the situation with the SS), and face-to-face communications in a relatively quiet location. It further allows shared access to information (e.g., displays and written documentation). The STA also is typically assisting in communications responsibilities (such as making required notification calls to the NRC, taking calls from the fire brigade, security, health physics, etc.). But, who provides such assistance (e.g., the STA, an extra RO on shift, and other operations personnel that arrive to assist the MCR) varies somewhat between plants.[43] This same model applies prior to the abandonment phase in MCRA fires.

In contrast, Figure B-5 shows the more complex situation once the crew has abandoned the MCR and the SS is managing the response from the RSDP through interactions with staff at one or more local panels. (The figure assumes staff in multiple plant locations.) Now the detection and monitoring activities are based on a combination of direct observations at the RSDP plus communicated inputs from the operators located at the various local panels.[44] Similarly, the response implementation is carried out in part by an RO located with the SS at the RSDP and by other operators at the distributed local panels.

Where and what the STA does following MCRA depends on plant-specific policies. For example, the STA may:

- Accompany the SS to the RSDP, continuing the role of assisting the SS in the decision-making activities
- Go to an alternate RSDP (if the plant has two), assisting the SS via phone or radio, plus performing actions at that RSDP
- Act as a field operator, going to one or more local plant panels to perform necessary actions
- Go to the TSC to take responsibilities in the Emergency Response Organization (ERO)

[43] The set of conditions described in this paragraph (e.g., a single procedure being followed by the entire crew; formal, face-to-face, and real-time communication; indications that can be monitored by all crew members; the expectation that other crew members will provide backup) supports the implicit assumption in most HRA methods that the MCR crew can be treated as a single entity. However, these conditions cannot be assumed to be applicable outside the context of at-power, post-reactor trip, non-abandonment, fire events prior to core damage.

[44] Although there are plant-to-plant variations (see Appendix A for examples), the indications at the RSDP are likely to be different and fewer than in the MCR. Also, RSDPs do not always have alarm panels or SPDS. Such differences can make obtaining information from the RSDP require more effort than to obtain the same information in the MCR.

In these conditions, the SS is reliant on communication systems for receiving information and directing actions; he or she may not have the ability to verify many readings and confirm actions, and the potential exists for him or her to become a “bottleneck” for conveying data between plant operators whose actions must be coordinated. In addition, the SS has the same communications responsibilities at the RSDP as existed in the MCR (e.g., calls to and from the fire brigade) but now may not have the same support from the STA and may not have the same amount or kind of communications equipment.

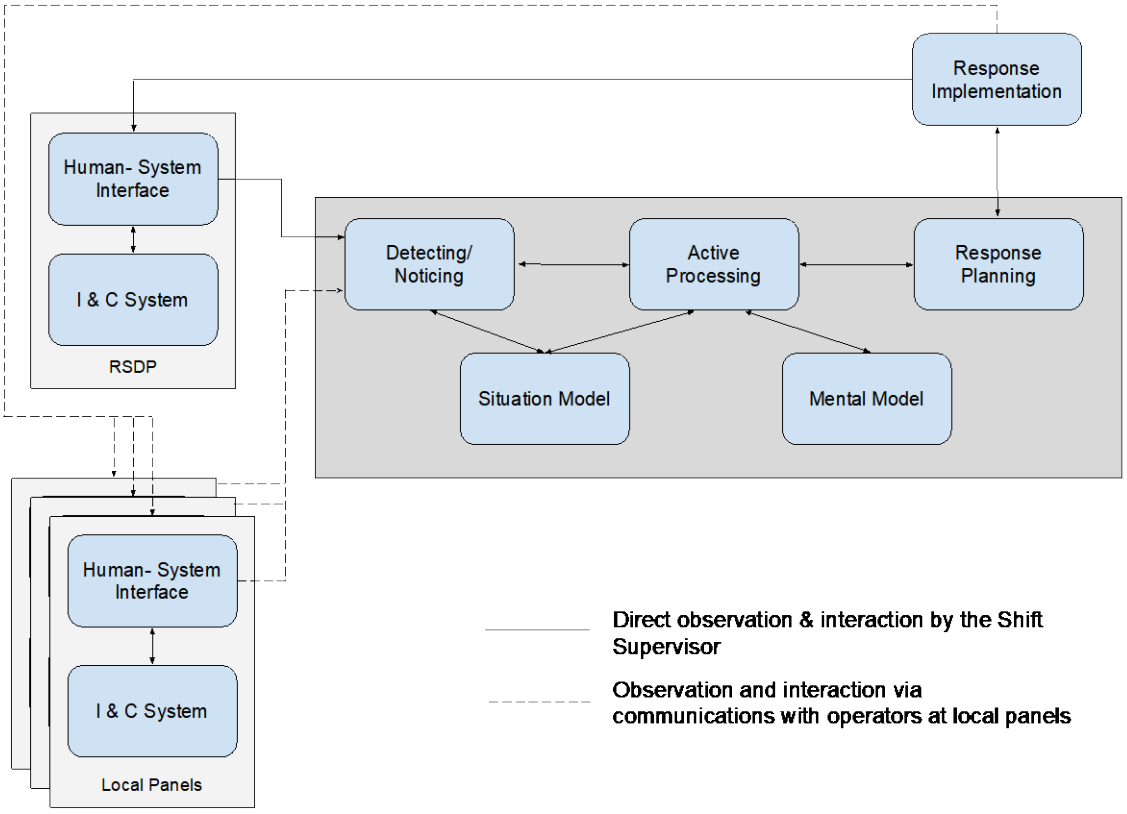


Figure B-5
Basic macrocognitive steps for post-event responses following MCRA

B.2.3 Communications

In terms of the content of communications, Moray [14] has described a set of styles and content of communications for different kinds of team structures from an international perspective. The context that most closely resembles the U.S. NPP practices for normal MCR operations (both at power and for in-MCR responses to prevent core damage) is shown in Figure B-6 (with minor adjustments for routing of communications). In most U.S. NPPs, the hierarchy is such that the SS interacts with the board operators in the control room. The board operators then *look* at the plant via the MCR panels, and take *actions* via the controls. In addition, the plant can *show*, via indications and alarms, when parameters have changed or conditions of importance are arising. In addition, the SS can look at the panels him/herself and see alarms and indications, but rarely takes any direct actions. Working with the board operators, the SS has a variety of types of interactions.

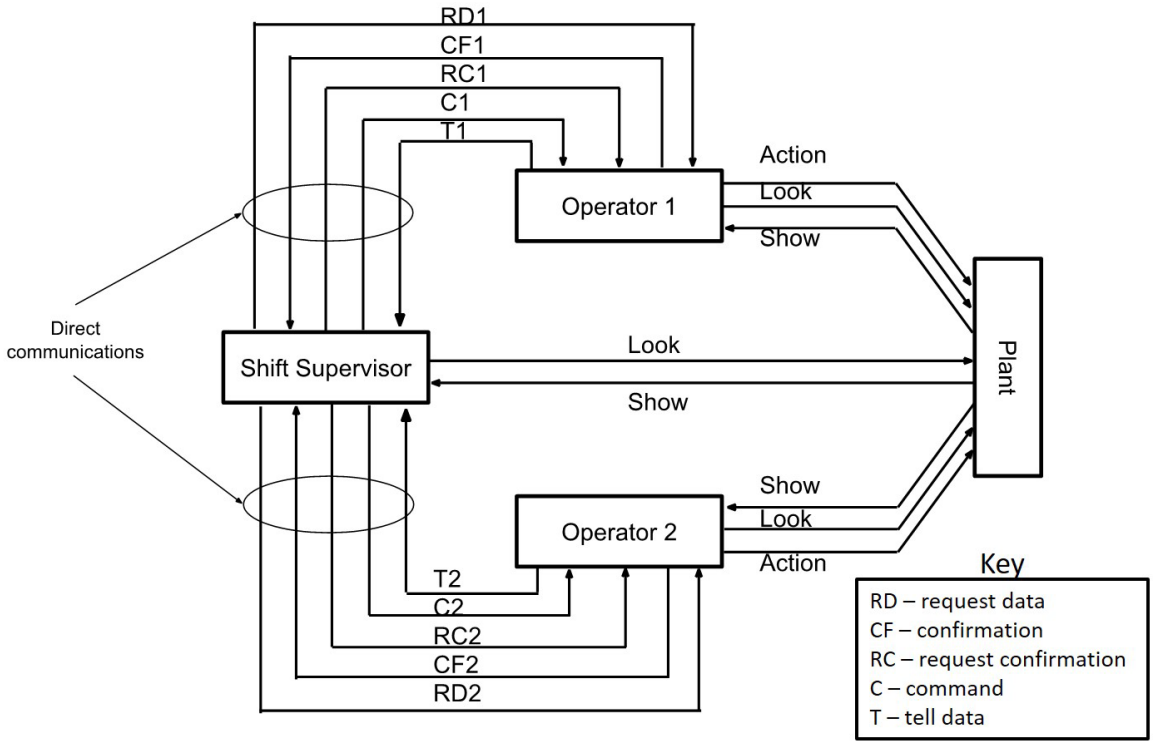


Figure B-6
Communication paths and content for normal MCR operations (based on Moray [14])

Moray identifies these interactions as:

- Requesting data
- Commanding actions
- Requesting confirmations

Similarly, the operator has two types of interactions:

- Telling data
- Providing confirmations

In the case of in-MCR operations, these interactions are direct (i.e., face-to-face, without the need for communication devices). Note that these are very general classes but summarize the essence of communications for the purposes of C&C.

Once the MCR is abandoned, the communication process is quite different, as shown in Figure B-7. Once the abandonment is complete and operators are at the RSDP and/or local control station(s), then the communications with the SS are via communication systems (e.g., radios, phones, etc.) and the interactions, while of the same types as those shown in Figure B-6, are based on the local controls where the operators are located. (There will, in most cases, be more than just two operators reporting to the SS but for the sake of simplicity Figure B-7 just shows two operators.) In addition, it shows direct interactions by the SS with the plant through a RSDP that has both indications and controls—see Section A.3 for a description of the variation in RSDP interfaces following abandonment.

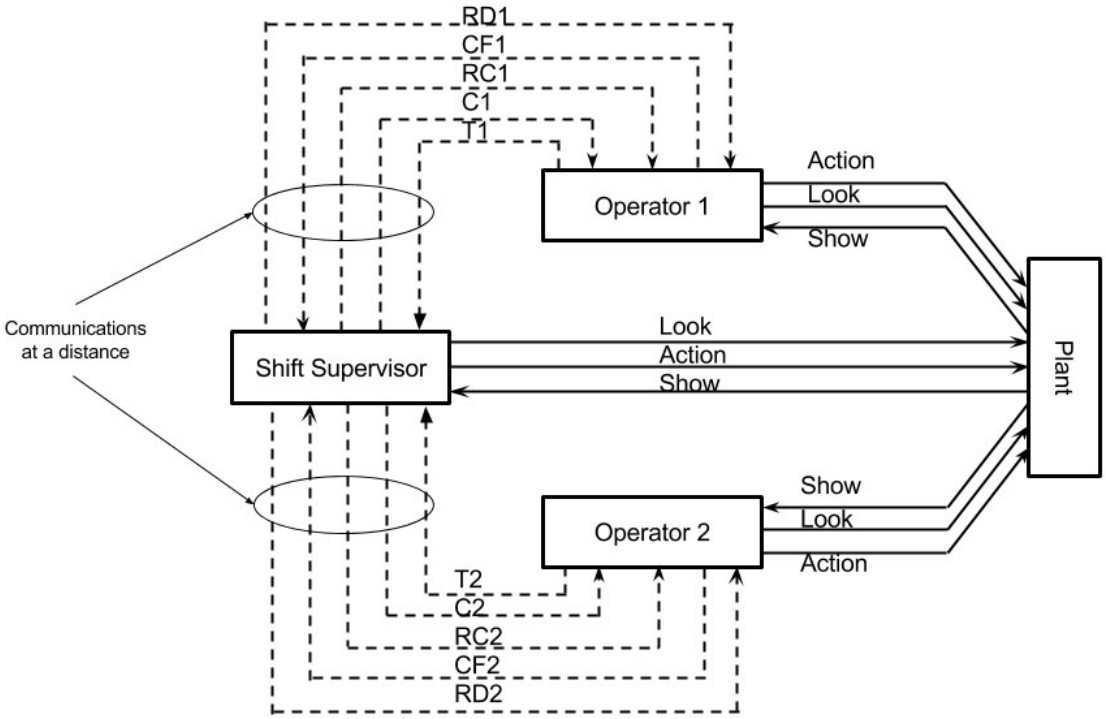


Figure B-7
Communication paths and content for MCRA operations (based on Moray [14])

In addition to interactions with the plant via the operators, the SS is also, in most cases, interacting with the plant via the RSDP, implicit in Figure B-7. As shown in Tables A-1 and A-2, there can be significant variations in the capabilities of RSDPs between plants and therefore the balance of interactions with the plant between the SS/RSDP and plant operators at local plant areas can also vary significantly.

In addition, accomplishing the change in communications from the in-MCR operations to operations from the RSDP can be a significant task. Depending on how often it is practiced in training and how realistic (e.g., establishing and using the number of radios needed, knowing which channels will be used for each function, how the SS will manage the multiple channels and radios at the RSDP), there is the potential for significant delays in getting to the operating state shown in Figure B-7. This potential needs to be judged based on the degree to which these tasks are rehearsed in training, and how broad the training is (e.g., all crews? all members of the crews?).

B.3 Definition of C&C in NPP Setting

The following is the working definition of C&C:

- C&C in NPP operational settings following an initiating event are those processes that ensure:
  - A coherent understanding of the plant state is maintained by the team
  - Timely decision-making is made to maintain plant safety
  - Resources are allocated as needed to ensure safety
  - Team performance is maintained and is coherent between members and across multiple tasks
  - Communications between team members are managed to be timely and effective

These, in many ways, reflect the concepts described by Smalley [3].

Typically, for operator post-initiator response in internal events, C&C is accomplished in the MCR by the SS directing the operating crew's activities (both the MCR board operators and field operators out in the plant) to perform actions identified in relevant procedures. These include, for example, the EOPs for post-initiating-event operations and the fire-related procedures for non-abandonment fires. The SS (and MCR crew) is supported, through a NRC requirement, by a STA who can assist the SS in his/her duties, serving as a "backup" to the entire crew and as an independent observer. Communication within the MCR is face-to-face and real-time, as operators (except those normally working in field positions) are working together through the same procedure and procedure steps. As an event evolves, other plant personnel (e.g., extra ROs or SROs, Shift Manager, other operations or plant management) are likely to be available to assist and support the SS, relieving his/her workload with such duties as:

- Making necessary notifications to the NRC and local authorities
- Taking phone calls from the fire brigade, health physics technicians, and other plant staff
- Necessary, face-to-face interactions between plant staff and MCR personnel (e.g., conferring on maintenance or repair activities, field operators, or technicians that need to check out keys, face-to-face reports)
- Conferring with plant management

In addition, many plants have protocols in place to limit the potential for interruptions disturbing the SS while managing the response, such as identifying designated "no-go" areas for staff who are not part of the MCR operational staff.

One thing to note is, while not considered explicitly in HRA, the additional staff that is likely to be available and the typical protocols regarding entry into the MCR both serve to control or ease the burden of communication for the SS. Also, usually HRA only directly addresses communications between the SS and MCR operators or the SS and field operators; the other types of communications and interactions illustrated above are not usually within the scope of the HRA.

During MCRA scenarios,[45] C&C transitions through a series of contexts whereby the person in charge of responding to the event (typically the SS) must: 1) decide to abandon the MCR, 2) transition to the RSDP, and 3) be responsible for determining what actions are necessary and communicating instructions to staff located in plant areas who are then responsible for taking the actions. These decisions can often be based on reports of indications and measurements communicated to the SS by the staff in distributed plant areas. In addition, the method of implementing the C&C needs by the plant operators at the local panels needs to be considered as part of the HRA.

Perhaps one of the greatest differences between abandonment and non-abandonment scenarios is the degree to which the expected responses are well practiced such that they can be considered recognition-primed decision-making (RPD). The concept of RPD has been developed by Klein [15] to describe the way in which experts rapidly converge on effective solutions to challenges such as those faced by NPP operators in emergencies. One of the core properties of this concept is that the level of expertise is built up through repeated practice from real events (as faced by, for example, fire fighters) and through realistic simulation, such as used in NPP training. RPD and its importance for effective and efficient NPP crew responses is discussed at length in NUREG-2114 [8].

Table B-2 summarizes the differences between the need for consideration of C&C issues in HRA for post-initiator operator actions where the crew remains in the MCR and where abandonment is necessary. Of particular note is the lack of RPD for abandonment scenarios because of the very limited training and realistic simulation practice for such scenarios.

Table B-2
Comparison of C&C issues between non-abandonment and abandonment scenarios

During in-MCR Operations (typical plant)	During MCRA Operations (typical plant)
• Control room team, acting as a single centralized “cognitive entity” – Coordination with fire brigade and some plant area staff • Shared visual cues • Well-rehearsed and tested plans and actions – Resources anticipated and available – Limited need for flexibility in response – RPD • Communications (mostly) face-to-face, voice • Restricted interruptions during response period	• Control room team distributed in plant areas – Shift supervisor alone at RSDP – Coordination with fire brigade and plant areas • Single views of plant information by individuals • Plans and actions occasionally rehearsed, rarely tested – Some resources anticipated and available but complete range untested – Potential need for flexibility in response – Non-RPD response • Communications mostly via radios, phones, etc. • Unknown potential for interruptions

[45] This report assumes the common U.S. arrangement for abandonment of the SS taking control from the RSDP and directing field operators in the plant by communication systems. Some plants may have different arrangements. The same principles apply in these arrangements, substituting the title and location of the person or people in charge for the SS and the RSDP, respectively. Also, there may be special cases where two operators at local panels are in communication with only each other, with one operator designated as the decision-maker.

While the discussion in Section B.2.3 may be helpful in understanding human performance in MCRA scenarios, each plant has a unique C&C structure while inside the MCR and then a different structure while outside the MCR. It is the HRA analyst's role to identify the expected C&C structure outside the MCR. Understanding the C&C structure is the key to understanding the impact on the reliability. The C&C structure can be defined by:

- Identifying the person or people leading the response, as well as each person's role and responsibility following MCRA
- Identifying where the person or people leading the response will be located once outside the MCR
- Evaluating how communications are expected to be performed:
  - Physical process, such as use of radios, sound-powered phones, or other means
  - Protocol, such as three-way communication, required reporting to SS when each step or task is performed or waiting to report until a major function or system is restored
- Identifying how procedures will be used by the person or people in charge and by the field operators – For instance, do the field operators have their own written procedures in hand at plant locations or do they rely only on directions from the person in charge?
- Identifying how many people will require interaction and communication (including plant staff and organizations beyond those needed only for safe shutdown)
- Identifying how much communication will be required to satisfy all communication needs
- Identifying who, beyond the SS, is available to help address communication needs

B.4 Lessons Learned in Event Analysis

To better understand what may occur in an off-normal situation such as MCRA, it is helpful to investigate past events. This investigation may help to identify possible contributing factors as well as broaden the analyst's understanding of what may confound the operator in a similar situation. ATHEANA [4, 5] (especially its retrospective event analysis approach and general perspective on understanding human error) can be particularly helpful in this investigation of past events. Unlike most other HRA methods, ATHEANA does not simply assess HEPs for situations described in general terms defined by a set of PRA-related plant conditions. Rather, "ATHEANA is a method for identifying plausible error-likely situations and potential error-forcing contexts that may result in human failure to correctly perform an action, and for estimating human error probabilities (HEPs) for the human events modeled in probabilistic risk assessments (PRAs)." [5]

The primary way in which ATHEANA is intended to be used is to identify the kinds of credible plant conditions under which the likelihood of failure is significantly higher than what might be called "normal" accident conditions. For example, at the event at Three Mile Island, Unit 2 in March 1979, the operators were misled by the increasing level indication of the pressurizer to believe they should terminate HPI. The particular location of the fault (i.e., the stuck-open pressurizer relief valve) created the impression of overfilling even though the stuck-open valve met the PRA criteria for a LOCA. That is, it was the particular location of the LOCA and its effect on the RCS that created the need in the operators' minds to terminate HPI; it was not

simply a random failure by the operators during a small LOCA. ATHEANA provides a search process to help identify such opportunities. It does this by a guided review of past events, interviews with operators and trainers, and a structured review of failure types for different plant conditions.

Following ATHEANA's approach of looking for operational experience and events relevant to C&C and related activities, one fire event of interest was identified: the March 28, 2010, event at H.B. Robinson, which involved fires in electrical equipment, a reactor trip, a subsequent safety injection actuation, and an "alert" emergency declaration. In the course of this event, several issues associated with operator responses were identified, as summarized in Section B.4.1.

In addition, other non-fire events were reviewed. One additional event of interest was identified in this review: Operators bypassed engineered safety features (ESF) actuation at Crystal River in 1991 in the belief that the transient could be terminated, even though the plant's parameters required activation of ESF. In other words, actions required by safety criteria were deliberately postponed.

B.4.1 H.B. Robinson, Unit 2, Event, 2010

The following summary is taken from the Augmented Inspection Team (AIT) report for this event [16] with more details available in the AIT report.

At 18:52 on March 28, 2010, with the H. B. Robinson Steam Electric Plant, Unit No. 2, operating in Mode 1 at approximately 100% power, an electrical feeder cable failure to 4kV non-vital Bus 5 caused an arc flash and fire. Bus 5 failed to isolate from non-vital 4kV Bus 4 due to a failure of Breaker 52/24 to open, which resulted in reduced voltage to Reactor Coolant Pump (RCP) B and a subsequent reactor trip on Reactor Coolant System (RCS) loop low flow. Subsequent to the reactor trip, an automatic safety injection (SI) occurred due to RCS cooldown. Plant response was complicated by equipment malfunctions and failure of the operating crew to understand plant symptoms and properly control the plant. During plant restoration, the operating crew attempted to reset an electrical distribution system control relay prior to isolating the fault, which reinitiated the electrical fault and caused a second fire.

The AIT report for this event [16] identified:

> The [AIT] team determined that operators exhibited weaknesses in fundamental operator competencies when responding to the event. Specifically, the team determined that the operating crew did not identify important off-normal parameters and alarms in a timely manner, resulting in a failure to recognize an uncontrolled RCS cooldown and a potential challenge to RCP seal cooling.

Specific operational problems identified in the report include [16]:

1. The crew did not recognize the magnitude of the RCS cool down caused by an on-going steam demand.
2. The crew did not recognize that the volume control tank (VCT) level was decreasing, a low VCT level alarm had annunciated, and automatic swap-over of the charging pump suction from the VCT to the refueling water storage tank (RWST) failed to occur, until indicated level in the VCT had decreased to approximately 2-3 inches and charging flow had degraded. Once the crew identified this condition, the RO attempted to manually align the

suction of the charging pumps to the RWST but made an error when performing the alignment. The error left the suction of the charging pumps aligned to the VCT. The Shift Technical Advisor (STA) determined the alignment was incorrect and the RO corrected the error. The crew did not reference APP-003-E3, VCT HI/LO LVL, which provided direction to manually transfer the charging pump suction to the RWST.

3. Following implementation of the EOPs, the operators did not complete a satisfactory review and evaluation of alarm conditions prior to the electrical fault. Instead, the operating crew entered GP-004, Post Trip Stabilization, and attempted to reset the generator lockout relay without using the information in the Annunciator Panel Procedures (APPs) to completely and accurately assess abnormal electric plant status. GP-004 is a normal operating procedure and is written with the assumption that the plant is in a normal (undamaged) configuration. The crew was not aware that a sudden pressure fault signal from the unit auxiliary transformer (UAT) was still applied to the generator lockout circuit logic, as indicated by a locked in UAT fault trip alarm. The attempted reset reenergized Bus 4 and caused a fault at breaker 52/24, initiating the sequence for the second fire. The team concluded that if the crew had performed a thorough control board walkdown, additional electric plant APPs and/or AOPs could have been identified and implemented before exiting to a normal operating procedure (GP-004).

B.4.1.1 Command and Control Issues

Specifically-identified failings related to C&C in the AIT are [16]:

1. The Shift Manager (SM), the overall manager of both units at Robinson, and STA became distracted from oversight of the plant, with the result that the SM consumed 20 to 25 minutes trying to establish the status of the plant, including awareness of major plant parameters such as RCS temperature and pressurizer level, during the response to the fire.
2. The SM did not effectively manage the frequency and duration of crew updates and crew briefs during the early portion of the overall event. Crew updates became so frequent that they interrupted the implementation of emergency procedures and distracted the operators from timely progression through the Path-1 EOP.
3. The SM and CRS (Control Room Supervisor) did not ensure that other control room crew members monitored and diagnosed key plant parameters, such as RCS temperature, pressurizer level, and VCT level.
4. The CRS was unaware that an Auxiliary Operator (AO) assigned to the shift (but not assigned to the Fire Brigade) was available to perform local operator actions contained in the Path-1 EOP. As a result, the B battery charger did not get restarted within 30 minutes of power loss as required by Path-1 (“Restart battery chargers within 30 minutes of power loss using OP-601”).
5. The management expectation for establishing positive control of equipment configuration was not implemented by the operating crew.

6. The SM and CRS did not ensure that sufficient information necessary to assess abnormal electric plant status was collected and evaluated prior to performing steps within a procedure that assumed a normal electric plant configuration.
7. The SM did not use technical resources available in the Outage Command Center (OCC) for performing an assessment of damage to the electric plant before the crew reset the generator lockout relays.

Failings related to resource allocation and utilization identified in the AIT are [16]:

1. Concurrent with board operation (see #2), the Balance of Plant (BOP) operator performed Abnormal Operating Procedure (AOP)-041, Response to Fire Event, during the first fire. The team observed that AOP-041 contains numerous steps to coordinate on-site and off-site fire brigade response and notifications. The team determined that having a licensed operator perform AOP-041, concurrent with the CRS and RO performing emergency operating procedures, is a licensee expectation in accordance with OMM-022, Emergency Operating User's Guide. Through interviews, the team determined that because the BOP operator was performing AOP-041, he was unavailable to assist the control room team in recognizing and diagnosing off-normal events and conditions for approximately the first 30 minutes of the first fire.
2. The two operators responsible for panel operation (the RO and CRS) consistently noted the unavailability of a third person (the BOP licensed operator) to perform independent panel checks. The team noted that during conditions of minimum manning, using the BOP operator to concurrently perform certain AOPs may hinder or prevent him or her from assisting the CRS and RO in stabilizing the plant during events that challenge the control room crew.

Problems associated with training, use of simulators, and operator knowledge were identified in the AIT [16]:

1. The team concluded that training contributed to an incomplete understanding of the plant response during the event by the crew.
2. One potential cognitive bias was displayed by operators during the event. This bias appears to have been introduced during a recent training cycle. During operator interviews, two crew members specifically stated that they knew safety injection was imminent for the event because the "B" RCP was not running. When questioned as to how they knew this, they indicated that the RCS cooldown rate during the event was consistent with what they had seen on the simulator. One operator specifically mentioned that safety injection is an expected response following loss of an RCP with a subsequent reactor trip. These operators believed a safety injection was "normal" for the plant conditions experienced (loss of an RCP) and did not seek out information that would disprove this belief. From the team's evaluation of the sequence of events, it appeared that an expedient response to the RCS cool down rate would have minimized the potential for an automatic safety injection.
3. The team identified a simulator scenario, run within the last year, involving loss of an RCP. This simulator scenario emphasized that loss of an RCP would result in a cool down and subsequent safety injection due to high steam line differential pressure. During the scenario a reactor trip from 50% power was initiated and, at this power level, the reactor trip and loss of an RCP resulted in a safety injection. From interviews and review of additional training lesson plans, the team determined that in the majority of training scenarios when RCP

conditions degrade, the crew rapidly reduced reactor power in anticipation of needing to trip the unit off-line. After a power reduction, other conditions were then introduced in the scenarios to cause the crew to manually trip the reactor and secure the RCP. The lower power condition that is trained on results in a high steam line differential pressure safety injection. However, the plant conditions simulated in these training scenarios are different than the plant conditions experienced during the March 28 event. Plant conditions at full power actually decrease the potential for a safety injection. The team found no evidence that operator training had included a discussion or simulation of the plant response to similar failures at higher power levels.

B.4.2 Crystal River Unit 3 Event, 1991

This event was reviewed and summarized in Appendix A, Section 2.1 of NUREG-1624, Rev.1 [4], which is one of several reports that document the development of ATHEANA. The following is a brief description of the event taken from that report:

> On December 8, 1991, a reactor coolant system (RCS) pressure transient occurred during startup following a reactor power increase. During a normal power increase, the pressurizer spray valve cycled open to control a slight increase in pressure. The actuator for the spray valve failed, which left the valve partly open but position indicating lights showed that the valve was closed. RCS pressure began to decrease and as a result of the erroneous indication, the operators failed to identify the cause. RCS pressure continued to decrease, reaching setpoints for arming the engineered safety features (ESF). Circumventing procedural guidance, operators bypassed ESF for 6 minutes, in anticipation of terminating the transient. Control room supervisors directed operators to take ESF out of bypass and the high-pressure injection system automatically started. Injection was secured because of fears of over-filling the pressurizer but eventually the operators reinitiated injection to increase and stabilize RCS pressure. The pressure transient was terminated after the pressurizer spray line isolation valve was closed, on the suggestion from a supervisor that it might be helpful.

B.4.2.1 Command and Control Issues

The following are the C&C issues as identified in the ATHEANA analysis [4]:

Key Mismatch(es):

- Supervision was not well matched to the inexperience of crew and the unusual plant conditions, in that supervision did not provide guidance for diagnosis or for which procedures to turn to in the early stages of the event.
- Procedures were a weak match for this particular scenario, in that the scenario was not specifically addressed.
- Training (inexperienced crew) was not well matched to this unusual plant condition; snap judgment of situation was incorrect, but adopted by entire crew without question. Strong confirmation bias (assumed cooldown confirmed by decreasing pressure, closed indications for the power-operated relief valve (PORV) and spray valve, and field reports of steam flow to the deaerators) led to failure to use procedures and failure to notice contradictory evidence.

Most Negative Influences:

- Both procedures and training were unclear regarding diagnosis of decreasing system pressure. (PSF)
- There was no indication of spray line flow to use to verify the valve position. (PSF)
- Training was not sufficient to prevent operators from taking action that was against procedure and policy (bypassing ESF system). (PSF)

Most Positive Influences:

- That experienced plant management was in the control room to advise in two key instances 1) to “unbypass” ESF system, and 2) to close the spray isolation valve. (Plant Condition)

The significance of this event from the perspective of C&C is that operators can delay taking actions, even when the procedure's criteria have been met to perform the action. The possibility exists that operators could be more willing to delay abandoning the MCR even though evacuation criteria have been met, since the MCR is the control center with which they are most familiar.

B.4.3 Event Analysis Conclusions

While ATHEANA is based on the concept of looking for examples of prior events where operators have demonstrated significant problems with specific combinations of plant conditions and operational factors (like PSFs), the fact is that there have been few instances of plant fires involving significant operational problems; the Robinson event is one. However, the example from Crystal River suggests that there are lessons from non-fire events that could apply equally to fire and MCRA events.[46]

B.5 Interim Guidance for Incorporating C&C in MCRA Scenarios

This section discusses preliminary concepts for addressing C&C in MCRA models and HFEs. It is not intended to be an exhaustive treatment, but provides interim guidance based on the background and initial research conducted and the experience of the authors.

The key to identifying whether or not C&C plays a role in the modeling and HFE definition for MCRA is the determination of the type and nature of cognitive processing that is involved in the MCRA tasks. As discussed previously, C&C generally involves the SS playing the central role of organizing and mediating the actions of other operators.

If it is determined that without this oversight and direction, the cognitive aspects of the task would fail, then some modeling of these aspects, either in the PRA model or in individual HFEs, should be included.

[46] These two events are examples, and do not represent the results of a systematic review of operational events.

These C&C aspects should be distinguished from the cognitive decision-making that is conventionally included in a given HFE based on co-located crew in the MCR. In those cases, all members of the crew are viewing the same indications and going collectively through (primarily) the same procedure. The entire crew can see and hear the same visual and audible inputs and hear commands from the SS. The cognition is therefore reflective of a communal decision-making. The SS ultimately makes the decisions, but the rest of the crew provides input on that decision so that decision may be considered to be more group-oriented.

For the MCRA case, the most common types of issues related to C&C include:

1. The decision to abandon on LOC, where the SS is responsible for making the decision based on an evaluation of the various inputs from the MCR indication (including the lack of it) and from field reports of fire severity and impacts to equipment,
2. Depending upon the complexity involved, the set of actions that are managed and monitored by the SS to transfer C&C from the MCR to the RSDP(s) and/or local control stations,
3. Coordination by the SS of tasks following MCRA that are performed by distributed operators, where the combined set of tasks require specific monitoring and direction for successful completion, and
4. C&C-related PSF influences within a given MCRA HFE.

Table B-3 provides a framework for potential treatment of the different aspects of C&C throughout the different phases of MCRA. This framework will be further examined and developed as part of the MCRA quantification effort.

Table B-3
C&C considerations during each phase of MCRA

Command and Control Attribute (from Section B.2)	Phase I – Before the Decision to Abandon	Phase II – During the Decision to Abandon (Note: since Ph. II is typically a single HFE, the factors below would be considered in the HEP development)	Phase III – After the Decision to Abandon
Situational Awareness	Addressed in cognitive models, multiple cues, indications, and staff result in optimal support of C&C such that C&C failures are negligible.	For LOH, situational awareness is not assessed to be an issue due to the global nature of the smoke and heat. For LOC, situational awareness is a potential issue. LOC may result from either failure of the switches and circuits used to start, stop, and control components such as pumps and valves. LOC may also result from instrumentation failures that fail to automatically start SSCs and also fail to give the operators the proper picture of the current plant status. Thus, failures of instrumentation potentially lead to a loss of situational awareness and this may impact the decision to abandon following a fire that leads to LOC.	Treat as a global impact on all operator actions where failure to establish and maintain situational awareness leads to failure of all actions. A single HFE may be used to represent a failure to understand the situation, especially if information is coming from multiple sources that are not co-located. Time lag may be also be a consideration. Given success of the general (global) action, additional situational awareness may be needed for individual HFEs that are part of Phase III. For example, if a plant cooldown is required then establishing and monitoring a cooldown rate for the duration of the cooldown typically requires a longer awareness of the situation than starting a pump. Current HRA methods address this for individual HFEs.
Timely Decision-Making	Addressed in cognitive models, multiple cues, indications, and staff result in optimal support of C&C such that C&C failures are negligible.	For LOH, timeliness is not assessed to be an issue due to the global nature of the smoke and heat, which have been growing since the start of the fire. For LOC, timeliness is a potential issue. Failure to establish and train on straight-forward, objective, measurable criteria will likely lead to delays that would impact the decision to abandon following a fire that leads to LOC.	May be included as part of the single HFE for situational awareness. Given success of the general (global) action, additional time-challenges may be encountered for individual HFEs that are part of Phase III. Current HRA methods address this for individual HFEs.

Table B-3 (continued)
C&C considerations during each phase of MCRA

Command and Control Attribute (from Section B.2)	Phase I – Before the Decision to Abandon	Phase II – During the Decision to Abandon (Note: since Ph. II is typically a single HFE, the factors below would be considered in the HEP development)	Phase III – After the Decision to Abandon
Resources Allocated	Addressed as a PSF in the qualitative analysis, looking for staffing constraints.	The decision to abandon typically is made by the MCR staff, for which there is a minimum staffing requirement. Thus, lack of resources (insufficient allocation) is not likely to impact the decision to abandon.	MCRA procedures are typically well scripted with roles for a minimal staffing contingent. Thus, consideration of an impact on all HFEs is not warranted. However, this lack of impact may be challenged by additional, random failures in the train credited for safe shutdown, especially those requiring additional, local manual actions (recovery actions). These failures would likely impact individual HFEs.
Coordination of Actions	Coordination is not typically addressed as a PSF in the qualitative analysis. However, current HRA methods typically include coordination by making one HFE dependent on another HFE and also ensuring the time required for response includes time needed to conduct and complete the coordinating activity.	For LOH, the decision to abandon typically does not require coordination. For LOC, the decision to abandon may involve coordination with local staff that are dispatched to check cues and indications located outside of the MCR.	MCRA procedures are typically well scripted and address coordination between operators. Thus, consideration of an impact on all HFEs is likely not warranted. However, coordination challenges may be associated with one (or some) individual HFEs.
Communications	While communications may be considered in feasibility, communications are not typically addressed as a PSF in the qualitative analysis. Additionally, current HRA methods typically do not address communications issues.	For LOH, the decision to abandon typically does not require additional communications systems or protocols. For LOC, the decision to abandon may involve coordination with local staff that are dispatched to check cues and indications located outside of the MCR.	MCRA procedures are typically well scripted and address communications between operators. Thus, consideration of an impact on all HFEs is likely not warranted unless the procedures did not have a means to address distractions on the staff monitoring and operating the safe shutdown components. Additionally, communication challenges may be associated with one (or some) individual HFEs.

B.5.1 Incorporating C&C in MCRA Models

Guidance is provided in Section 3 regarding the first two C&C cases that require specific treatment with separate HFEs in the model, but this section introduces the third case for a post-abandonment C&C HFE. More generally, Section B.5 of this appendix provides interim guidance on the aspects of HRA for C&C, and a list of areas for intended development.

B.5.1.1 Decision to Abandon HFE

Section 3.2.4 discusses the inclusion in the fire PRA model of a separate HFE for the failure of decision to abandon such that the failure of this decision would result in the failure of all actions associated with the abandonment procedure. This HFE is represented as H-MCRA-COG in the example fault trees provided in Figures 3-3 and 3-4 (see additional guidance in Sections 4 and 5).

B.5.1.2 C&C HFE for Transfer of Control from MCR to RSDP(s) or Local Station(s)

Section 3.4.2 discusses modeling the set of actions associated with the transfer of control from the MCR to the RSDP(s) or station(s). These are commonly referred to as the “enabling” actions: they isolate the control circuits in the MCR and activate (or permit) the local control circuits to allow operation of the required equipment locally at the panels/stations. These transfer-of-control actions can be assumed to all be required in order for the MCRA to be successful, and should be incorporated into the model such that failure to transfer control leads to a failure of the MCRA scenario. For that reason, these actions can be incorporated into a single HFE in the model. For the LOC case, they could be considered as the execution part of the cognitive failure to abandon, but a separate HFE would be required for the LOH case, since there is no cognitive failure to abandon in that case.

This HFE is represented as H-MCRA-EXE in the example fault trees provided in Figures 3-3 and 3-4. This HFE is developed through a review of the MCRA procedure to identify the transfer steps. The logic model shown in Section 3 also reflects the equipment required for this transfer

It should be noted, however, that these transfer of control actions may be sufficiently clear or simple or may be performed by a single operator, in which case a separate HFE may not be necessary and/or C&C issues may not apply.

B.5.1.3 C&C HFE for Complex MCRA Tasks After Abandonment

The example fault trees provided in Figures 3-3 and 3-4 include a gate named H-SYS-X-MCRA-AFTER. This gate includes the actions that take place after abandonment that will fail the restoration of the specific system under abandonment conditions, regardless of the cause of the abandonment. Two modeling approaches are identified where either (a) the distinction between certain actions based on relevance to the scenario (e.g., diesel start and load shedding actions for AC power recovery cases) may be functionally warranted, or (b) where all individual actions required could be represented by a single HFE that represents the bounding case for failing to successfully reach a safe, and stable condition (i.e., it would include all actions required to recover all systems addressed by the MCRA procedure).

In the latter case, C&C aspects would be considered as PSFs within the boundary of the single HFE, as discussed in Section B.5.2.

However, in the former case, if the complexity of the C&C warrants, a separate C&C HFE could be identified under this gate to characterize and evaluate the diagnosis, decision-making and coordination required by the SS to ensure that the functional tasks are properly performed.

In many cases, the MCRA procedure is organized as separate attachments that are performed by individual operators at various locations in the plant. Often these attachments are self-inclusive and include clear, step-wise direction that does not require interface with the other operators and their attachments. The operator is simply required to report the completion of the attachment to the SS, who is usually stationed at an RSDP. In these cases, the individual operators located throughout the plant do not require situational awareness for all aspects of the plant.

In other instances, however, these attachments contain coordination points that depend on other attachments, for example, stating that the completion of one step in Attachment A is dependent upon (and must wait for) completion of a step in Attachment B. If there are multiple attachments, which is often the case, and multiple interactions between them, these “hold points” could become opportunities for failure to perform the actions in the proper order, which could lead to failure of the post-abandonment ex-MCR actions. Communication is also associated with these “hold points.” The procedure directs the operator to report to the other operator and the SS when a step that is a prerequisite to another attachment has been completed. The next step in the dependent attachment cannot be performed until the operator receives confirmation that the prerequisite step is complete. Although this situation may not require a complete situational awareness by the local operators, a certain level of awareness (particularly the actions of other operators) is needed by them in order to correctly coordinate the actions.

The definition of a separate C&C HFE under the H-SYS-X-MCRA-AFTER gate would need to be coordinated and discussed with the PRA analyst to ensure that the individual operator actions coordinated by the C&C HFE are properly represented in the model. The definition of this HFE should be consistent with guidance provided in Section 5. The timing of this C&C HFE would need to consider the Phase III timing discussed in Section 7 and the timing of the individual system/function actions being coordinated.

B.5.2 Situational Factors Influencing C&C in MCRA HFEs

The purpose of this section is to provide an integrated perspective of the factors surrounding the C&C issues for each timeframe and location, specifically for the context of MCRA scenarios. Roth, Mosleh, et al. [9] developed sets of SFs based on the model described (Section B.2.2 and Table B-1). These SFs may be considered in light of the timeframes in which C&C may be particularly relevant. Although the model and SFs described in Roth, Mosleh, et al. present one way in which to consider the effects of C&C, it is not suggested that it presents the complete picture or captures all the complexity inherent in the impact of C&C.

There are two primary timeframes for considering C&C effectiveness: the time up to abandonment of the MCR, and post abandonment. The actions taken to transfer control outside the MCR, if sufficiently complex, can be considered comparable to post-abandonment actions. The time up to abandonment is considered separately for LOH and LOC scenarios as the SFs are somewhat different. During the post-abandonment phase, C&C issues need to be considered

both at the RSDP and at the plant areas. Thus, there are four contexts to be assessed for C&C issues, pre-abandonment for LOH and LOC, post-abandonment at the RSDP, and post-abandonment at other plant areas. The subsections below describe how the SFs apply to each time phase and context.

Situational factors related to MCRA analyses are presented in Tables B-4, B-5, B-6 and B-7. The SFs listed in these tables are considered to make the decision to abandon less likely or delayed for LOH scenarios (Table B-4) or for LOC scenarios (Table B-5). The SFs in Table B-6 are considered to make the post-abandonment responses at the RSDP less reliable or timely, and those in Table B-7 to make the post-abandonment responses at the plant locations less reliable or timely.

While every plant has unique designs for the interfaces for controls, indications, and manually operated devices, NRC's guidelines for the review of human-system interfaces, NUREG-0700 [17], sets standards for these and other command and control-related systems (like communications and environments). While these guidelines are primarily seen as relating to the design of the MCR, they do limit (if fully applied) the extent to which the SFs developed by Roth, Mosleh, et al. [9] can play a role in creating opportunities for human-performance problems outside the MCR. The assessment of the local control stations and the RSDP should still be assessed against the PSFs discussed earlier in Section 8.

B.5.2.1 Pre-Abandonment Actions

The analysis of the decision to abandon the MCR is discussed in Section 4, but this section specifically addresses the C&C issues related to this decision.

LOH Scenarios

As discussed in Section 4, there is very little potential for failure to abandon during LOH events as the compelling effects of fire on the MCR environment are clear and direct—at least in terms of the actions as modeled in the PRA.[47] The only potential SF is the possible stress from a reluctance to abandon control from the MCR because of the change from a familiar to an unfamiliar setting. Since this is a scenario for which training is required, in practice this is not likely to be a significant issue when training is frequent.

1. The SS (and the rest of the crew) could be feeling greater stress compared to responding to plant events for which more frequent simulator training is provided. (*Directing attention/managing workload*)

LOC Scenarios

Unlike the LOH case that has immediate and unambiguous cues of the need to abandon the MCR, the cues for abandonment in LOC scenarios may not be as direct or obvious. As discussed in Section 4.3, there may not be specific guidance in the procedures on what constitutes the required evidence of a LOC scenario needing abandonment. In addition, fire alarms, local verification of the fire severity and location, and the failure of controls and

[47] Some reviewers consider that the decision to abandon in LOH scenarios may well come before the criteria are met; however, this would have the effect of extending the time for the post-abandonment response beyond that assumed in the current HRA models as discussed in Sections 4 and 7 of this report.

indications in the MCR require the operators (particularly the SS) to determine whether the degree of damage is sufficient to require abandonment, for example:

1. The cues, indications, components, and systems that are required to safely shutdown the plant following EOP guidance may be impacted by the fire. When these systems, components, and indications are unavailable (from the MCR) or their status cannot be determined from the MCR, then operators will be forced to make the decision to control the plant from outside the MCR. (*Detecting/noticing and sense making/understanding*)
2. There may be a high information load on the SS associated with understanding the causes of multiple, fire-induced, plant indications, from comprehending potentially-false equipment alarms and the potential for verbal/phone/radio reports from plant areas associated with the fire. (*Sense making/understanding*)
3. There is considerable variability in the level of guidance provided for abandoning the MCR during fires, especially when due to LOC. Deciding to abandon the MCR is likely to prove stressful in the absence of explicit training for the abandonment-decision-making portion of LOC events. (*Incomplete procedural guidance*)
4. The decision to abandon the MCR will likely be made with great reluctance since the MCR is: (a) the place the operating crew is most familiar with and practiced in using as a team, and (b) the location where the greatest resources are available (documentation, communications, etc.). Abandoning the MCR will also likely create concern among the plant staff, since it indicates a severe event. (*Decision has foreseeable potential consequences to the plant and the staff*)
5. During the time to decide to abandon, it is likely that the SS will be receiving much information from both the MCR and plant areas about the fire and its effects. The information and the need to decide will be fast paced and there are potentially many interruptions and distractions. (*Directing attention/managing workload*)
6. Given items 4 and 5 above, the SS (and the rest of the crew) will likely be feeling significantly greater stress compared to responding to plant events for which frequent simulator training is provided. (*Directing attention/managing workload*)

B.5.2.2 Transfer of Control and Post Abandonment Actions

Following the decision to abandon, the control of the plant is transferred from the MCR to the RSDP. The post-abandonment operations comprise the activities necessary to ensure a safe shutdown once the MCR has been abandoned.

Operations at the RSDP

1. The first actions taken when transitioning from the MCR to the RSDP(s) are to officially transfer control to the RSDP. This can be done via transfer switches or multiple actions to activate the RSDP(s). The SS will be following the MCRA procedure, but, depending upon the complexity of these actions and if the control is distributed among several RSDPs or a combination of RSDPs and local control stations, it may be necessary for the SS to coordinate these actions to ensure all of the control stations have been properly enabled. (*Directing attention/managing workload and manipulating/acting*)

2. Once the SS has left the MCR, the information available outside the MCR will, in most cases, be less than what would be available in the MCR during normal operations and during non-abandonment fires. While the information at the RSDP may be adequate for the range of plant conditions it was designed for, it is likely that the SS will need to ensure that there are no conditions arising that would further complicate the response. Information that is not available at the RSDP will need to be obtained from plant areas from local operators using communication systems. (*Detecting/noticing*)
3. Because of the need to process reported information from plant areas, it is likely that the SS will face a high information workload compared with operations in the MCR due to having to keep track of reported values, etc., rather than rely on face-to-face reports and direct observations. (*Sense making/understanding*)
4. Unlike operations in the MCR, it may be that the SS and plant operators do not have a well-designed work place in terms of the adequacy of workspace, lighting, noise, etc., and the design of the control interface that may make reviewing information and taking actions more difficult. (*Manipulating/acting*)
5. To take actions, the plant personnel will not be using the normal controls with which they are most familiar (in the MCR) but, instead, will be using the other controls and indications at the RSDP and plant areas. The possibility exists that the RSDP is not designed to modern human-factors standards. The NUREG/CR-6146 [18] review of local control stations identified human factors concerns such as inadequate or confusing labeling, controls that violated population stereotype, and inadequate position indication for valves. Even if upgrades were performed, labels might have been added that contained more information than necessary and are therefore hard for operators to read. While the guidelines of NUREG-0700 [17] (or equivalent) apply to control stations outside the MCR, the level of guidance is less extensive, and therefore the operators may have to be more vigilant in selecting controls or indications. (*Manipulating/acting*)
6. Perhaps the most significant SF associated with MCRA is the need for close and frequent communications and coordination between the RSDP and the field operators in the plant areas. (*Communicating/coordinating*)
7. When field operators are in multiple locations, the SS has to coordinate and oversee the activities of each individual (even if they have their own local procedures) in parallel, which involves a significant workload using communications systems. In most cases, there will need to be multiple channels of communication available; the management of these multiple channels (such as several radio channels or even multiple radios) will be a significant challenge. (*Supervising/directing personnel*)
8. Because field operators may have to access areas that are security-protected or involve accessing radiation barriers, it may take significant time for the staff to reach their control positions, which would delay their ability to perform their actions. (*Supervising/directing personnel*)
9. The need to supervise and direct the field operators during the post-abandonment period will involve multiple, concurrent demands on the SS. These demands will probably be high-tempo at times while coping with interruptions from other operators (and possibly plant management). This post-abandonment period will involve periods of sustained attention and monitoring to cope with the workload and the interruptions, which will be stressful. Further, the potential exists for a need to remember data in the absence of the normal MCR displays and paperwork. (*Directing attention/managing workload*)

Operations in Other Plant Areas

1. The potential exists for field operators in plant areas to have to use indications and controls that are not ideally designed from a human-factors perspective. Section 12.2 of NUREG-0700 [17] requires indications and controls at local control stations to be designed not to violate population stereotypes or to have to identify displays and indications in a confused design. However, as the NUREG/CR-6146 [18] review of local control stations indicated, this requirement may not result in designs that meet the full specifications of NUREG-0700. *(Manipulating/acting)*
2. Operations in plant areas can involve harsh or uncomfortable environments. *(Manipulating/acting)*
3. Frequent communications between the SS and the field operators will be required. *(Communicating/ Coordinating)*
4. In some circumstances (depending on the accident scenario and required operator actions), operators may be involved in performing concurrent or "close-in-time" actions with associated time pressure. Actions may require sustained or continuous monitoring and may be performed in the face of multiple distractions or interruptions (due to communications needs, for example). Operators may need to remember data values or perform mental calculations as parameters change. *(Directing Attention/ Managing Workload)*

B.5.3 Addressing C&C in MCRA HFEs

The previous section identified SFs that have the potential to degrade human performance for both the period leading up to the decision to abandon and the post-abandonment period. Actions for both sets of SFs relate to broadly similar PSFs. These are discussed in Sections B.5.3.1 through B.5.3.10. More specific guidance on the assessment of PSFs is provided in Section 8.

B.5.3.1 Complexity and Stress

From the operating crew's perspective, complexity and stress are intertwined: the greater the complexity the greater the stress. The major sources of complexity and stress are:

- The need to abandon the familiarity of operating from the MCR for operations in locations that are rarely if ever used in practice
- SS having to cope with control via communications at a distance and potentially having to cope with multiple distractions and simultaneous communications
- SS coping with uncertainties about what the plant behavior is (compared with the information available in the MCR)

The analyst needs to consider the extent to which these sources can degrade the performance (particularly of the SS) to respond to the situation in a highly reliable and efficient manner. In many ways, complexity and stress represent challenges to C&C; the more complex the event, the greater the stress and a greater need for effective C&C. Any weaknesses, therefore, in the PSFs discussed below will likely increase the disruptive effects of complexity and stress.

In addition, the analyst needs to assess the levels of workload, leading to time pressure and stress, on the SS and the field operators before the decision to abandon and in the control period following abandonment.

B.5.3.2 Crew Dynamics

Because C&C is different for MCRA than for actions in the MCR, the assessment of crew dynamics is an essential consideration in C&C.

Pre-Abandonment

For the most part, the SS will be in charge of the decision to abandon the MCR, but the dynamics about how inputs to that decision are relayed depends upon which crew members are tasked with monitoring what parameters or set of parameters. It is often the case that a field operator is tasked with going to the source of ex-MCR fires that cause abandonment to do a visual check, confirm the fire location and severity, and report back to the MCR. Other ROs may be tasked with the activities to transfer control to the RSDP or local stations prior to leaving the MCR.

The MCRA procedures will indicate who is responsible for doing what, but the SS is generally the ultimate decision-maker and the person conducting C&C for the operation.

Post-Abandonment

At some plants, in addition to the SS providing C&C at the RSDP, the STA may play a role in maintaining the “big picture” of the situation and may assist with monitoring parameters and following the procedure(s). At other plants, the STA may be deployed as a field operator to take actions as directed by the SS. The use of the STA as an additional resource is plant-specific and needs to be determined based on interviews and observation of simulator exercises.

The distribution of crew members who take an MCRA procedure attachment and perform it independently with potentially no additional crew backup (as would be available for actions performed in the MCR) is another C&C factor for consideration.

B.5.3.3 Communications

Pre-Abandonment

Prior to MCRA, information flow about the status of the fire (depending on its location and how visible it is) is an important input. This information could be directly solicited by the SS by contacting a field operator to obtain visual confirmation about the fire location and severity. However, it is also possible that the SS in the MCR will become flooded with calls and other communication inputs coming in from plant operators outside the MCR who are noticing “odd” plant behavior. On top of the information the SS is processing regarding loss of MCR instrumentation and control, these additional calls may become a distraction to the SS while making the decision to abandon the MCR. The analyst should evaluate through operator interviews and, ideally, through observation of simulator training exercise(s) whether these distractions are a potential source of delay in making the decision to abandon the MCR. See Section 6 concerning the feasibility of communications based on the plant’s MCRA communication plan.

Post-Abandonment

Following MCRA, many of the control actions will be directed by the SS from the RSDP using any or all of the communications systems available to him/her. The analyst needs to assess how reliable and effective the available communications systems are between the RSDP and all the control stations in the plant that are necessary for performing post-abandonment actions. In particular, the analyst needs to make a judgment as to the plant's use of techniques and protocols that increase the effectiveness of communications (for example, 3-way communications) when the technology used for communications may not be ideal. As discussed in Section 6, there should be a communications plan, including an expected level of staffing to support the amount of increased communications. There are many possible impacts of ineffective communication, including miscommunication of indications, excessive workload due to inadequate communications plan, and delay of actions.

B.5.3.4 Cues and Indications

Pre-Abandonment

The analyst should consider the degree to which spurious (false) cues and indications will be present, particularly for LOC events that have the potential to slow down the response of crews to decide that the fire is real and that the MCR needs to be abandoned.

Post-Abandonment

The limited information provided at the RSDP will require the SS to rely on information provided by field operators in plant areas. The location of such information sources may or may not be well designed in terms of access, observability, and ergonomic design. The analyst needs to ensure that the relevant information can be obtained reliably and in a timely manner.

The limited information available at the RSDP may leave the SS concerned that there are conditions in the plant that he/she cannot observe which may act to distract him/her. The analyst can inquire during interviews as to whether there any concerns by the SS or staff as to plant conditions they may not be able to observe that might act as a distraction or source of stress.

B.5.3.5 Procedures

Pre-Abandonment

To assess how long it will likely take for the SS to decide to abandon the MCR in an LOC, the analyst should consider the amount and level of detail of procedural guidance provided to operators concerning when to abandon the MCR in LOC scenarios.

Post-Abandonment

The analyst should evaluate the degree to which the procedures provide the necessary guidance to the SS for monitoring and coordinating the actions of the field operators. For example, the analyst should identify specific procedural hold points and coordination points between operators and communication points that provide the SS with the status of the overall plant response. The analyst should consider that there is a trade-off between information flow and the amount of workload on the SS. Without sufficient information, the SS does not obtain crucial input; however, with too much information, the SS could be overwhelmed such that C&C becomes challenging.

B.5.3.6 Training

Pre-Abandonment

It is possible that the training may not specifically cover the decision to abandon itself, but that the trainers provide the basis or rationale for abandonment to the crew, such as “a sabotage event that requires a MCRA.” The analyst must, therefore, evaluate whether the timing allocated to the decision process should be increased to reflect any potential uncertainty. If training does cover the decision-making process, analysts should note whether training augments the procedural direction and, if so, how.

Training for the abandonment scenarios has the capability of reducing the stress and workload on the SS (by making the task more familiar) and ensuring that the necessary tools, procedures, knowledge of work locations, etc. have been preplanned. The analyst should assess the effectiveness of any integrated training of MCRA in providing this familiarity and reducing the stress and workload on the SS.

B.5.3.7 Timing

Assessing the timescale for MCRA actions is discussed in Section 7 and the elements associated with the decision to abandon are discussed in Section 4. For assessing the timing influences on C&C, the analyst needs to ensure that the times available for operator decisions and actions account for coordination, communication, delegation, and potential interruptions and calls.

Poorly performed C&C will most likely result in using up the time available and lead to a reduced “margin for maneuver.” As indicated in the example of the H.B. Robinson fire, the SM consumed 20 to 25 minutes trying to establish the big picture, thereby distracting the STA. The SM was already under caution by the utility for poor C&C performance. As a result of poor management, the SS and RO carried out step-by-step EOPs independent of the SM and STA.

An example of a scale of the C&C influences on timing can be considered as follows:

A. Good: Imposes no time penalty on performance vs. time available

B. Moderate: Imposes some time penalty to perform overall tasks vs. time available

C. Poor: Imposes significant time penalty to perform overall tasks vs. time available

B.5.3.8 Human Machine Interface

A walkthrough of the MCRA strategy should be conducted to see the RSDP, access local areas where actions will occur, and to note the key parameter indicators and interface points at each location to see whether they appear clear or confusing.

B.5.3.9 Environment

The analyst should evaluate whether the environment at the RSDP could be an influence on the C&C of the process, by virtue of being poorly lit, cramped, noisy, or hot.

B.5.3.10 Staffing and Availability

Procedures are evaluated during training to find the proper balance between staffing and task performance. However, since the analyst is developing a timeline for MCRA, he/she should evaluate the availability of staff to perform the required MCRA actions based on observations of walk/talk-throughs and simulator exercises. The analyst should determine whether C&C is challenged by waiting on one operator to complete more tasks than they can reasonably handle (either due to travel to multiple locations or the complexity of the task) within the required timeframe.

Table B-4
List of situational factors associated with decision to abandon MCR (LOH)

Detecting/ Noticing	Sense Making/ Understanding	Planning/ Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/ Directing Personnel	Directing Attention/ Managing Workload
• None	• None	• None	• None	• None	• None	• Psychological stressors and physical stressors

Table B-5
List of situational factors associated with decision to abandon MCR (LOC)

Detecting/ Noticing	Sense Making/ Understanding	Planning/ Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/ Directing Personnel	Directing Attention/ Managing Workload
• Missing information (e.g., failed alarm) • Degraded information (i.e., the primary info is not available, which requires the use of secondary info) • Misleading information (e.g., valve indicates closed when actually partially open) • Status of automatic control system/automatic control actions not clearly indicated (e.g., complex interlocks) • Unfamiliar or unrecognizable alarm pattern	• Ambiguous cues • Unreliable cues (e.g., indicator has a high false alarm rate) • Multiple malfunctions • High information load (e.g., large number of incoming reports)	• Incomplete procedural guidance • Ambiguous or conflicting guidance • Decision has foreseeable grave damage to plant properties, staff safety, and/or society	• None	• None	• None	• Multiple concurrent demands for operator attention and action • High tempo, time-pressured tasks • Multiple distractions and interruptions • Psychological stressors and physical stressors

Table B-6
Hierarchical list of situational factors associated with post-abandonment responses at RSDP

Detecting/ Noticing	Sense Making/ Understanding	Planning/ Deciding	Manipulating/ Acting	Communicating / Coordinating (Teamwork Functions)	Supervising/ Directing Personnel	Directing Attention/ Managing Workload
• Degraded information (i.e., the primary info is not available, which requires the use of secondary info)	• High information load (e.g., large number of incoming reports)	• None	• Inadequate system feedback (feedback about control state is missing or too slow) • Population stereotype violations (e.g., red for normal, green for abnormal) • Confusable controls/Poor control coding (multiple controllers that look alike and are next to each other). • Less than adequate work space design (e.g., size, orientation, and nominal lighting) • Hazardous, harsh or uncomfortable work environment	• Close/frequent communications and coordination between RSDP and field operators in plant areas	• Need to supervise and coordinate multiple independent activities in parallel • Key personnel missing, unavailable, or delayed in arrival	• Multiple, concurrent demands for operator attention and action • High tempo, time-pressured tasks • Multiple distractions and interruptions • Demands on memory/Need for mental calculation • Need for sustained attention/continuous monitoring • Psychological stressors and physical stressors

Table B-7
Hierarchical list of situational factors associated with post-abandonment responses at plant locations

Detecting/ Noticing	Sense Making/ Understanding	Planning/ Deciding	Manipulating/ Acting	Communicating/ Coordinating (Teamwork Functions)	Supervising/ Directing Personnel	Directing Attention/ Managing Workload
• None	• None	• None	• Inadequate system feedback (feedback about control state is missing or too slow) • Population stereotype violations (e.g., red for normal, green for abnormal) • Confusable controls/poor control coding (multiple controllers that look alike and are next to each other). • Less than adequate work space design (e.g., size, orientation, and nominal lighting) • Hazardous, harsh or uncomfortable work environment	• Close/frequent communications and coordination between RSDP and field operators in plant areas	• None	• Multiple concurrent demands for operator attention and action • High tempo, time-pressured tasks • Multiple distractions and interruptions • Demands on memory/Need for mental calculation • Need for sustained attention/continuous monitoring

B.5.4 Possible Assessment of PSFs Associated with C&C in MCRA HFEs

Clear guidance is not yet available for analysts as to how to definitively assess (even qualitatively) those PSFs considered important in C&C. Table B-8 provides the current thinking on this assessment, but the analyst should use this information with care. In particular, note the following thoughts and cautions:

1. There is significant overlap with the assessment of PSFs in Section 8. In Section 8, the PSFs are considered in relation to the more frequently used HRA methods for cognitive and execution actions. In this context, the concern is the influence on C&C, and therefore may have a different effect.
2. The analyst should consider the PSFs for C&C as a collective indication of their influence on C&C performance. In other words, the analyst should look at the combination of ratings and come to his or her own judgement as to what the net effect will be on C&C, rather than consider them as separate PSFs each having its own influence. The overall rating of C&C can be explained by describing the likely effect of the combination of PSFs listed in Table B-8.
3. More guidance is expected in the next phase of development. This development may significantly modify or replace what is provided here.

Table B-8
Possible qualitative assessment scale for PSFs associated with C&C

PSF for C&C	Measure	Good	Moderate	Poor
Complexity	Difficulty of C&C due to variety and multiple locations of tasks to monitor; number of distractions to SS; cumulative effect of additional PSFs	Low	Medium	High
Crew dynamics	Clear delineation of chain of command and personnel roles (including STA)	Clearly identified in procedures and practiced in training	General guidance provided for all operations teams	Discretionary by SS; varies by team
Communications	Plan and equipment in place	Equipment verified through testing and crew understands what functions where; training follows communication plan and protocols	Communication observed in training exercises usually but not always follows plan; lack of clarity by crew for what system works in what locations/ conditions	Plan is unclear and equipment use is not specified or well understood

Table B-8 (continued)
Possible qualitative assessment scale for PSFs associated with C&C

PSF for C&C	Measure	Good	Moderate	Poor
Cues and indications	RSDP provides indication for key parameters and equipment status monitored in MCRA procedure	Provides all or most	Provides many but some require local monitoring	Mostly absent and requires local monitoring (and reporting to SS)
Procedures	Detail and clarity of guidance for C&C	Significant detail with step-by-step coordination points	Detailed but no clear direction for coordination of remote operators	Minimal guidance
Training	Run-throughs of procedure and C&C roles	Covers decision to abandon; follows procedure and simulates communication and coordination required	Cue for decision handed to (not made by) crew; verification by SS for remote tasks done sporadically	No coverage of decision to abandon; Run-throughs of entire procedure infrequent or appear disorganized; communication unclear
Timing	Time penalty to perform overall tasks vs. time available	None	Some	Significant
Human-machine interface	Degree and clarity of controls available at RSDP	Majority of controls available at RSDP; some local actions required. All available controls readily usable and readable	About half and half	Only local control station actions
Environment	Issues of lighting, noise, temperature and humidity, and physical access to equipment	Optimal	Moderate	Hostile
Staffing and Availability	Staffing vs. tasks cited in MCRA procedure	Optimal staffing for task performance	One or two tasks are done by the same operator in multiple locations	Inadequate staffing

B.6 References

1. Globalsecurity.org, U.S. Army Field Manual 6.0, *Mission Command: Command and Control Army Forces.* 2003. Last retrieved September 12, 2016 from: http://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm.
2. Stanton, N.A., Baber, C., and Harris, D., *Modelling Command and Control: Event Analysis of Systemic Teamwork.* 2008: Burlington, VT: Ashgate Publishing Co.
3. Smalley, J., *Cognitive factors in the analysis, design and assessment of command and control systems*. In *Modelling Command and Control: Event Analysis of Systemic Teamwork.* Stanton, N.A., Baber, C., and Harris, D., eds., 2008, Burlington, VT: Ashgate Publishing Co.
4. U.S. Nuclear Regulatory Commission, NUREG-1624, Revision 1. *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA),* Rockville, MD: May 2000.
5. U.S. Nuclear Regulatory Commission, NUREG-1880, *ATHEANA User's Guide,* Rockville, MD: May 2007.
6. Klein, D.E., Klein, H.A, et al., *Macrocognition: Linking Cognitive Psychology and Cognitive Ergonomics.* 5th International Conference on Human Interactions with Complex Systems, University of Illinois at Urbana-Champaign: 2000.
7. Klein, G., Ross, K.G., et al., *Macrocognition.* IEEE Intelligent Systems **18**(3): 81-85. 2003.
8. U.S. Nuclear Regulatory Commission, NUREG-2114, *Cognitive Basis for Human Reliability Analysis*, Rockville, MD: 2016.
9. Roth, E.M., Mosleh, A., et al., *Model-based framework for characterizing contextual factors for HRA applications.* PSAM/ESREL2012, Helsinki, Finland: 2011.
10. Klein, G., Philips, J.K., et al., *A Data-Frame Theory of Sensemaking.* In *Expertise Out of Context*. R.R. Hoffman, ed. 2007, New York: Lawrence Erlbaum Associates,
11. Vicente, K.J., Mumaw, R.J., et al., *Operator Monitoring in Complex Dynamic Work Environment: A Qualitative Cognitive Model Based on Field Observations.* Theoretical Issues in Ergonomic Science **5**(5): 359-384: 2004.
12. Mumaw, et al., *There Is More to Monitoring a Nuclear Power Plant than Meets the Eye.* Human Factors **42**(1): 36-55: 2000.
13. Salas, E.D., Sims, D.E., et al., *Is there a 'Big Five' in Teamwork?.* Small Group Research **36**: 555-599: October 1, 2005.
14. Moray, N., *Cultural and National Factors in Nuclear Safety*. In *Safety Culture in Nuclear Power Operations*. B. Wilpert, and N. Itoigawa, eds., 2001, London: Taylor and Francis.
15. Klein, G.A., *A Recognition-Primed Decision (RPD) Model of Rapid Decision Making.*, In *Decision Making in Action: Models and Methods*, G.A. Klein, et al., eds. 1993, Ablex Publishing: Westport, CT.

16. U.S. Nuclear Regulatory Commission, Region II, *Augmented Inspection Report No. 05000261/2010009, H. B. Robinson Steam Electric Plant, Unit 2*, Atlanta, GA: 2010.

17. U.S. Nuclear Regulatory Commission, NUREG-0700, Revision 2, *Human-System Interface Design Review Guidelines*, Rockville, MD: 2002.

18. U.S. Nuclear Regulatory Commission, NUREG/CR-6146, *Local Control Stations: Human Engineering Issues and Insights*, Rockville, MD: 1994.

APPENDIX C
GUIDANCE AND TIPS FOR MCRA-RELATED INFORMATION COLLECTION

This appendix provides guidance to collect information needed to evaluate the unique conditions that require MCRA, including the various plant information involved in assessing the operator response.

As valuable as it is for analysts to carefully review the MCR abandonment procedure, the way it is actually used and the nature of the tasks and their environment cannot be truly known unless discussions are held with the operators and trainers who use it. Guidance is therefore provided for conducting talk-throughs and walk-throughs for MCRA.

C.1 Plant-Specific Information Collection for MCRA HRA/PRA

This appendix builds upon the foundation in the Qualitative Analysis section of NUREG-1921 [1] to identify the MCRA information that needs to be collected. As noted in Section 2.2, MCRA is a special case of fire PRA where HFEs from the internal events PRA are not used as the basis for fire HRA modeling and where the procedure used as the basis for HFE modeling is likely not a fire response procedure (or an EOP). For this reason, it is crucial for the analysts to begin by collecting the information they need to evaluate the unique conditions that require abandonment, including the various documents that are involved in assessing operator response. This information should allow the analyst to understand the MCRA strategy, how it is trained and evaluated at the plant, the capability and HMI of the RSDP(s), and the PSFs that influence operator performance.

All of these topics, information inputs, site visits, and talk-throughs and walk-throughs are discussed below.

C.1.1 MCRA Information Inputs

The PRA, plant, and HRA information cited in Section 4.2 of NUREG-1921 [1] should be available at the start of the MCRA analysis (e.g., system descriptions), but this information should be augmented with the information listed in Table C-1.

Table C-1 lists several possible sources of information; however, not all sources are required to start the analysis. As the analysis progresses, it may be useful to follow up with some of the more specific references. For example, the very first pieces of information the HRA analyst would want to review would be:

1. MCRA procedure
2. Fire-induced risk model
3. Fire modeling
4. Fire PRA success criteria
5. Any available feasibility study

Table C-1
Input information used for MCRA

Type	Item	Use in MCRA
Fire PRA Information		
Plant Partitioning	• Fire compartments included in the MCRA analysis (NUREG/CR-6850 Task 1) • Plant layout information	• Identifies the fire compartments relevant to MCRA and the SSCs (including cables) potentially affected by fire. • Shows the proximity of the relevant fire compartments to the MCR and RSDP and provides input to travel path assessment for local actions.
Initiating Event/ Event Tree	• Plant response (both success and failure paths) • MSOs modeled in the fire-induced risk model (NUREG/CR-6850 Task 5)	• Defines the modeled PRA context consisting of the initiating event, the successful plant response path, and the failure paths; includes the modeled plant functions and systems. • Identifies operator actions credited in the MCRA model. • Identifies MSOs that can damage equipment catastrophically before it can be recovered (e.g., diesel overload, pump running with suction closed, etc.).
Thermal-Hydraulics	• Plant thermal-hydraulics data	• Provides the scenario timing for different accident sequences that may apply to MCRA, as well as information on cues such as temperatures, pressures, and levels.
Circuit Analysis and Routing Information	• Circuit failure information such as cables that, if damaged by the fire, could lead to spurious failure of equipment or indications and the probability of these spurious failures. • Routing information for cables associated with the RSDP.	• Identifies equipment susceptible to spurious failures that might cause distraction during MCRA. • Provides input to evaluation that RSDP will function as needed during MCRA.
Fire-Induced Risk Model	• MCRA modeling strategy in fire PRA (fault trees) • MSOs included in the fire-induced risk model, and any associated operator actions to mitigate them (NUREG/CR-6850 Task 5).	• Provides the modeled fire PRA context for binning decisions and for determining the nature and number of HFEs needed for MCRA. • Identifies operator actions to be credited in the MCRA model.
Fire Modeling	• Fire compartments that may require MCRA (NUREG/CR-6850 Task 11) • Smoke accumulation calculations from deterministic fire modeling analysis	• Provides equipment damage and fire location information for MCRA scenarios. • Provides insights to the fire progression portion of the MCRA timeline.

Table C-1 (continued)
Input information used for MCRA

Type	Item	Use in MCRA
	Plant Information	
Alarms	• Fire alarms • SSC alarms • Indications of smoke accumulation (most likely) and flames (unlikely)	• Identifies the fire alarms in the modeled areas of the MCR, specifically the fire alarm system panel location(s) in MCR. • Input to the plant response (mitigation) portion of the MCRA timeline. Alarms can be both inside the MCR and at the RSDP. Not all SSC alarms are initially cable traced, and as the analysis develops, additional alarms may be cable traced and credited in the HRA. • Identify additional indications of a fire that potentially requires MCR abandonment. Typically not collected initially, but may be used as secondary or tertiary cues for model refinements.
Procedures	• MCRA procedure − Obtain latest draft version of MCRA procedure and understand timeframe for changes so analysts can obtain latest information from Operations and Training. − Existing procedure- As a point of reference in order to understand the operator's inherent perspective. − Procedures calling MCRA procedure – other procedures that direct the operators into the MCRA procedure. − Site Emergency Plan • Procedures/practices for operator roles and responsibilities during power operations and following reactor trip. For example, the specification of when the STA will be available and when the TSC will be available (see also Site Emergency Plan). • Control room HVAC procedure for alignments following a fire.	• Structures the entire MCRA HRA strategy and typically also identifies the roles of the different on-shift plant staff. • Provides input to determining the cues for the MCRA diagnosis HFE. • Identifies tasks to include in the execution analysis (qualitative and quantitative). • Identifies who declares the fire as a site emergency and the roles of various individuals in responding to the fire; may indicate which staff becomes the fire brigade and specifies interfaces with site or local fire departments. • Provides information for timeline, feasibility assessment, execution task development; includes: − Site-specific fire brigade, site fire department, local fire department response practices − Electrical safety practices and protective gear for high voltage breaker operation − Communication systems, communication testing, communication practices and usage preferences, keys, tools, SCBA storage location(s), upkeep and accessibility • Identifies the smoke build-up rate in conjunction with the deterministic fire modeling analyses.

Table C-1 (continued)
Input information used for MCRA

Type	Item	Use in MCRA
Plant Information		
Training	• Training schedule • Insights or summary from previous training • Training materials related to MCR abandonment. For example, instructor lesson guide • If available, results of MCRA training exercises (especially timing)	• Used in the qualitative analysis and timeline development.
Job Performance Measures	• JPMs or other timed walk-throughs used in MCRA training	• Provides execution timing information as well as identification of special tools or PPE used as execution PSFs.
Operator Action Feasibility Assessment	• Appendix R feasibility assessments for MCRA and operator manual actions or nuclear safety capability assessment (NSCA) feasibility study. This is a deterministic analysis performed by fire protection demonstrating the feasibility of operator actions credited in the safe shutdown (licensing) analysis.	• Collect at the beginning of the analysis. • Used in the qualitative and feasibility analyses. • Typically provides the following: − Timing (but may not be as applicable as JPMs, simulator data, timed walkthroughs) − Communications − Lighting: emergency and portable lighting usage, availability, and locations − Access paths
Remote Shutdown Panel Design Information	• List of instrumentation and controls located on RSDP(s) • See also Plant Partitioning (Plant Layout) and Circuit Analysis and Routing Information	• Provides information on the RSDP capabilities for assessing operator response during MCRA scenarios (functions can be performed at RSDP vs. locally). • Identifies location of RSDP in plant so that travel time can be assessed and routing of cables for RSDP to assess functionality.

Table C-1 (continued)
Input information used for MCRA

HRA Information		
Internal Events and Fire HRA Notebooks and Quantitative Analysis Calculations	• HFEs for comparable local actions • Previous operator interviews (especially for fire but also for internal events PRA), walk-throughs, talk-throughs, and/or simulator data. • Time Critical Operator Actions (TCOA) information from Appendix R	• Provides timing information and other plant-specific insights that have already been investigated for the baseline HRA; particularly useful for actions similar to those included in MCRA as execution actions

C.2 Site Visit Preparation

As valuable as it is for analysts to carefully review the MCRA procedure and other inputs discussed above, the way operators actually use the procedure and the nature of the MCRA tasks and their environment cannot be truly known unless discussions are held with the operators and trainers who use it. Because of the uniqueness of MCRA, this section provides additional guidance for conducting talk-throughs and walk-throughs for MCRA.

It is important to prepare for the site visit to maximize the information-gathering process when there, since time with the operations and training staff will be limited. The following steps are important:

- **Identify the site visit team and ensure representation from HRA, fire PRA and fire protection.** The team should not so be so large that it makes walk-downs difficult, but having someone with knowledge of the MCRA modeling in the PRA is helpful to provide the equipment availability and scenario perspective.
- **Recommend site contacts in operations and training with familiarity with the MCRA procedure.** Examples of such contacts are Shift Supervisors/SROs who would actually make the decision to abandon. If the MCRA procedure is in the process of being updated, then the procedure writer also would be a useful contact.
- **Coordinate with the contacts provided for site operations and training regarding available days and times.** Dates for site visits should be coordinated with respect to the availability of relevant plant staff.
- **Determine the security access requirements.** The analyst needs to identify who will arrange for security access for plant walkdowns.
- **Prepare a work plan to structure the site visit.** Since time on-site is valuable (and limited), the site visit needs to be planned such that it is concentrated on the information-gathering objectives.
- **Entry into the MCR and walkdowns of the back-panel areas typically requires a pre-job brief.** This requirement is especially true if the plant is at-power and the MCR panels have open backs.

An operator interview questionnaire form has been issued by EPRI as part of version 5.1 of the HRA Calculator and is shown in Table C-2. This form can be reviewed against other formats and questions that the analysts may have used for previous operator interviews to develop a comprehensive form. The use of one interview form for the pre-abandonment phase and a separate interview form for each of the different operator roles following the decision to abandon is recommended.

Prior to the visit, the analysts should have reviewed the MCRA procedure in detail and should be familiar with other input materials, particularly potentially relevant T-H runs and fire modeling information to estimate the associated timing. Taking an initial cut at identifying the specific MCRA HFEs can be very helpful to identify questions for the talk-through and walk-through sessions. (The details of the draft HFEs can be shared with operators before the site visit.)

The length of the site visit is mainly based on the availability of operators for talk-throughs and walk-throughs and resource constraints, but the preferred schedule would include three to four days on-site to have the opportunity to ask follow-on questions, if possible.

HRA analysts and practitioners might find the following tips helpful:

- Do not use HRA or human factors jargon (e.g., do not talk about “performance shaping factors”)
- Learn to “speak operations” (e.g., focus discussions on indications, plant behavior, equipment performance, and specifics of how actions are performed)
- Avoid leading questions
- Listen more; talk less (e.g., use short, open-ended questions but ask for follow-up or clarifying information)

C.3 Talk-Throughs and Walk-Throughs

As stated in Section 4.11 of NUREG-1921 [1] on Reviews with Plant Operations, “The talk-through and walk-through processes are activities that seek to determine the likely outcome(s) of a situation based on starting conditions and the effects of decisions made—the former through structured discussions and the latter through enactments under the most realistic conditions possible.”

Given the unique nature of the conditions that prompt MCRA, performing “enactments under the most realistic conditions possible” is particularly challenging for the analyst, but can be achieved primarily by prompting operations staff to envision the conditions they would be faced with and to recall their training and simulator run-throughs of an abandonment scenario.

Section 4.11 of NUREG-1921 also provides a general background on collecting information from plant-specific interviews and it discusses important aspects of conducting talk-throughs and walk-throughs. That information will not be repeated here; the following sections will focus instead on issues specific to MCRA.

C.3.1 Talk-Throughs

Talk-throughs can provide valuable insights into the detection, diagnosis and decision-making associated with the cognitive portion of the operator actions. This is especially true during the MCRA evaluation, since the decision to abandon may not have clear cues or indications. For the execution portion of the analysis, talk-throughs can provide insights into access paths, PPE, and tools, as well as the time required to complete the actions.

The talk-throughs begin with an introduction of the team and an explanation of the reason for the visit, stressing that this is not an evaluation, but an activity that supports the PRA and provides valuable input to the realism and accuracy of the analysis. It is also important to stress that the discussion is to confirm the success path, as well as to discuss the operator response when the success path is challenged (such as when failures occur). During the talk-through, the analyst

should keep in mind that the discussion is intended to elicit information from the operator(s) and not to impose the analyst's views on how things ought to be done. Although the analyst may have to lead the discussion at times to help the operator understand exactly what is being asked, he or she should refrain from biasing the responses.

The discussion continues with general questions, such as normal crew composition, C&C structure during abandonment, on-site fire department capability, and operations crew required to support the fire brigade.

Once the general response of the crew to a fire is covered, the specific entry conditions for the MCRA procedure are discussed. One of the key pieces of information that has to be gathered is the set of decision criteria for abandonment for LOH and LOC. While conditions leading to a LOH are based on fire modeling, LOC is plant-specific and depends on the loss of critical equipment or instrumentation. Generally, these conditions occur for fires in either the MCR (primarily involving panels of the MCB itself, although there are exceptions) or the CSR and/or relay rooms, but fires in other plant-specific fire compartments may also cause such conditions.

It is important for the analysts to be familiar with the level of guidance provided by the MCRA procedure to the crew member responsible for the decision to abandon. Some procedures provide clear direction, while others leave the decision largely to the discretion of a designated decision-maker. For the purposes of the PRA, it is important to elicit from the operators as specifically as possible the systems or functions that would have to be lost in order for the decision to be made to abandon, and also the means by which the decision would be made (i.e., while the decision is likely initiated at the discretion of a single individual, the extent to which that individual would solicit other input would not be specified by the procedure, and so would need to be ascertained through the interview process).

The analysts must also assist the operators in envisioning a fire of the magnitude that would require abandonment since there is often a credibility issue as well as natural reluctance to consider leaving the MCR for the lesser capability for control and monitoring provided at the RSDP(s). It is possible that the initial response would be that they would "never" leave. This is mostly because they cannot envision the types of scenarios to which the PRA intends to apply MCRA credit. So, the full extent of what they would see and be able to do (or not see and not be able to do) from the MCR needs to be clearly described. This can be aided by "queries" of the PRA model to develop a list of all the failures that are postulated to occur for the representative LOC scenarios.

Part of the abandonment decision process is likely to involve confirmation of the fire severity in fire areas outside the MCR. It is important to elicit information from the operators regarding the travel time for the individual assigned under the fire response procedure to reach the location of the fire, assess the severity/controllability of the fire, and relay that information back to the MCR. This information will be factored into the MCRA timeline and the decision to abandon. Additionally, it is important to ask how the severity of the fire is assessed, since, in many cases, a visual inspection may be impaired due to smoke or equipment such as cabinets or raceway covers.

Following the discussion of the decision to abandon, the talk-through continues by discussing the specific operator actions included in the MCRA procedure.

It is common for MCRA procedures to contain actions that are “nice to do” versus those that are “crucial to do” from the standpoint of the PRA (i.e., required actions to reach a safe, stable plant state). It is, therefore, important for the analysts to review the MCRA procedure beforehand to identify the steps that are PRA critical and ensure that the talk-through focuses on these steps, and to be patient in explaining why these are the important items and others are not so.

Experience with such interviews has shown that operations staff often consider some non-PRA critical steps to be important. The primary reason for this is that, in the past, operators have been trained (and procedures written) using a deterministic assessment of fire impacts. For example, operators expect that, with respect to the occurrence of spurious operations, "if it can happen, it does happen – every time and for every fire scenario in the fire area." However, in the PRA, frequencies are assigned to scenarios and probabilities assigned to failures, and it is often the case that the scenarios of concern do not include some of these failures. This sometimes requires extensive discussion to break through the paradigm and bias built up over the years, so the analysts will have to provide the PRA perspective and emphasize that the time required to perform these steps may delay the critical actions or even render the overall strategy infeasible. This process will require patience between both the HRA analyst and operators. Sometimes these discussions result in revisions to the MCRA procedure to consolidate or re-order procedure steps to allow for these actions, in addition to the PRA critical actions

During the talk-through, it is important for the analysts to identify: 1) the responsibilities of each crew member who is executing the procedure, 2) the locations of the actions, 3) any keys or tools needed, and 4) the associated communication protocols. Many MCRA procedures are structured with the Shift Supervisor/SRO going to the RSDP to direct the overall strategy and handing out procedure attachments to individual operators to perform at remote locations. For the HRA, determining which operator actions require diagnosis and decision-making versus those which are simply following procedural direction is important because any diagnosis time would need to be factored into the HFE.

In addition to obtaining answers to the interview questions while at the site, it is important to identify a particular operator who can serve as a point of contact for post-visit questions and clarifications.

Table C-2 provides a structure for the MCRA talk-through, including introductions and the questions that are typically asked.

Table C-2
MCRA HRA talk-through structure

Introduction
My name is _____from _____ and these are my colleagues _____. We have been tasked with helping conduct the fire PRA for your plant. We know the plant has a good safety and reliability record, but we look at what systems and components could fail to operate to try to figure out how likely those combinations of failure are. We do a ranked list of these combinations of failures to see which of them are most likely to happen so we can identify where the challenges are and where the focus on improvements could be. One part of plant reliability is the equipment, but we also know that operators are the ones with the training, experience and procedures to bring the plant to a safe, stable condition when the equipment failures happen. We are here to learn from you – we can look at the procedures, but we don't get the real feeling for how things happen and what you actually do. So this is not a test or a performance review. We are just gathering information to help us figure out what you look at and how you assess the plant conditions and situations. We would like to ask you questions and take notes and also do a walk down in the plant. Our specific task is to look at fires in the plant and understand how you use the fire procedures, especially when a fire is so severe that it would make you leave the control room.
Specific Questions
Fire Detection Indications:
1. How do you find out about a fire and where it is located?
2. Where is the fire alarm panel located in the MCR (front or back panel)?
3. Do you have to figure out where the fire is or does the fire alarm panel tell you?
4. Do you send someone to locally verify the fire severity (or contact an out-plant operator)? How long do you think it would take to get that information?
5. What indications would you expect for CSR fire (or other fire outside the MCR that required MCRA)?
Fire Fighting:
6. How many and which MCR operators are assigned to the fire brigade? How many non-licensed operators (NLOs) are assigned to the fire brigade?
7. Do you have an on-site fire department? If not, how close is the nearest fire department?
MCR Fire Response:
8. What indications would be lost or unreliable due to MCR or CSR fire?
9. Which procedure would you be using first? Are several procedures used in parallel?
10. Is there a list in the procedure of protected instruments that are reliable in case of fire?
OPS Training on MCR Fire Response:
11. Are you trained on a plant response to a fire in the MCR or CSR?
12. How often are you trained on MCRA scenarios? Do you use the simulator?

Table C-2 (continued)
MCRA HRA talk-through structure

Decision to Abandon:
13. For an MCR fire, are there particular panels that if lost would make you more likely to leave?
14. Who makes the decision to leave the MCR?
15. The procedure doesn't specifically say if you lose X, Y, Z equipment you should go, so is there a list like that covered in training or in your experience?
16. Do you have any feeling for the time it would take to make that decision to leave the MCR, based on your training?
17. Would you wait as long as possible before going to the RSDP? Would you try to stay in the MCR in SCBAs?
Transfer of Control:
18. When you decide to leave the MCR, what happens next? Is there a disconnect switch you need to actuate? Do you need to get keys or other items before you go?
Travel to RSDP:
19. What is the travel path from the MCR to the RSDP and how long does it take to get there?
Actions at RSDP:
20. Is the RSDP used prior to abandonment? Is anyone sent to the RSDP in anticipation of abandonment and what is his/her function when they are there?
21. How much control and instrumentation do you have on your RSDP? Is that a factor in the decision to leave the MCR? (for positive or negative?)
22. Which operator goes where? Does the Shift Supervisor/Manager go directly to the RSDP?
23. Are different people stationed in different places?
24. What communications system(s) do you use?
25. Are all of the operating procedures called out in the MCRA procedure stored at the RSDP?
26. Is EOP usage allowed at the RSDP? If so, do the operators have access to these procedures while at the RSDP?
27. Is there a podium or flat surface available at the RSDP for the SS and RO to place procedures to which they are referring, including the fold-out page of continuous action statements, if applicable?
28. Is significant background noise expected in the RSDP area? At local control stations?
29. Is there portable lighting that you get and use (flashlights? headlamps?) or do you count on local emergency lighting?
30. If you need tools or gear, where are they located? Do you need keys to access them and if so, where are the keys and do you need time to get them? Are the tools/gear checked and replaced regularly?
31. Would fire impact the security system and would access to areas be a problem?
32. Does the Shift Supervisor/Manager go to the RSDP and coordinate the overall strategy? Or does each operator act independently? What is the communication process like?
33. What are the primary parameters or functions you are going to be focused on controlling?
34. Is the workload greater than for other transients you train for or have experienced?
35. Do you recall how long it takes when you run through the abandonment procedure during training?
Onsite Fire Experience
36. Have you experienced an actual fire? How serious was it and what happened?

It is a great benefit to the analysis if separate talk-through sessions can be conducted with several different operators to see if there are differences in perspective. Any inconsistencies can be noted as topics to cover in the walk-through and to consider as sources of uncertainty in the analysis.

Aside from the questions that relate to obtaining a general understanding of the strategy and procedure steps, the talk-through should also collect more specific information for application to the qualitative and quantitative analysis of the MCRA HFEs. Prior experience with performing an MCRA HRA or a review of the examples in this guidelines document can be used to scope out preliminary HFEs for major tasks, functions, or operator actions. A template of topics that should be addressed for the HRA, such as the interview form from the EPRI HRA Calculator v.5.1 release notes [2] shown in Table C-3, can be used to ensure that the following items are covered during the talk-through:

- Expected cue to alert operators to the need to take the specific action
- Time to reach the specified cue from beginning of event (i.e., plant trip) where the cue is based on a specific procedure step
- Time to evaluate conditions and make decision to take the specific action
- Time to complete the action once a decision is made
- Location and complexity of action steps
- Human-machine interfaces

De-briefs are recommended after each talk-through among the analysts on the team to identify points that were particularly obvious, confusing, or differed between operators. These points can then be emphasized during subsequent talk-throughs as well as the walk-through.

Table C-3
HRA interview form (from EPRI HRA calculator v. 5.1 release notes)

PRA/HRA Analysts		
Worker(s) Interviewed		
Date of Interview		
Location of Interview		
Basic Event ID	**HFE Description (indicate if all of the HFE or a portion of the HFE)**	
Initial Conditions, Initiating Event, Accident Sequence, Success Criteria [from Scenario Description field]		
Cue including Instrumentation, System signal or reading	[from Initial Cue field]	Additional Notes on Cue
Procedures including Informal Instructions, Training, or Guidance	Cognitive Procedure	Cognitive Procedure Description and Revision #
		Cognitive Step # and Instructions
	Execution Procedure	Executive Procedure Description and Revision #
		Execution Instructions

Table C-3 (continued)
HRA interview form (from EPRI HRA calculator v. 5.1 release notes)

Timing	**T_{sw}**	**Required time window for performing the action**
	T_{delay}	Time from start of event to presentation of cue to worker that action is required
	T_{cog}	Diagnosis and decision-making time
	T_{exe}	Execution (manipulation) time
	Timing Notes	[from Time Window Notes field]
Manpower	[Required crew members in the HRA Calculator field]	
Stress	Stress Level	Stress decision tree outcome based on PSFs
	Workload	Yes/No based on stress decision tree
	Performance Shaping Factor (PSF)	Could be Nominal or Negative based on stress decision tree
	Notes on Stress	
Location	Cognitive Location	
	Execution Location	
Execution PSFs	Environment	
	Heat/Humidity	
	Atmosphere	
	Special Requirements such as Tools and/or PPE	
	Factors contributing to Complexity of Response	
HRA/PRA Assumptions		
1. Given the scenario description, starting with the initiating event, what is the progression required by the crew to reach the guidance for this action?		
2. Given the discussion in 1, are there other progressions possible?		
3. What signals/cues/triggers lead to the decision to perform this action?		
4. How long would it take to reach the guidance for this action?		
5. Who is required to perform this action?		

Table C-3 (continued)
HRA interview form (from EPRI HRA calculator v. 5.1 release notes)

6. Where does the execution take place?
7. Is there any special equipment required for the execution? For example, tools, flashlights, protective gear.
8. Is the location readily accessible?
9. Is the operator's environment impacted in anyway? For example, is there reduced lighting, high temperature, or smoke?
10. How long would it take to perform this action, including travel time from original to another location (T_{exe})?
11. What type of training is performed for this activity (classroom or simulator or mock-up)? How often is training performed on this activity?
12. What other activities would be required at the same time?
13. Notes
Additional MCR Abandonment-specific Notes:
14. Relationship between this action and the overall MCR Abandonment response.
15. Communications. What communications are conducted during the conduct of this action?
16. Coordination. What other actions rely on this action? What other actions are needed before this action can succeed?
17. Instrumentation.
18. Actions Needed in the first 30 minutes.
19. Actions Needed after the first 30 minutes (through the mission time)

C.3.2 Walk-Throughs

During the talk-through, the emphasis is on obtaining an overview of how the procedures are used, some of the key decision points and time constraints of the strategy and, in general, gaining a sense of the operations and training perspective on the scenario, how it evolves and how it has been trained.

The walk-through provides the analysts the opportunity to view the locations of actions; conditions, communications, instrumentation, alarms/annunciators, and controls at the RSDP; and other equipment cited in the MCRA procedure steps. This walk-through allows the analysts to identify potential challenges to successful plant response. These challenges include, but are not limited to, the following:

- Difficult actions due to equipment location (time required to get there) and local environment (e.g., heat, noise)
- Limited access to components to be operated (e.g., cramped workspace or up a ladder)
- Physical workload (e.g., several hundred turns of a small operator to operate a large valve)
- Travel times from one point to another
- Performance times for key tasks including time to obtain tools, lighting and/or PPE
- Communications circuits that will be used
- Seeing what needs to be done in a timely manner in the MCR prior to abandonment and during the transfer of control to the RSDP (These insights potentially feed into plant or procedure modifications that could simplify actions, save time, and impact operator reliability.)

In other words, the MCRA strategy that may still be somewhat abstract during the talk-through(s) becomes more "real" to the analysts during the walk-through.

Based on the talk-through, the analysis team should have identified the locations associated with the PRA-relevant procedure steps in the MCRA strategy that they would like to observe during the walk-through. These will have to be identified prior to the walk-through to ensure that the appropriate access is obtained. The walkthrough needs to be organized, even if informally, so that the analysis team can see what they need to see during the time allotted. Ideally, more than one local operator would be available for the walk-through in order to evaluate coordination of actions between separate operators at different locations to observe the time required and how the communications and coordination are conducted. Visiting the RSDP and the locations of other local actions is crucial since the analysts must understand the plant-specific RSDP displays, capabilities and limitations.

The number of locations visited during the walk-through is highly plant-specific and depends on the plant’s remote shutdown strategy and a review of the MCRA procedure. There may be several locations necessary for operators to start up the RSDP, start up support systems, and establish control of the plant. For each location, the HRA analyst should note the travel time, communication capabilities, and coordination required with other operators at other locations. In addition to timing information, the analyst should also be noting insights on other PSFs.

During the walk-through, the analyst should clarify and record the travel time and performance time for each key procedure step identified during the talk-through. The performance time includes the time required for communication with other remote operators and communication to confirm actions completed. The timing should be recorded for use in the qualitative and quantitative analyses (including the feasibility assessment). Since the walk-through will focus on the execution portion of the actions, any particularly challenging or difficult actions, should be noted. For example, is access to the equipment time-consuming? Or, does a valve take many turns of a handwheel to close? Actions that require some decision-making and not just following procedure steps (e.g., the procedure lists several types of injection sources and the SS must determine which one will be attempted first), should be noted as well since the cognitive portion of that HFE will have to be addressed. Key factors addressed in the THERP Chapter 20 [3] tables should also be considered during the walk-through. These factors include the nature of the HMI (e.g., presence of mimics, type of displays used, type of manual control), whether the equipment is one among many in a similar grouping, and whether there is clear and unambiguous labeling of equipment.

The walk-through also provides an excellent opportunity to gather information to assess feasibility criteria such as communications, lighting, and accessibility of tools/keys/PPE. (See NUREG-1921 Section 4.3 [1] and Section 6 on Feasibility for further details.)

There should be someone taking notes throughout the walk-through, particularly on timing aspects, to ensure that these key details are preserved. It is rare to get a chance at a second walk-through.

Once the walk-through is completed, any remaining time at the site should be used to review the information already gathered, discuss it among the analysis team to gain consensus on key actions and timing, identify any scenario variations from the PRA model that should be addressed, and start applying the information to the HRA to see if there are any outstanding or follow-up questions that can be addressed by the operators or trainers while at the site.

C.4 Managing Resources

Most analyses have limited resources for MCRA, so resource management is important. The MCRA analysis can become a time-consuming (and resource draining) activity due to the level of detail and intricacy of the process. This section addresses the resource management process and provides tips on utilizing other information from the fire PRA/HRA.

C.4.1 MCRA PRA Scenario Binning

Discussions with the fire PRA team are essential to understanding the minimum set of unique scenarios that must be evaluated by the HRA. It is often useful to group similar MCRA scenarios into bins. A bin is a group of MCRA scenarios that can be assessed as a single analysis. Example of MCRA bins include:

- MCRA scenarios related to LOC
- MCRA scenarios related to LOH
- MCRA scenarios with loss of offsite recovery

- MCRA scenarios with no offsite power recovery
- MCRA scenarios related to loss of feedwater
- MCRA scenarios with feedwater available

It is often useful to create bins within these bins to account for differences in the details of what is available in terms of instrumentation and equipment. For example, LOH abandonment scenarios involving fire in a non-safety panel can range from very little (if any) equipment damage to impacts on several key safety functions. The complexity of the execution actions (and the need for them) varies greatly. For LOC, different scenarios could make the diagnosis of LOC more or less difficult.

Binning the scenarios is a mutual decision by the PRA and HRA analysts that allows the HRA to focus on a manageable set of actions while still maintaining some distinctions where local actions dominate.

C.4.2 Use of Previous MCRA HRAs

One way to conserve resources in HRA is to review previous analyses to see what aspects can be carried over to a new study or as a reminder of the issues that dominate a particular type of operator action. Although MCRA is highly unique and plant-specific, there may be aspects of a prior analysis that can be re-used. It would be good practice to review the following:

- Appendix R analysis for MCRA
- Previously performed PRA analysis for MCRA scenarios
- Sister plant MCRA analysis or for multiple unit sites, the other unit's MCRA analysis (taking care to consider unit and plant-specific differences).

Examples of actions modeled in previous/comparable MCRAs are provided in Section 5 on identification and definition.

The analyst should also check similar or comparable operator actions already modeled in the internal events and fire PRAs to see what information is applicable to MCRA, such as the thermal-hydraulics for the fire scenario that is most constraining for MCRA to provide the overall timeframe within which the actions need to be taken. In addition, JPMs and operator interviews for actions that would be performed in a MCRA scenario can provide insights to manipulation and travel timing.

Care should be taken, however, not to carry over an approach for convenience without considering the plant-specific nature of the actions and interfaces and how they should be grouped and developed as HFEs.

C.5 References

1. *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines.* EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, D.C.: 2012. EPRI 1023001 and NUREG-1921.
2. *EPRI HRA Calculator Version 5.1.* EPRI, Palo Alto, CA. EPRI 3002003149: June 2014.
3. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* U.S. Nuclear Regulatory Commission, Washington, D.C. NUREG/CR-1278: August 1983.

APPENDIX D
INSIGHTS FROM OPERATOR INTERVIEWS

D.1 Introduction

The context and environment encountered by operators during MCRA scenarios is unique compared to control room operations, even under abnormal or emergency conditions.

Several of the authors already had direct experience with interviewing plant personnel for the purposes of supporting fire PRAs. They had conducted table-top interviews with operators to review the MCRA procedure steps and ask questions about their understanding of the process and training experience. Some authors had also conducted walkthroughs of MCRA scenarios to see the equipment manipulated, the operating environment in the context of the timelines, and the actions required. In some cases, they were also able to witness MCRA simulator training exercises. These interviews provided insights into the plant-specific differences in the types of MCRA and fire procedures at various sites, the interpretation of the procedural guidance by the operators and trainers, the interactions between the operations crew, and the equipment (including the RSDP if available). These insights, in turn, provided valuable input to the main sections of this report.

To supplement this experience and provide other authors the opportunity to better appreciate these MCRA differences and the impact they have on operations and plant control, the team conducted a series of interviews with NRC staff who were formerly licensed operators, operator trainers, or STAs.

Two preliminary, shorter interviews were performed, serving two different purposes. The first interview was aimed at understanding previous research and to understand how operators were modeled in that work. A second interview was performed to assist in the development of interview questions for later interviews.

Recognizing that there may be differences between NPP types and vendors, three additional interviews, each roughly three to four hours long, were performed for groups of former operators, trainers, and STAs for:

1. General Electric BWRs
2. Westinghouse PWRs
3. Combustion Engineering PWRs

This appendix provides a high-level summary of the interviews. In particular, the interview participants are identified and general insights from the interviews are summarized. Finally, a list of questions and topic areas used for the interviews is provided.

D.2 Insights from Interviews

The interviews were intended originally to provide information on two aspects of MCRA: 1) general background on how operations change when moving from the MCR to the RSDP, and 2) information on how control of plant parameters may be the same or different for MCRA scenarios compared to non-abandonment scenarios. However, because the interviews were not restricted to the pre-planned questions and topics, the project team was able to gather additional, unexpected information. The discussion below summarizes the insights that were gained. In addition, these interviews, coupled with the authors' experiences, led to a focus on "command and control" discussed in Appendix B.

Several themes arose during the interviews helping the authors to better understand the context surrounding MCRA as well as to better define the situations and PSFs that may have the biggest impact. Feedback was received on various issues such as how a two-unit shutdown is handled, what parameters might be difficult to control locally, how training is conducted, determination of timing used during training, and variability of RSDP capabilities at the various plants.

To begin with, the operators were asked to identify the key features for nominal MCR operations and EOP-directed operator actions. These key features include:

1. High familiarity (i.e., frequent training and practice) with:
    a. Steps, format, content, and intent of the EOP procedure set (including many memorized steps)
    b. Operator actions that are taken in MCR, especially those contained in EOP procedure set
    c. MCR panels, their layout, etc.
2. Several avenues for "backing up" operator actions, including:
    a. Support from other operators in the MCR, STA, etc.
    b. Feedback and additional or continuing cues from MCR alarms, computer systems, readouts, etc.
    c. Instructions in EOP procedure set often will provide opportunities for feedback, etc.
3. Workload (in terms of crew structure, communications, etc.) is controlled, by design, to support operator actions taken in the MCR
4. Co-located operators facilitate communication, coordination, shifts in workload, etc.
5. Communications in MCR are easier to understand, whereas communications between operators at multiple locations takes more time and can be misunderstood due to problems with communications equipment

The unique circumstances encountered in MCRA and the divergence from the elements listed above lead to the increased complexity and stress with MCRA. The interviews helped the team to better understand these divergences and understand the operations during MCRA. Numerous changes can be noted for the movement of command and control from the MCR to an RSDP. Consideration of training, realistic timing, staffing available, condition and availability of the

RSDP are important in understanding the response following abandonment. Furthermore, the decision to abandon, in and of itself, needs consideration to understand what prompts the operators to abandon (whether for LOH or LOC) and what factors may influence (either positively or negatively) that decision.

Some high-level conclusions that the team was able to draw from the interviews include:

- **Each plant has a unique alternate shutdown strategy.** These variations make it difficult to draw general conclusions for performing HRA for these scenarios.
- **There is great variability between plants in how MCRA would proceed**. This variability manifests itself in the placement, design, and configuration of the RSDP, the training received, and the approach to the decision to abandon.
- **There is a greater sense of uncertainty when moving to MCRA scenarios**. This uncertainty may stem from a greater unfamiliarity with the procedures used during this time, but it is also influenced by the training received and the condition and availability of the RSDP.
- **Within the MCR, the operators have backup for actions taken (or not taken).** In addition, the systems and indications associated with those actions are available and visible to the entire crew. These operational features may not exist at the RSDP. Consequently, not only for local actions, but for actions at the RSDP, there is less (or no) backup available.
- **Communications are different and more difficult in MCRA scenarios.** Most notably, communication can be more time-consuming due to the distribution of crew members and operators across the plant.
- **The workload shifts with MCRA.** Operators, both the in-control room crew and field operators, may not function the same way once abandoning the MCR. In other words, indications and controls required for operator actions are no longer co-located like they are in the MCR. In the MCR, indications and controls for equipment are located close to each other such that, for example, a single operator can observe the indications and annunciators that indicate the need for an action AND perform the associated action. However, for MCRA, operator actions are likely to be distributed among multiple operators and multiple locations.
- **A two-unit shutdown is not automatically more difficult.** However, it may require more operators to implement.
- **Realistic training from the RSDP can be important to improving command and control (e.g., communications, coordination of operator actions) and the performance of operator actions.** Realistic training is especially important when the MCRA strategy must be implemented within a certain timeframe.

D.3 Participants

As noted above, there were two preliminary interviews, and three plant-type and vendor-specific interviews. The NRC staff who participated in the two preliminary interviews, with their respective inputs, were:

- Kevin Coyne - Information on modeling operators in the ADS-IDAC [1] dynamic PRA simulation model, especially regarding the control of plant parameters and use of Gary Klein's cognitive behavior models.
- Jim Kellum - General feedback and insights, as operator and operator trainer, regarding questions to ask in the interviews.

NRC staff who participated in the three plant-type and vendor-specific interviews were:

1. BWR operator/operations experience:
    a. Harry Barrett
    b. Michelle Kichline
    c. Bernie Litkett
2. Westinghouse PWR operator/operations experience:
    a. Sean Curie (formerly with the NRC)
    b. Mark King
    c. Bernie Litkett
    d. Ross Telson
3. Combustion Engineering PWR operator/operations experience:
    a. Jack McHale (retired)
    b. John Thorp

D.4 Outline of Interviews

The interviews were structured around the following questions and topic areas, although additional topics and questions emerged during the interviews:

1. Discussion of plant parameters that are required to be “controlled” or “maintained”
    a. Difference in meaning for “control” versus “maintain”
    b. What plant parameters require control/maintain?
        i. SG level
        ii. SG pressure
        iii. ADV control
        iv. RCS temperature
        v. RCS pressure
        vi. PZR level
        vii. Other?
    c. Specific training (classroom and simulator – distinguish which) for control of plant parameters:
        i. MCR without fire (i.e., expected accident response)
        ii. MCR with a fire
        iii. RSDP
        iv. Local panels:
            1. Command-and-control in MCR, no fire (e.g., SBO)
            2. Command-and-control in MCR, with a fire (also how different from Case 1?)
            3. Command-and-control at RSDP, with a fire (also how different from other two cases?)
    d. What is the definition of "success" for control of plant parameters - from training, PRA, etc. (e.g., maintain within certain bands)?
    e. By whom or how are "bands" defined (e.g., procedure, training, SRO)?
2. Talk-through of MCR operator response: General transient (using example plant procedures)
    a. Who's doing what?
        i. ROs
        ii. SRO
        iii. STA
        iv. Other?
    b. What communication occurs related to control of plant parameters?
        i. Are there specific expectations when "control" or "maintain" is communicated?

   c. Are there challenges related to man-machine interface, other hardware/software, or T-H response time?
      i. What, when, etc.
   d. What is used (e.g., written notes) to remind operators to continue monitoring parameters?
   e. What context or factors might cause operators to "fail"? With what consequences?
   f. Simulator training and/or event experiences (throughout discussion and as needed)
3. Talk-through of MCR and local operator response: SBO (or other scenario TBD)
   a. Same questions as above for general transient case
4. General discussion of MCRA scenarios and control of plant parameters
   a. Same questions for:
      i. If control is accomplished at the RSDP
      ii. If control is on a local panel
   b. Bring in discussion of H.B. Robinson event, as needed

D.5 References

1. Coyne, K. and Mosleh, A., “Nuclear Plant Control Room Operator Modeling Within the ADS-IDAC, Version 2, Dynamic PRA Environment: Part 2 - Modeling Capabilities and Application Examples,” International Journal of Performability Engineering, Totem Publisher, Inc., Plano, TX, Nov. 2014, Vol. 10, Issue 7, pgs. 705-716.

NRC FORM 335 (12-2010) NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG-1921
Supplement 1
Final

2. TITLE AND SUBTITLE
EPRI/NRC-RES Fire Human Reliability Analysis Guidelines - Qualitative Analysis for Main Control Room Abandonment Scenarios Supplement 1

3. DATE REPORT PUBLISHED

MONTH	YEAR
January	2020

4. FIN OR GRANT NUMBER
NRC-HQ-60-14-D-0022

5. AUTHOR(S)
Paul Amico (Jensen Hughes), Erin Collins (Jensen Hughes), Susan Cooper (U.S. NRC), Kaydee Kohlhepp Gunter (Jensen Hughes), Stacey Hendrickson (SNL), Jeffrey Julius (Jensen Hughes), Ashley Lindeman (EPRI), Nicholas Melly (U.S. NRC), Mary Presley (EPRI), Tammie Rivera (U.S. NRC), John Wreathall (John Wreathall & Co., Inc)

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)
9/12/2014 - 08/31/2017

8. PERFORMING ORGANIZATION
U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC 20555-0001
Electric Power Research Institute, 3420 Hillview Avenue, Palo Alto, CA 94303
Sandia National Laboratories, PO Box 5800 Albuquerque, NM 87185
John Wreathall & Co. Inc, 4157 MacDuff Way, Dublin, OH 43106

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Electric Power Research Institute
3420 Hillview Ave
Palo Alto, CA 94303

10. SUPPLEMENTARY NOTES
Tammie Rivera, NRC Contracting Officer Representative

11. ABSTRACT (200 words or less)
Main control room abandonment is analyzed as a special case of fire human reliability analysis. While NUREG-1921/EPRI 1023001– EPRI/NRC-RES Fire Human Reliability Analysis Guidelines briefly addressed abandonment, additional guidance and inputs are needed to properly address the unique contexts of abandonment scenarios. Therefore, this effort builds upon previous fire PRA research efforts that developed explicit guidance for estimating human error probabilities for human failures events under fire-related conditions. In particular, this guidance builds upon, rather than replaces, NUREG-1921, which provides, among other items, a process for conducting fire human reliability analysis through several steps including: identification and definition, qualitative analysis, quantification, recovery analysis, dependency analysis, and treatment of uncertainty.

The success of performing shutdown from outside of the MCR is dependent on a number of factors including the plant strategy and procedure, capabilities of the remote shutdown panel, and the number of local operator actions. This report provides additional guidance beyond NUREG-1921 in several areas, including: modeling considerations, feasibility assessment, identification and definition, timing, performance shaping factors (including a preliminary assessment of command and control), and walk-through and talk-through guidance. Overall, this report provides guidance to develop a qualitative foundation for MCRA scenarios that will ultimately support quantification of human failure events related to abandonment.

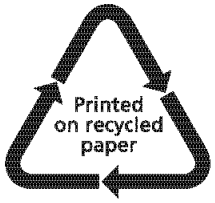
12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Human Reliability Analysis
(HRA) Fire
Fire Protection
Probabilistic Risk Assessment
(PRA) Command and Control
Main Control Room Abandonment (MCRA)

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

NUREG-1921
Supplement 1, Final

EPRI/NRC-RES Fire Human Reliability Analysis Guidelines—Qualitative Analysis for Main Control Room Abandonment Scenarios

January 2020