U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

April 2015
Revision 1

Technical Lead
Wesley Held

REGULATORY GUIDE

REGULATORY GUIDE 5.74

(Revision 1 of Regulatory Guide 5.74, dated June 2009)

MANAGING THE SAFETY/SECURITY INTERFACE

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for nuclear power plant licensees (hereinafter "licensees") to assess and manage changes to safety and security activities so as to prevent or mitigate potential adverse effects that could negatively impact either plant safety or security at power reactors. New applicants may wish to consider this guidance in preparing an application for a license under 10 CFR Parts 50 or 52.

Applicable Rules and Regulations

- Title 10, Part 73, of the Code of Federal Regulations (10 CFR Part 73), "Physical Protection of Plants and Materials" (Ref. 1), prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and at plants in which special nuclear material is used. Specifically, Section 73.58, "Safety/Security Interface Requirements for Nuclear Power Reactors," requires that licensees shall assess and manage the potential for adverse effects on safety and security before implementing changes to plant configurations, facility conditions, or security.

- 10 CFR 73.55(m) prescribes requirements for the review of each element of a licensee's physical protection program at least every 24 months. Specifically, the review must include an audit of the effectiveness of the safety/security interface activities.

Related Guidance

- RG 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, tests, and experiments," (Ref. 2) describes processes for evaluating changes, tests, and experiments at facilities licensed under 10 CFR Part 50, including nuclear power plants.

- RG 1.219, "Guidance on Making Changes to Emergency Plans for Nuclear Power Reactors," (Ref. 3) provides guidance on implementing the requirements of 10 CFR 50.54(q), Emergency plans, at facilities licensed under 10 CFR Part 50, including nuclear power plants.

Written suggestions regarding this guide or development of new guides may be submitted through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html.

Electronic copies of this regulatory guide, previous versions of this guide, and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/. The regulatory guide is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under ADAMS Accession No. ML14323A549.

Purpose of Regulatory Guides

The NRC issues RGs to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-002. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

Reason for Revision

This revision (Revision 1) of RG 5.74 incorporates editorial changes and the current format for RGs and is administrative in nature. These changes are intended to improve clarity and do not alter the staff regulatory guidance. These changes include additional questions to assist the user in the screening of planned and emergent activities or changes, and clarification to the requirement that the safety-security interface must be maintained at all times.

Background

The purpose of establishing and maintaining an effective interface between safety and security at a facility is to ensure that potential adverse effects from implementation of changes to safety and security measures are considered and addressed prior to implementation.

Site security programs include physical security and cyber security. Therefore, when the general term "security" is used in this RG, it is meant to encompass physical and cyber security. The proliferation of digital technology must be considered and addressed when changes are made to safety systems – safety system components which previously contained no digital equipment are becoming increasingly digital. Also, as cyber security measures are put in place, impacts to safety analyses must be considered and addressed.

The interface between safety and security is an important element of both programs relative to ensuring public health and safety. The licensee should address plant activities that could compete or conflict with the capability of the site security program to provide high assurance of adequate protection of the common defense and security. Conversely, changes in the site security program could also adversely affect plant operations; safety-related structures, systems, and components; operator actions; or emergency responses necessary to prevent or mitigate postulated design-basis accidents and to protect public health and safety and the environment.

Licensees of operating nuclear power reactors use management controls for reviewing, assessing, and managing plant activities or changes to provide continued assurance of adequate safety and security. However, 10 CFR 73.58 adds a requirement for such licensees to assess and manage changes to these activities effectively. Licensees may expand or take credit for other plant processes to ensure an adequate interface between safety and security.

Each licensee is responsible for balancing the needs of both safety and security to ensure that all program goals, requirements, and procedures are met. The information provided in this RG is intended to clarify the NRC staff's position associated with the effective interface between safety and security to ensure that a licensee implements changes to its safety or security programs without adversely affecting other site programs (e.g., operations, security maintenance, emergency response).

Harmonization with International Standards

The International Atomic Energy Agency (IAEA) has established a series of safety guides and standards constituting a high level of safety for protecting people and the environment. IAEA safety guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of safety. Pertinent to this RG, IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," (Ref. 4) issued January 2011 contains recommended operational guidance for nuclear security personnel. This RG incorporates similar recommendations for analyzing potential conflicts between safety and security considerations at nuclear power plants.

C. STAFF REGULATORY GUIDANCE

1. Requirements

a. In accordance with 10 CFR 73.58(b) and (c), licensees must review planned and emergent changes and activities to identify any potential adverse impact of these changes or activities on safety and security before implementation. Each licensee is responsible for establishing, implementing, and maintaining site procedures that not only ensure that personnel knowledgeable in each program area participate in the site work control process, but also provide a means of communicating proposed changes to the appropriate personnel within each program area for review. Management controls or processes used to assess proposed facility changes may be qualitative, quantitative, or a combination of both based on the complexity of the proposed changes or planned activities.

b. Licensees shall assess and manage their safety and security program activities in a manner that ensures that there are no adverse impacts on safety and security activities as required by 10 CFR 73.58.

c. Licensees should consider reviewing and updating existing procedures to reference the requirements of the interface between safety and security as outlined in 10 CFR 73.58. These procedures should clearly define processes to ensure that effective communications between the operations (safety) and security staffs are maintained at the facility.

d. In accordance with 10 CFR 73.55(m), each licensee is responsible for ensuring that the reviews and audits of its site security programs include activities involving the safety/security interface.

2. Scope

a. The licensee's established controls and processes for managing the interface between safety and security should ensure that security personnel are notified of planned or unplanned changes to the characteristics of the site's physical layout (including topographical changes); the configuration of facilities; structures, systems, and components; and the site's operations procedures. Controls and processes should also ensure that the security organization has the opportunity to review proposed changes and activities to identify potential adverse impacts on the functions and performance of the elements of the site security programs established within the owner-controlled area, protected area, and vital areas. When physical and/or administrative changes are driven by operation or emergency planning, the licensee should assess the potential impacts of these changes on the functions and performance of the elements of its site security programs to prevent the inadvertent degradation of site protective strategy.

b. Personnel knowledgeable of the site security programs should review proposed changes to the program areas for potential adverse effects on security. The following list includes a set of program areas for this review; additional areas may necessitate review as appropriate:

(1) operations,
(2) maintenance,
(3) work management (control and planning),
(4) nuclear training,
(5) nuclear engineering and support,
(6) radiation protection,
(7) emergency preparedness or planning,
(8) fire protection,
(9) chemistry (chemical safety),
(10) environmental protection,
(11) industrial health and safety,
(12) security, and
(13) target sets.

c. Personnel knowledgeable of the site security programs should review planned or emergent activities for potential adverse effects on security. The following list includes a set of activities for this review; additional areas may necessitate review as appropriate:

(1) activities that could cause a loss of primary power to security systems;
(2) the installation or removal of a barrier that could adversely impact safety, security, or emergency response;
(3) the placement of trailers or heavy equipment that could obstruct detection or assessment functions or increase the response times of security personnel;
(4) the installation of chemical or hazardous material storage tanks adjacent to a protected fighting position;
(5) fire protection manual operator actions that do not account for paths of travel through the security fields of fire, which could delay or prevent operator response and invalidate safety assumptions and credit for operator actions;
(6) construction activities that remove or degrade physical barriers, thus allowing established access controls to be bypassed;
(7) the installation of barriers that increase the security response timelines that interfere with protected fighting positions and fields of fire, and that interfere with or prevent detection and assessment functions;

(8) changes to target set equipment that could impact its availability or operability;
(9) activities that require the removal of personnel from designated areas due to the dangerous nature of the activity (e.g. overhead lifting, extreme heat, etc.); and
(10) changes to the location in which radiological sources requiring protection against theft or diversion are stored.

d. To facilitate the safety/security assessment process, the licensee may choose to evaluate changes using predetermined questions that are specifically designed to identify potential conflicts in an efficient, yet adequately detailed, manner. Current "change management" processes that licensees may consider for use in developing screening questions include, but are not limited to:

(1) 10 CFR 50.54(a) process for screening changes to quality assurance plans;
(2) 10 CFR 50.54(p) process for screening changes to the security (physical security, training qualification, contingency) plan;
(3) 10 CFR 50.54(q) and 10 CFR 50.47(b) processes for screening changes to the Emergency Plan; and
(4) 10 CFR 50.59, "Changes, tests, and experiments," and RG 1.187 "Guidance for Implementation of 10 CFR 50.59, Changes, tests, and experiments," processes for evaluating changes, tests, and experiments.

e. Appendix A of this RG contains examples of questions that may aid the user with the screening of planned and emergent activities or changes. Upon screening of these activities, if it is determined that compensatory or mitigative actions or both may be necessary to maintain safety or security, the licensee should communicate the action to the appropriate personnel.

3. Management Controls and Processes

a. For those plant changes that could affect security, the licensee should establish controls or processes to assess and manage operational changes to include emergency planning for both planned and emergent activities that could impact:

(1) the effectiveness, reliability, and availability of the systems of the site security programs;
(2) the effective implementation of the site protective strategy; and
(3) the effectiveness of the site security plans, implementing procedures, or license conditions.

The objective is to verify that a proposed change or activity will not inhibit compliance with security requirements or reduce the effectiveness, reliability, or availability of the licensee's site physical protection program credited for protection against the design basis threat.

b. Using existing controls to implement the interface between safety and security will help to ensure that assessment and management of facility changes and activities includes the physical protection program.

One acceptable method to meet the requirements of 10 CFR 73.58 is for licensees to evaluate existing and proposed programmatic controls and the Cyber Security Plan including computer software Secure Analysis of digital safety systems developed under a Secure Development and Operational Environment (SDOE). Additional examples of existing programmatic controls include, but are not limited to, plant operations review committees; plant review boards; safety review committees; independent safety reviews; work planning and controls; configuration

management; review and audit programs; corrective actions and reporting programs; engineering, design, project management; and maintenance.

c. The licensee should develop or consolidate crosscutting controls, processes, and procedures to assess and manage the potential for adverse safety and security interactions that may result from changes to the configuration of the site, changes in equipment status, and changes to site procedures. These management controls or processes typically ensure that licensee personnel identify, describe, review, approve, monitor, implement, and document emergent and planned operations or activities.

d. For those security changes that could affect safety, the licensee should establish controls or processes to assess and manage security-related changes to both planned and emergent activities that could impact safe plant operations, including emergency planning.

e. The licensee should use the existing management controls and processes to evaluate proposed changes for adverse effects on safety and security, including the site emergency plan **before** [emphasis added] implementing changes to plant configurations, facility conditions, or security (e.g., work control, modifications, or 10 CFR 50.59 evaluations).

f. 10 CFR 73.58(b) requires that, "The licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan before implementing changes to plant configurations, facility conditions, or security." However, the guidance for implementing 10 CFR 50.59 in RG 1.187 provides an exception for maintenance activities and certain temporary modifications that are expected to be in place for less than 90 days. The licensee is required to ensure that any adverse effects on security from these maintenance activities and temporary modifications are addressed either through the 10 CFR 50.59 process or other processes (e.g., work control) **before** [emphasis added] an activity is initiated. With regard to emergency plans, the applicable change process is 10 CFR 50.54(q). 10 CFR 50.54(q)(2) requires that the license follow and maintain the effectiveness of the emergency plan at all times.

g. The licensee should conduct reviews and audits to confirm that procedures established to control any changes to the plant configuration, including emergencies, comply with the licensee's security program. The review should encompass plant operations; plant modifications; and plant safety programs, work control processes, and procedures. The licensee may audit engineering and design, safety analysis, work controls, construction, maintenance, and other activities. The procedures governing these and other activities should include security reviews:

(1) to identify safety activities or conditions that could affect security;
(2) to identify security activities or conditions that could affect safety; and
(3) to provide a means for resolving conflicting or competing safety and security interests.

To prevent recurrence, corrections to specific or programmatic issues should be managed through the site's corrective action program for tracking, trending, communications, and completion.

4. Training

The licensee should provide training that addresses changes in the updated procedures and corresponding guidance documents to managers involved in the process of facilitating the interface between safety and security.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[1] may use this guide and information regarding the NRC's plans for using this RG. In addition, it describes how the NRC staff complies with 10 CFR 50.109, "Backfitting" and any applicable finality provisions in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Applicants and Licensees

Licensees may voluntarily[2] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this RG may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this RG for actions that do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59, "Changes, Tests, and Experiments." Licensees may use the information in this RG or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this RG. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this RG, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this RG to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this RG. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the RG, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this RG, generic communication or promulgation of a rule requiring the use of this RG without further backfit consideration.

During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this RG, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this RG are part of the licensing basis of the facility. However, unless

---

[1] In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

[2] In this section, "voluntary" and "voluntarily" mean that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

this RG is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this RG constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised RG and (2) the specific subject matter of this RG is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this RG or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

Additionally, an existing applicant may be required to comply with new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

If a licensee believes that the NRC is either using this RG or requesting or requiring the licensee to implement the methods or processes in this RG in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 7), and in NUREG-1409, "Backfitting Guidelines" (Ref. 8).

REFERENCES[3]

1. *U.S. Code of Federal Regulations* (CFR), "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy," Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission (NRC), Washington DC.

2. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments," U.S. NRC, Washington, DC.

3. NRC, RG 1.219, "Guidance on Making Changes to Emergency Plans for Nuclear Power Reactors," U.S. NRC, Washington, DC

4. International Atomic Energy Agency (IAEA), Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/255/Revision 5), IAEA, Vienna, Austria, 2011.[4]

5. NRC, RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

6. NRC, RG 1.168 "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

7. NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," U.S. NRC, Washington, DC.

8. NRC, NUREG-1409, "Backfitting Guidelines," U.S. NRC, Washington, D.C.

---

3 Publicly available NRC published documents such as regulations, regulatory guides, NUREGs, and generic letters listed herein are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail PDR.Resource@nrc.gov.

4 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their Web site: WWW.IAEA.Org/ or by writing the International Atomic Energy Agency P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria. Telephone (+431) 2600-0, Fax (+431) 2600-7, or E-Mail at Official.Mail@IAEA.Org

APPENDIX A

The following questions may be used to aid with the screening of planned and emergent activities or changes. If the answer to any of these screening questions is "yes," compensatory or mitigative actions or both may be necessary to maintain safety or security.

(1) Could the proposed change or activity decrease the reliability or availability of a security system to perform the intended functions?

(2) Could the proposed change or activity increase the likelihood of malfunctions of security equipment or systems?

(3) Could the proposed change or activity decrease the effectiveness of NRC-approved security plans or invalidate the site protective strategy (e.g., communications, response timelines and pathways, equipment and systems (particularly target sets), or protected fighting positions and fields of fire)?

(4) Could the proposed change or activity interfere with detection (i.e., interior and exterior sensors, zone of detection and field of view, alarm communications, or access control systems), delay barriers, and assessment functions?

(5) Could the proposed change or activity impact response times of emergency or armed security personnel (e.g., manmade or natural and active or passive vehicle barriers, vehicle access control and channeling barriers, access delay systems, exterior (protected area) delay barriers, interior delay barriers (passive, active, or dispensable))?

(6) Could the proposed change or activity increase the numbers of, change configurations of, or create a new target set(s) from those previously evaluated?

(7) Could the proposed change or activity reduce adversary task times?

(8) Could the proposed change or activity result in noncompliance with the NRC's security regulations?

(9) Could the proposed change or activity in either cyber security controls or in the area of Secure Analysis create an adverse effect by altering the original intended design? Specifically, have the reviews for interfacing physical and cyber security controls for safety system functional development found in RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 5) been performed; and if so, did the review of the Secure Analysis for digital computer software as stated in RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 6) (see staff regulatory guidance number C.7.c of RG 1.168) occur with an outcome contrary to the requirements?

(10) Could the proposed change or activity adversely impact current agreements with local law enforcement agencies (LLEAs) which are needed to ensure that offsite emergency preparedness personnel or responders (e.g. LLEAs) are permitted access to the site?

(11) Could the proposed change or activity negatively impact mitigative actions that are necessary to be performed by emergency response organization during a declared radiological emergency, including an adversary attack provided for in site security plan?

(12) Could the controls put in place to reduce risks during a force-on-force exercise adversely impact the safety security interface (e.g. safety-related equipment barriers being placed to prevent bumping by security personnel or negative interactions that could result from the use of blank ammunition, laser equipment emissions, radio transmissions, etc.)?

(13) Could the proposed change instituted as a result of emergent or temporary activities negatively impact the safety-security interface (e.g. 1: Does the placement of security barriers diminish access to fire suppression equipment; 2: Does the fire protection manual operator actions account for paths of travel through security fields of fire which could delay or prevent operator response; 3: Does the placement of scaffolding during maintenance activities or the staging of temporary equipment affect security lines of fire within security isolation zones; 4: Will the placement of trailers or heavy equipment obstruct detection and assessment functions or increase the response times of security personnel; or 5: Will construction activities that remove or degrade physical barriers allow established access controls to be bypassed)?

(14) Could cyber security activities such as installing password protection programs on devices plant operators use for safe plant shutdown result in time critical delays for plant operators when they attempt to actuate a device during a safety-related incident?

(15) Could system maintenance, construction, or repair activities result in degradation that requires compensatory measures (e.g. does a pipe system that is being drained lead to a degradation and has there been an evaluation of the need for compensatory measures)?

(16) Could emergency response actions result in a negative impact on the safety security interface (e.g. did emergency response actions fail to involve security personnel in decisions to install equipment or take actions designed to mitigate potential damage to safety significant systems that may be caused by a natural disaster)?