U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-07

Task Working Group #7:
Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities

Interim Staff Guidance
Revision 0-For Public Comments

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-07

Task Working Group #7: Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities

Interim Staff Guidance

Revision 0—For Public Comments

OFFICE	NMSS/FCSS	NMSS/FCSS	NRR/DE	OGC/NLO	NMSS/FCSS
NAME					
DATE	/ /	/ /	/ /	/ /	/ /
OFFICE	NRO/DE	NSIR/DSP	RES/DFER	NMSS/FCSS	NRR/ADES
NAME					
DATE	/ /	/ /	/ /	/ /	/ /

OFFICIAL RECORD COPY

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-07

Task Working Group #7:
Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities

Interim Staff Guidance
Revision 0 – For Public Comments

Introduction

The application of well-designed digital system technology can result in a significant improvement in the reliability of control systems. However, the selection of digital system technology for use in safety applications requires a thorough understanding of the unique operational and performance aspects of digital control technology, an appropriate evaluation of the potential for new modes of control system failures, and knowledge of potential risks associated with the occurrence of natural phenomena, electromagnetic or other induced environmental phenomena, human error, hardware/software performance issues, and security vulnerabilities.

This Interim Staff Guidance (ISG) provides licensing review criteria that address acceptable means of implementing digital I&C applications used to accomplish safety functions in fuel cycle facilities. Title 10 of the Code of Federal Regulations (CFR) section 70.61 (e) requires that each engineered or administrative control or control system necessary for the facility to meet its licensed performance requirements shall be designated as an item relied on for safety, and that a facility safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements for the facility. Further, Section 70.64 (a) (1) requires new facilities or new processes at existing facilities to address baseline design criteria, including the use of quality standards which direct that "the design must be developed and implemented in accordance with management measures, to provide adequate assurance that items relied on for safety will be available and reliable to perform their function when needed." Management measures are defined as the functions performed by the licensee, generally on a continuing basis that are applied to items relied on for safety (IROFS), to ensure the items are available and reliable to perform their functions when needed. The phrase "available and reliable," as used in 10 CFR Part 70, means that, based on the analyzed, credible conditions in the ISA, IROFS will perform their intended safety function when needed to prevent accidents or mitigate the consequences of accidents to an acceptable level. Management measures are implemented to provide reasonable assurance of compliance with the facility performance requirements, considering factors such as maintenance, operating limits, common-cause failures, and the likelihood and consequences of failure or degradation of the IROFS and the measures. Management measures include configuration management, maintenance, training and qualifications, procedures, audits and assessments, incident investigations, records management, *and other quality assurance elements*. (Ref.: 10 CFR 70.4)

10 CFR 70.62 (d) pertains to establishing management measures, and states that the application of such measures must ensure that engineered and administrative controls and control systems identified as IROFS are properly "*designed, implemented*, and *maintained*, as necessary, to ensure that they are available and reliable to perform their function when needed."

The identification and selection of appropriate management measures may use a risk-informed process. Such a process should be used to identify and select management measures to ensure adequate protection of the health and safety of the public in a manner that is commensurate with the reduction of risk attributable to the controls identified as IROFS. An ISA Summary must include, pursuant to 10 CFR 70.65 (b) (4), a description of the management measures. An ISA Summary must also identify, pursuant to 10 CFR 70.65 (b) (8), all IROFS that are the sole item mitigating or preventing an accident sequence for which the consequences could exceed the 10 CFR 70.61 performance requirements.

The Interim Staff Guidance that follows describes license application or amendment review criteria pertaining to key digital I&C design, implementation, and maintenance issues for which there is either little existing guidance because the technology has been developed recently in comparison with currently published guidance, or for which the existing guidance needs to be enhanced to provide for a more consistent review process from application to application. The topics covered in this ISG are:

Note: The information provided in this document constitutes guidance for the review of new license applications, review and evaluation of proposed amendments for existing fuel cycle facilities, and the review and evaluation of license renewal applications. This information is not intended to substitute for NRC regulations, but to provide clarification for NRC staff reviewers as to the determination of acceptable approaches by which a licensee or applicant may satisfy those regulations.

Cyber Security for the Protection of IROFS

Issue

Guidance is needed in reviewing the adequacy of license applications and amendments describing cyber security measures proposed for securing digital instrumentation and control equipment used as items relied on for safety at fuel cycle facilities to ensure that licensed performance objectives will continue to be met.

Introduction

In reviewing a license application, renewal application, or license amendment for a fuel cycle facility, the staff must determine whether there is reasonable assurance that the facility can and will be operated in a manner that will adequately protect the health and safety of workers, the public, and the environment. To carry out this responsibility, the staff evaluates the information that the applicant provides and, through independent assessments, determines whether the applicant has proposed an adequate safety program that is compliant with regulatory requirements. To assist the staff in carrying out this responsibility, a Standard Review Plan clearly states and identifies those standards, criteria, and bases that the staff will use in reaching licensing decisions.

Key design goals stated in 10 CFR Part 70 associated with the use of instrumentation and control systems in fuel cycle facilities pertain to the use of such systems in the prevention and/or mitigation of identified hazards or potential accident sequences. Digital control systems used to mitigate such events are designated as items relied on for safety (IROFS). Licensees are required to implement management measures to ensure that such controls are available and reliable when called upon to perform their intended functions. One management measure which can be applied to assure that such digital IROFS are available and reliable is to provide assurance that such control systems are designed, implemented, and maintained such that they are protected against the effects of potential cyber events, including the potential for introduction of undesired software onto these systems.

“Cyber events,” as used in this interim staff guidance, covers a wide variety of digital equipment based events that could modify, destroy, or compromise the confidentiality, integrity, and availability of data or software; deny access to systems, networks, services, or data; and impact the operation of systems, networks, and associated equipment. A “cyber event” is the manifestation of either a physical or logical hazard to facility computers, digital control systems, communication systems, data networks, or digitally-controlled support systems for this equipment effected through electronic transmission, removable software media, or embedded software that may (1) originate from either inside or outside the facility, (2) have internal or external components, (3) involve physical or logical perils, (4) be deliberate or non-deliberate in nature, (5) be conducted by agents having either malicious or non-malicious intent, and (6) have the potential to result in adverse effects or consequences to the intended operations of digital equipment or systems within the facility.

Cyber events may originate through deliberate exploits or through inadvertent or unintended consequences of plant activities on inadequately protected digital facility assets. Cyber events could involve the use of computer viruses, worms, malware, false data, denial of service, or other types of exploits. Cyber events also may involve physical attempts to affect the availability of digital controls, such as the altering of environmental conditions maintained by digitally-controlled HVAC equipment in order to impact the functionality of a digital system. Cyber

events may be directed at a specific plant digital system or facility or may be generic (e.g., a virus or worm that exploits a specific security flaw in an operating system but is not targeted against a specific control system or facility). Cyber events may arise from internal sources, external sources, or a combination of the two. Those playing a role in launching or facilitating a cyber event may have malicious intent or be inadvertent contributors. The originator of a computer virus, for example, may have had malicious intent, but it may not have been directed at a specific facility. The virus could be inadvertently introduced into inadequately protected maintenance or test equipment which comes into contact with facility equipment much later than when the virus was originated. Facility safety equipment must be protected in a way that ensures that there will be no compromise in availability or reliability in the event of such inadvertent introduction to the facility.

Management measures are defined in 10 CFR 70.4 as "the functions performed by the licensee, generally on a continuing basis that are applied to items relied on for safety (IROFS), to ensure the items are available and reliable to perform their functions when needed. Management measures include configuration management, maintenance, training and qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements." Paragraph 70.62 (d) requires that the management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety pursuant to the facility performance requirements of paragraph 70.61(e) are designed, implemented, and maintained, as necessary to ensure that they are available and reliable when needed.

This Interim Staff Guidance (ISG) provides criteria which may be used by NRC staff reviewers to assess whether licensees and license applicants have provided reasonable assurance that proposed digital systems and networks within their facilities that are relied upon to protect the health and safety of workers, the public, and the environment, are designed, implemented, and maintained such that they are protected from cyber events.

Discussion

Fuel cycle facilities may implement control systems that make use of digital technology for control measures designated as Items Relied on for Safety (IROFS). Digital information systems may be used to monitor operations of the facility, alert personnel to potential hazardous conditions, or keep track of special nuclear material within the facility. If such systems become compromised through a cyber event, the ability to meet facility performance requirements, prevent radiological sabotage, or prevent the theft or diversion of special nuclear material may be compromised. Therefore, it is prudent to implement management measures to secure such systems from potential compromise due to a cyber event.

Digital control systems and digital information systems may be used to ensure that a facility's production, safety, security, and administrative functions are safely accomplished. Specialized digital control systems may be used to accomplish manufacturing process functions as well as perform critical process safety functions. Digital systems may also be used to keep track of material (including special nuclear material) within the facility and to verify mass of material present at various locations to prevent accidental criticality. Digital systems may be used to support the performance of regular maintenance of critical process equipment at the facility, as well as to maintain configuration of facility procedures and track the accomplishment of training for personnel at the facility. To facilitate the use of the information contained or originating within these systems, fuel cycle facilities often are designed with connections to communications networks which allow access by personnel who need information from these

systems to accomplish their daily work activities. Such connectivity, while providing ease of access to critical information from these systems, also provides a potential path for compromise of the digital control or information systems providing this information, and a potential for accidental compromise of key systems through network-based incidents, such as communications errors that cause buffer overflows or other forms of data transmission errors.

While 10 CFR Part 70 requires that management measures be implemented to assure the availability and reliability of Items Relied on for Safety (IROFS), it is equally important that all such critical digital information and control systems and processes be protected from compromise through either embedded or introduced viruses, Trojan horses, worms, back doors, etc., or through its connectivity features to other digital devices. Since the use of digital systems and equipment throughout the facility may be pervasive, it would be prudent to protect all such digital systems and equipment in a consistent, programmatic manner. However, as a minimum, 10 CFR Part 70 requires that licensees implement management measures to ensure that digital assets performing safety functions or that support the performance of safety functions for the facility are continually protected.

The NRC staff reviewer guidance provided below addresses performance goals, elements, and characteristics of management measures which could be used at fuel cycle facilities to provide reasonable assurance that the functions performed by digital safety equipment at the facility will be designed, implemented, and maintained such that they are programmatically protected.

Management measures should be implemented to ensure that effective cyber security provisions are in place. These measures should prevent cyber events from compromising the confidentiality, integrity, and availability of all IROFS.

The management measures described below are similar to those which would be considered good practice recommendations for implementation at any type of facility for which there is a potential danger to the health and safety of the public should facility digital assets become compromised by a cyber event. Performance goals for these recommended management measures and recommendations for implementing these goals are as follows:

(a) Each license applicant or licensee should provide reasonable assurance that digital computers, instrumentation and controls, and communication systems and networks supporting functions required by the facility to meet its licensed performance requirements are adequately protected against cyber events.

(1) Licensees should protect digital computers, instrumentation and controls, and communication systems and networks associated with:

(i) Safety-related and important-to-safety functions, including all IROFS, and

(ii) Support systems and equipment which, if compromised, would adversely impact the performance of required safety functions.

(2) Licensees should protect the systems, controls, and networks identified in (a)(1) from cyber events that would:

(i) Adversely impact the availability, integrity, or confidentiality of data and/or software;

(ii) Deny access to systems, services, and/or data; and

(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) To accomplish this, licensees should:

(1) Analyze digital computer, instrumentation and controls, and communication systems and networks and identify those facility assets that should be protected against cyber events to satisfy paragraph (a) above, and

(2) Establish, implement, and maintain effective cyber security management measures for the protection of the assets identified in (b)(1) above from cyber events.

(c) The cyber security management measures should be designed to:

(1) Implement security controls to protect the assets identified in (b)(1) above from cyber events;

(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber events,

(3) Mitigate the adverse affects of cyber events; and

(4) Ensure that the functions of protected assets identified in (b)(1) above are not adversely impacted due to cyber events.

(d) As part of the cyber security management measures, licensees and should:

(1) Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

(2) Evaluate and manage cyber risks.

(3) Ensure that modifications to assets identified in (b)(1) above, are evaluated before implementation to ensure that the cyber security performance objectives identified in (a)(1) are maintained.

(e) To ensure that each element of the cyber security management measures is addressed appropriately, it is recommended that licensees establish, implement, and maintain a cyber security plan to implement the cyber security objectives.

(1) The cyber security plan should describe how the performance goals outlined in (a) above will be implemented, including how the facility accounts for site-specific conditions that affect implementation.

(2) The cyber security plan should include measures for incident response and recovery from cyber events. The cyber security plan should describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber events;

(ii) Mitigate the consequences of cyber events;

(iii) Correct exploited vulnerabilities; and

(iv) Restore affected systems, networks, and/or equipment affected by cyber events.

(f) To ensure that the performance goals in (a) above are continuously carried out as a part of facility normal operating and administrative practices, licensees should develop and maintain written policies and implementing procedures to implement the cyber security plan, or incorporate the applicable implementing steps into existing facility procedures, such as the facility configuration management program procedures. Such plans, implementing procedures, site-specific analyses, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the license application. However, a high level summary of the management measures proposed to accomplish the protection of IROFS from cyber events should be included in the discussion of management measures contained in the license application. This discussion should be sufficiently detailed to describe how the licensee plans to assure the availability and reliability of IROFS and supporting systems and equipment identified in the ISA Summary through the implementation of management measures designed to protect them from cyber events. The specific facility implementing processes and procedures are subject to periodic inspection at the facility by NRC staff.

(g) Licensees should annually assess the effectiveness of the cyber security management measures, making compensating adjustments to the program where this assessment indicates that the performance objectives in items (a)--(f) above are not being met.

The term “reasonable assurance” in paragraph (a) above implies that adequate protective measures can and will be taken to prevent adverse impacts to IROFS and systems and equipment that support the functions of IROFS from cyber events. Reasonable assurance is based on licensees’ complying with NRC regulations while addressing guidance and other recognized cyber security standards and guidance from professional organizations. Further, reasonable assurance is based on licensees demonstrating that they are effectively implementing plans, procedures, and processes that can prevent, detect, block, mitigate, and recover from a cyber event that could potentially compromise the availability or reliability of IROFS.

The term “safety related” described above generally refers to those IROFS functions identified through an Integrated Safety Analysis process for the facility that are needed to assure facility safety, and the health and safety of the public, in the event of all relevant hazards, including radiological, nuclear criticality, fire, and chemical. It applies to, but is not necessarily limited to, the functions of all systems, networks, equipment, and components designated as IROFS. “Support systems and equipment” refers to those systems and equipment needed to allow the safety related systems to perform their protective actions, such as the electrical power needed to energize the safety equipment, or the heating, ventilating, and air conditioning equipment needed to assure that the safety equipment is performing within its design basis environmental conditions.

"Available and reliable to perform their function when needed" means that, based on the analyzed, credible conditions in the integrated safety analysis, items relied on for safety will perform their intended safety function when needed, and management measures are implemented to ensure compliance with the performance requirements of 10 CFR 70.61, considering such factors as necessary maintenance, operating limits, common-cause failures, and the likelihood and consequences of failure or degradation of the items or the management measures. (Ref. 10 CFR 70.4).

Staff Guidance

To assist in the review of applications for new licenses, license renewals, and license amendments, the NRC staff has developed the following guidance for the review of proposed management measures used to mitigate or prevent cyber events from compromising the functions of IROFS at fuel cycle facilities. Acceptable management measures are those which address all of the following programmatic elements:

- developing effective cyber security management measures, and implementing them through a cyber security plan,
- applying appropriate and sufficient resources within the facility to implement the cyber security management measures whose mission is to protect facility safety functions against compromise by cyber events,
- identifying and defining the roles and responsibilities of personnel to implement all management measures requirements,
- developing facility cyber security policies and implementing procedures,
- implementing risk-management practices that assure a continuous process exists for identifying and documenting the digital assets that need to be protected; performing consistent assessment methods for evaluating the vulnerabilities of these assets to potential cyber events; evaluating the potential consequences to the facility or process systems within the facility due to such events; selecting appropriate digital protection or security controls commensurate with the degree of overall risk to these assets to limit the risk; and evaluating the residual risk to the facility to ensure that once the digital security controls have been implemented, the remaining risk is acceptable and will allow the facility to continue to meet its performance requirements,
- incorporating elements of the cyber security management measures into the facility configuration management program,
- identifying appropriate defense-in-depth protective measures and appropriate risk-based security controls for each digital asset needing protection,
- identifying and implementing appropriate cyber event mitigation measures,
- establishing an effective training and awareness program for personnel designing, operating, maintaining, and updating digital assets; the contents of which are commensurate with the organizational roles and responsibilities assigned,
- performing effective cyber security evaluations of equipment and support systems required to meet the facility performance requirements, prior to implementing new or modifying existing digital assets,
- maintaining the effectiveness of the cyber security management measures by performing periodic cyber security evaluations of the facility to identify where improvements may be required,
- developing effective incident response and recovery plans and identifying organizational resources and personnel responsibilities for implementing these plans, and
- protecting cyber security related information.

License applications and license amendments should address the use of management measures to accomplish the protective actions described above in areas that facilitate the ability of the applicant to meet the facility safety performance requirements. The licensee or license applicant should include with his amendment or license application a description of the management measures proposed for implementing facility cyber security processes that contains, among other topics, the location where a listing of the anticipated critical digital systems, networks, and assets performing facility and process safety functions may be inspected by NRC reviewers; the approach that is being used for identifying or classifying all critical assets needing protection; the location of where a high-level overview may be inspected by NRC staff that describes the proposed architecture demonstrating proposed connectivity among assets or between the control room and the assets, or between the internal plant networks and external corporate and public networks; a description of the proposed defense-in-depth strategies that will be used to protect the equipment; a description of the licensee's or applicant's plan to detect the onset of and prevent cyber events; a description of the proposed event response and recovery process; identification of the proposed management organization ultimately responsible for implementing the elements of the management measures; a description of the cyber security awareness and training program to be administered and the characteristics of the specific training requirements for the various classifications of personnel who will receive such training; and a description of the proposed method for protecting digital assets that have no normally-connected external connections.

For new safety related digital system or equipment applications proposed for use within a new facility or proposed new addition to an existing facility, licensees and applicants should describe the steps that are planned to assure that such new assets have been procured through a process in which the equipment, while being developed and integrated, are maintained free from hidden viruses, Trojan horses, back doors, worms, etc. beginning with their initial conceptual design stages and extending through in-process development and validation/verification testing, final factory testing, through their ultimate installation, acceptance testing, and start-up testing within the fuel cycle facility, and that elements for maintaining the digital equipment free from such unwanted software are included in the facility configuration management program.

Individual IROFS that make use of digital technology may be equipped with ports through which maintenance or operating information is transmitted. Since these ports may be accessible to plant personnel using laptop computers, removable data media (such as flash drives,) or programmable maintenance and test equipment, these ports may be susceptible to inadvertent cyber intrusion. Further, such devices are often connected to in-plant networks which have the potential for compromise by cyber intrusion. Such networks may also be connectable via network switches through firewalls, or individual components on the network may communicate via modem to authorized personnel for accomplishing maintenance functions. Such connectivity enables those networks or devices to be susceptible to cyber events. Examples of such equipment may be devices which are used to fulfill both process safety and material control functions, such as weighing scales used for both criticality prevention and to perform material tracking functions. Procedural controls should be in place to ensure that the existence of such ports for connectivity and the potential for use of removable digital media are identified for each digital asset and that these features are protected using appropriate digital security controls. Sources of information which may be used to assist in identifying appropriate digital security controls may be found in References 8 through 11 of this ISG section. A source of information which may be used to identify and analyze facility assets for potential cyber vulnerabilities and classify them as to level of risk may be found in Reference 12.

Often, digital controllers are designed to be maintained using an engineering workstation or hand-held device through which configuration changes to the control software, control settings, desired operating parameters, security updates, or other software configuration changes may be installed and/or verified and tested prior to placing the controller back into service. Whenever a configuration change is being made to a digital controller, regardless of how limited or insignificant the change, there is a possibility that an accidental change may be introduced which could result in an undesirable operation of that controller. For this reason it is critical that access to such engineering workstations or hand-held devices be carefully controlled so as to prevent accidental introduction of undesired or untested software or logic instructions which could compromise the intended operations of the software in the control system being maintained. Further, certain controllers are designed to be made accessible for maintenance by vendors or systems integrators to implement operating or applications systems upgrades or to assist the facility with troubleshooting activities, including through the use of remote access means. Effective security controls should be continually maintained such that no changes to the control system may be made by personnel who have access to the controller without proper authorization processes, authentication techniques, or through the use of secure communications channels through which the changes may be made. Such changes should only be allowed through communications sessions which are time-limited and monitored by cognizant facility Information Technology (IT) personnel responsible for digital security. All data packets sent through facility firewalls and routers to local control networks containing backup software, historical process information, or control equipment with ultimate connections to IROFS, or which can have potential adverse effects on the functions of IROFS, should be monitored by intrusion detection or intrusion prevention devices. All such traffic should be logged, be regularly reviewed for evidence of unusual or out-of-the-ordinary activity, and be made available for recall in the event that it is suspected that a cyber event has occurred so as to provide for a timely diagnosis to support recovery from the cyber event. The facility configuration management program should incorporate appropriate elements of the management measures implementing cyber security protective procedures and practices.

The plant corporate network is often used to access maintenance records or design information for equipment performing safety and process control functions. The plant corporate network may also be used to develop, implement, and track plant procedures, such as operating and maintenance procedures, and training plans. Precautions should be taken to maintain adequate separation of the networks and control systems used to perform plant process control functions and active engineered safety controls from networks used for processing management information. Plant networks and communication channels should be arranged such that critical process control, safety, and material control equipment is protected in a strategic manner so as to apply defense-in-depth protective measures. An example of this would be the use of a succession of network layers, each of which are equipped with firewalls that allow only anticipated authorized traffic and which are continuously monitored using intrusion detection and/or prevention systems. Another acceptable method is to not allow the connection of critical safety equipment to plant networks, even though the device may be equipped with ports to allow such connections.

Coordination of the Safety/Security Interface

Licensees are required to address security advisories originating from federal, state, or local authorities summarizing identified cyber security risks or other vulnerabilities as they arise. When implementing such security advisories, it is important that the potential effects of such security implementations which may interface with facility safety features are evaluated to ensure that any provisions made for assuring facility safety are not negated or compromised by

a proposed security "patch." Similarly, when implementing management measures designed to assure the reliability and availability of safety controls, such implementation should be evaluated to ensure that facility security controls are not compromised. For example, security advisories issued to industrial sectors on a national scale have already been identified as having applicability to nuclear facilities, including fuel cycle facilities. One such advisory concerns recommended security control measures which should be taken to enhance the ability of the facility to protect itself against a particular risk to facility equipment due to a potential digital intrusion event on the transmission and distribution grid system providing power to the facility. Interim Staff Guidance document FCSS ISG-11, Revision 0 (Reference 5 of this section of the ISG) has been prepared to provide guidance for the review of new applications for fuel cycle facilities to ensure that license applicants have adequately addressed this potential vulnerability. License applications addressing this vulnerability should be reviewed in accordance with the guidance contained in FCSS ISG-11. (Note: Specific content of FCSS ISG-11 has been withheld from this ISG, because it addresses material considered to be "Official Use Only—Security Related Information.") Reviewers should evaluate whether the applicant has appropriately considered the potential for adverse interactions to IROFS or conflicting requirements arising out of the implementation of security-related facility management measures.

Acceptability

License reviewers should evaluate the description of the applicant's proposed management measures for IROFS digital cyber security in light of the guidance described above. The application should be considered acceptable if:

a) management measures will be implemented to ensure that effective cyber security practices are in place to protect all IROFS and supporting systems and equipment from compromise in confidentiality, integrity, and availability due to cyber events.
b) the proposed approach addresses the elements described above, and
c) there is sufficient evidence that the proposed management measures, when implemented, will allow the licensee to continually assess the effectiveness of these measures and enhance them in areas indicating improvements in effectiveness are needed.

Regulatory Basis

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," including Section 70.1, "Purpose," Section 70.4, "Definitions," Section 70.21, "Filing," Section 70.22, "Contents of applications," Section 70.34, "Amendment of Licenses," and Subpart H-Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material, Sections 70.61 through 70.76.

Technical Review Guidance

The reviewer should use the information contained in this ISG, as applicable, to evaluate whether a licensee or applicant has described in his application appropriate management measures to ensure that digital equipment performing IROFS functions or supporting functions are designed, implemented, and maintained such that they are adequately protected against cyber events. Specifically, the application should describe how the establishment and maintenance of effective management measures for protecting digital IROFS from cyber events will ensure that such digital control and information systems will be available and reliable when called upon to perform their protective safety functions. License reviewers should evaluate the

materials provided in the application and make a determination whether it provides reasonable assurance of adequate safety, or reasonable assurance of adequate compliance with the technical requirements of Subpart H of 10 CFR Part 70.

If the applicant is using NUREG-1520 or NUREG-1718, the reviewer should use the guidance in this document to evaluate the adequacy of the applicant's ISA Summary. The purpose of the ISA Summary review is to verify whether the applicant has an acceptable methodology such that there is reasonable assurance of maintaining an adequate safety basis over the facility lifetime, by ensuring that the methodology results in preventing or mitigating the effects of cyber events on digital assets within the facility which would prevent it from meeting the performance requirements of 10 CFR Part 70, paragraph 70.61.

Recommendations

This guidance should be used to supplement the guidance contained in NUREG-1520 and NUREG-1718 with regard to the provisions for applying management measures to assure the continuous reliability and availability of items relied on for safety per the requirements of 10 CFR Part 70, such that the facility performance requirements of 10 CFR Part 70.61 will continue to be met. Such provisions include the provision of management measures implementing administrative, operational, and technical controls to protect digital equipment so as to assure the reliability and availability of items relied on for safety.

References

1. U.S. Code of Federal Regulations, Title 10, Energy, Part 70, "*Domestic Licensing of Special Nuclear Material*."
2. U.S. Code of Federal Regulations, Title 10, Energy, Part 73, "*Physical Protection of Plants and Materials*," including Section 73.1*, "Purpose and scope;"* Section 73.2*, "Definitions;"* Section 73.20*, "General performance objectives and requirements;"* Section 73.45 *"Performance capabilities for fixed site physical protection systems;"* Section 73.46*, "Fixed site physical protection systems, subsystems, components, and procedures,"* and 10 CFR 73.54*, "Protection of Digital Computer and Communication Systems and Networks"*
3. U.S. Nuclear Regulatory Commission (USNRC). NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility." NRC: Washington, D.C. March 2002.
4. U.S. Nuclear Regulatory Commission (USNRC). NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility." NRC: Washington, D.C. August 2000.
5. U. S. Nuclear Regulatory Commission (USNRC) Office of Nuclear Material Safety and Safeguards, Division of Fuel Cycle Safety and Safeguards FCSS-ISG-11, Revision 0, "Grid Security Vulnerability"
6. U.S. Nuclear Regulatory Commission (USNRC) Draft Regulatory Guide DG-5022, "Cyber Security Programs for Nuclear Facilities," December 2008
7. U.S. Nuclear Regulatory Commission (USNRC) Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," March 2009
8. National Institute of Standards and Technology. 2006. *Recommended Security Controls for Federal Information Systems* Special Publication 800-53, Gaithersburg, Maryland.

9. National Institute of Standards and Technology, 2008. *Guide for Assessing the Security Controls in Federal Information Systems* Special Publication 800-53A, Gaithersburg, Maryland.
10. National Institute of Standards and Technology. 2007. DRAFT *Guide to Industrial Control Systems (ICS) Security* Special Publication 800-82, Gaithersburg, Maryland.
11. ANSI/ISA-TR99.00.01-2007 *Security Technologies for Industrial Automation and Control Systems*
12. U.S. Nuclear Regulatory Commission (USNRC). NUREG-6847, *Cyber Security Self-assessment Method for U.S. Nuclear Power Plants,* released for industry use in October, 2004

Independence of Controls used for Safety Functions

Issue

Guidance is needed in reviewing the adequacy of license applications and amendments describing the adequacy of proposed approaches for addressing "independence" for digital instrumentation and control system channels and functions designated as items relied on for safety (IROFS).

Introduction

In reviewing a license application, renewal application, or license amendment for a fuel cycle facility, the staff must determine whether there is reasonable assurance that the facility can and will be operated in a manner that will adequately protect the health and safety of workers, the public, and the environment. To carry out this responsibility, the staff evaluates the information that the applicant provides and, through independent assessments, determines whether the applicant has proposed an adequate safety program that is compliant with regulatory requirements. To assist the staff in carrying out this responsibility, a Standard Review Plan clearly states and identifies those standards, criteria, and bases that the staff will use in reaching licensing decisions.

Key design goals stated in 10 CFR Part 70 associated with the use of instrumentation and control systems in fuel cycle facilities pertain to the use of such systems in the prevention and/or mitigation of identified hazards or potential accident sequences. Digital control systems used to mitigate such events are designated as items relied on for safety (IROFS). Licensees are required to implement management measures to ensure that such controls are available and reliable when called upon to perform their intended functions. One management measure which can be applied to assure that such digital IROFS are available and reliable is to provide assurance that such control systems are designed, implemented, and maintained such that redundant or diverse controls will have a low likelihood of being compromised by a potential common-cause failure.

During the preparation and review of Integrated Safety Analysis (ISA) Summaries and License Applications there have been several different interpretations made by licensees, license applicants, and reviewers as to how to treat potential common cause failures associated with digital controls acting as independent control measures that serve as IROFS. The discussion below describes the licensing background and definition of terms supporting the NRC staff guidance which follows. This discussion is based in part on Fuel Cycle Facility Interim Staff Guidance Documents FCSS ISG-01, Rev. 0, "Qualitative Criteria for Evaluation of Likelihood"; FCSS ISG-03, Rev. 0, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle"; and NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility," dated March 2002.

Part 70 of 10 CFR, Subpart H contains three separate requirements to ensure nuclear criticality safety. One requirement, 10 CFR 70.61 (b), requires that high consequence events (which typically will include criticality accidents) be highly unlikely. Another, 10 CFR 70.61 (d), states that the risk of nuclear criticality accidents must be limited by assuring that under normal and abnormal conditions all nuclear processes are subcritical, including use of an approved margin of subcriticality. This provision also requires that the primary means of criticality protection be

prevention. The third requirement, 10 CFR 70.64 (a) (9), requires that the design provide for criticality control, including adherence to the double contingency principle. Licensees have historically committed to the double contingency principle as described in ANSI/American Nuclear Society Standard 8.1, "Nuclear Criticality Safety in Operations with Fissionable Materials outside Reactors." (ANSI/ANS-8.1). Within the context of this standard, the double contingency principle is stated as:

> "Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible."

This standard also requires that nuclear processes be maintained subcritical under normal and credible abnormal conditions. By contrast, the DCP is stated as a "recommendation" of ANSI/ANS-8.1. Therefore, the standard recognizes that adherence to the DCP can be one means, but is not necessarily the only means of meeting the underlying subcriticality requirement.

Section 70.64 applies both to new facilities, and to new processes at existing facilities, and contains a set of key baseline design criteria. Licensees are required to maintain the application of these criteria unless the ISA prepared per requirements of Section 70.62 (c) demonstrates that a particular item is not relied on for safety or does not require adherence to the specified criteria. Among the criteria required to be addressed is a criterion that the design must provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety. Another criterion is that which has been described above, concerning the requirement that the design provide for criticality control, including adherence to the double contingency principle. Facility and system design must be based on defense-in-depth practices.

In addition, § 70.64(b)(1) requires that the design must incorporate, to the extent practicable, preference for the selection of engineered controls over administrative controls to increase overall system reliability. Passive engineered controls are generally preferable to active engineered controls. In addition, the process design should rely on diverse means of control (e.g., reliance on two different criticality parameters or different means of controlling one parameter) whenever practicable, to minimize the potential for common-cause failure. Cases in which these preferences cannot be complied with will generally require justification to show how adherence to the performance requirements will be accomplished. For example, one cannot claim that the double contingency principle is met with only two controls (regardless of type) if the resulting configuration fails to protect against all credible pathways to criticality or limit the risk of inadvertent criticality as required in 10 CFR 70.61(d).

Section 70.62 (d), "Management measures," requires that licensees establish a system of management measures to ensure that engineered and administrative controls and control systems that are identified as IROFS are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed. The provision further states that the measures must ensure compliance with the performance requirements of Section 70.61, and that such management measures may be graded commensurate with the degree of risk that is attributable to the control system.

This Interim Staff Guidance (ISG) provides criteria which may be used by NRC staff reviewers to assess whether the management measures proposed for the facility will provide adequate assurance that digital I&C equipment relied on for safety are designed, implemented, and maintained such that they will be available and reliable to perform their safety functions when

needed. ISG topics include criteria for assuring the independence of channels of digital instrumentation and controls credited in the achievement of protective safety functions, and criticality prevention.

Discussion

NUREG-1520, "Standard Review Plan (SRP) for the Review of a License Application for a Fuel Cycle Facility," describes a process acceptable to the NRC staff for the development of an Integrated Safety Analysis (ISA) Summary to establish reasonable assurance that the applicant has conducted an ISA of appropriate detail for each applicable process, using methods and qualified personnel adequate to achieve the requirements of 10 CFR 70.62(c)(1) and (2). Such a process requires the identification and evaluation of all credible events (accident sequences) involving process deviations or other events internal to the facility (e.g., explosions, criticality events, and fires); and credible external events that could result in facility-induced consequences to workers, the public, or the environment, that could exceed the performance requirements of 10 CFR 70.61. It also requires that licensees designate engineered and administrative IROFS, and correctly evaluate the set of IROFS addressing each accident sequence, as providing reasonable assurance, through preventive or mitigative measures, and through application of supporting management measures that the performance requirements of 10 CFR 70.61 are met.

The description of each IROFS in the ISA Summary should identify its expected function, conditions needed for the IROFS to reliably perform its function, and the management measures needed to assure its availability and reliability. Other documents which are maintained by the licensee or license applicant but not submitted as part of the license application or ISA Summary may need to be reviewed in order to ascertain the effects on the facility due to a failure of the IROFS. The description within an ISA Summary should identify what management measures, such as maintenance, operations and maintenance personnel training, configuration management, cyber security, etc., are applied to IROFS identified in the ISA Summary. If a system of graded management measures is used, the grade applied to each control should be determinable from information provided in the ISA Summary or in the description of the proposed facility Quality Assurance (QA) Program. The reliability required for an IROFS is commensurate with the degree of risk reduction relied on within the ISA. Thus, the quality of the management measures applied to an IROFS may be graded commensurate with the required reliability. The management measures should ensure that IROFS are designed, implemented, and maintained, as necessary, to be available and reliable to perform their function when needed. The degree of reliability and availability of IROFS ensured by these measures should be consistent with the evaluations of accident likelihoods. The IROFS description should contain sufficient detail about items within a hardware IROFS, such that it is clear to the reviewer(s) and the applicant, what structure, system, equipment, or component is included within the hardware IROFS' boundary and would, therefore, be subject to management measures specified by the applicant. Some examples of items within a hardware IROFS are sensors or detectors, logic devices, valves, pumps, etc. In addition, ISA Summary documentation should also identify essential utilities and support systems on which the IROFS depends to perform its intended function.

One type of IROFS that may be considered for use during facility design is one that makes use of digital instrumentation and control systems equipment. Such equipment includes a channel that is composed of a sensor, a communications path to a "logic solver" (e.g., a programmable logic controller (PLC) or a distributed control system (DCS)), an output driver, and a solenoid valve. If the ISA Summary indicates that a particular IROFS needed to prevent or mitigate an

identified process hazard must provide a high degree of risk reduction to allow the facility to meet its performance requirements, one method of implementing management measures to increase the availability and reliability of the controls may be to include in the design a redundant channel of controls to accomplish the IROFS functional requirements or a diverse channel of controls IROFS to accomplish the IROFS function (or one that is both redundant and diverse) that independently monitors the process and communicates with an independent logic solver, output driver, and solenoid valve to provide added assurance that the total system performance will be sufficiently reliable for the facility to meet the performance requirements. Another approach may be to utilize multiple channels of controls, each providing low risk reduction credit, but when functioning collectively, provide for a high degree of risk reduction. A redundant IROFS is one which is separate from but performs essentially the same safety function as another IROFS. Redundant IROFS may be either diverse or non-diverse; it is not necessary for them to consist of identical equipment. However, when redundancy is provided by identical equipment or operator actions, it is important to ensure that all credible common-cause failures have been identified and taken into account when estimating the reliability of the protective measure.

Double Contingency Principle

Section 70.64 (a)(9), states that the design for criticality control/prevention for new facilities and new processes at existing facilities must adhere to the double contingency principle. Interim Staff Guidance FCSS-ISG-03, Revision 0, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle," provides clarification on how to address designs meeting the double contingency principle in a facility that is required to meet the performance requirements of § 70.61. The double contingency principle is stated in paragraph 4.2.2 of ANSI/ANS-8.1-1998, "Nuclear Criticality Safety in Operations with Fissionable Material Outside Reactors" as,

> "Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible."

Alternatively stated, at least two, rarely occurring, independent, concurrent failures of control measures must occur, each of which results in a change to the process conditions, before it is possible for a criticality event to occur. Guidance in FCSS-ISG-03 further provides the following NRC staff positions:

> At least two: "The presence of two controls may not be necessary, or may not be sufficient, to meet the DCP. The DCP does not necessarily require two controls; it requires that "at least two…changes in process conditions" occur before criticality is possible. Meeting this may necessitate one, two, or more than two controls depending on the possible conditions that can lead to criticality. In general, there may be several possible pathways for a process to reach criticality and, therefore, in many cases, more than two controls may be required to meet the DCP for a particular process application where a criticality event is credible."
>
> Unlikely: "Unlikely changes in process conditions should be expected to occur rarely, or not at all, during the lifetime of the facility. Operational failure events that occur regularly should not be counted as a contingency relied on to meet the DCP although they may constitute part of a contingency if a combination of events may be considered unlikely. Therefore, the occurrence of any such event generally reveals a deficiency in the design

that should result in corrective action. Determination that a failure contingency is unlikely should be based on objective attributes of the criticality controls, rather than on subjective judgment alone. Examples of such attributes are environmental factors that can degrade the reliability and availability of controls, margin, and redundancy and diversity of controls. (Guidance on some of the availability and reliability qualities that should be considered is provided in NUREG-1520, Section 3.4.3.2(9).) Management measures must be provided, as needed, to ensure that the failure of the criticality controls is an unlikely contingency."

Independent changes in process conditions are such that one contingent control measure failure neither causes another contingency nor increases its likelihood of occurrence. This means not only that the occurrence of one contingency (synonymous with the failure of one control measure) does not cause the occurrence of the other, but that it also does not make the second failure significantly more likely. The existence of a credible common-cause failure resulting in the occurrence of both contingencies means that it is not valid to consider them truly independent. This definition is stricter for systems of control measures that are required to meet the double contingency principle than for other control measures that only have to meet the requirements of 10 CFR 70.61. However, if the resulting process condition due to the failure of either control measure leg of the double contingency is such that the process remains sub-critical, including margin, then the performance requirements of 10 CFR 70.61 are still being met, (provided there is an analysis to show that there would be no synergistic effects on the process due to the concurrent double failure that can then lead to a loss of sub-criticality,) even though the requirements for meeting the double contingency principle are not strictly being satisfied.

Concurrent does not mean that the two changes in process conditions must occur simultaneously, but that the effect of the first failure contingency persists at least until the second contingency occurs. Timely detection and correction of abnormal conditions should thus be provided to restore double contingency protection. (For a discussion of what constitutes a "timely" response, please see the section entitled "Practical Considerations Regarding the Evaluation of Potential Common Cause Failure Conditions for Control Systems" below.) The time (duration) required for the detection and correction of failures should be significantly shorter than the anticipated time between failures in order for there to be significant risk reduction provided from failure detection.

"Changes in process conditions" does not imply that reliance on two different parameters is mandatory to meet the DCP. Reliance on two different parameters is preferable to reliance on two controls on a single parameter, however, because it is more difficult to achieve independence when applying two control measures on one parameter. In instances in which single parameter control is unavoidable, great care should be taken to ensure that the potential for common-cause failures is minimized.

Paragraph 70.64(b) requires that new facilities and new processes at existing facilities be designed using defense-in-depth practices. "Defense-in-depth" is a term used to describe the degree to which multiple layers of protective measures, including measures designated as IROFS or systems of IROFS, must fail before the undesired consequences (e.g., criticality, chemical release, fire, etc.) can result. These defenses may be protective measures that are over and above those listed as IROFS and which are not credited for meeting the performance criteria. Defenses which provide for defense-in-depth may be either independent or dependent,

although they should be independent whenever practical because of the possibility that the reliability of any single IROFS may not be as great as anticipated. The use of defenses maintaining independence from one another to achieve a particular safety function will make the results of the risk evaluation more tolerant of error (i.e., less uncertain.) In addition, IROFS must be truly independent if the method for likelihood determination assumes independence (such as methods relying on summation of indices). IROFS are independent if there is no credible single-event (common cause failure) that can cause the safety function of each IROFS to fail. Multiple independent IROFS generally provide the highest level of risk reduction. The degree of redundancy, independence, and diversity are important factors in determining the amount of risk reduction afforded by the system of IROFS.

Consequences of non-Independence: As stated above, to qualify as being independent, the failure of one IROFS should neither cause the failure nor increase the likelihood of failure of another IROFS. No single credible event should be able to defeat the system of protective measures and IROFS such that an identified consequence event/criticality is possible. A systematic method of hazard identification should thus be used to provide a high degree of assurance that all credible failure mechanisms that could contribute to (i.e., initiate or fail to prevent or mitigate) an accident have been identified. Methods commonly used for likelihood evaluation generally assume that the chosen IROFS are independent. Examples of these methods include Layer of Protection Analysis (LOPA) and the index method of Appendix A of NUREG-1520. In a small number of cases, it may not be feasible to entirely eliminate the possibility of dependent or common cause failures. For those instances, methods of evaluating likelihood that rely on independent IROFS should not be used to evaluate the likelihood of systems of IROFS with dependent failures. Instead, the analysis of likelihood should be adjusted such that the contribution to the calculation of event likelihood appropriately takes into account the dependency due to the common-cause failure mechanism.

If, however, the common-cause failure is sufficiently unlikely, it may be possible to treat IROFS as independent for purposes of the ISA and ISA Summary. The establishment as to whether a common-cause failure is sufficiently unlikely is discussed below under “Staff Guidance.”

There are numerous factors that could lead to IROFS not being independent, and the presence of these factors can have a significant effect on the degree of protection offered by what are considered to be independent IROFS. A partial list of conditions that may lead to two or more IROFS not being independent follows:

1. Administrative actions that are performed by the same individual.
2. Administrative actions that are performed by two different individuals but using the same equipment and/or procedures.
3. Two engineered controls that share a common hardware component, communications path, or common software that has not been developed through a high quality design process or has not been thoroughly validated and verified. For example, redundant controls may make use of the same type of logic controller, which may utilize identical microprocessors, operating systems, applications software, and may have been developed by the same design and implementation personnel. In applications where different types of logic processors are applied to achieve a level of diversity within the same process safety control, however, hardware components such as random access memory (RAM), flash memory, communications gateways, etc. may still be of the same manufacturer and model within the two different logic processors. It is important to analyze and understand the implications of the arrangement of hardware and software components of IROFS that require redundancy to determine whether the level of

commonality between proposed redundant controls could pose a significant potential contribution to common cause failure for these IROFS to not be truly functionally independent.

4. Two engineered controls that measure the same physical variable using the same model or type of hardware. (However, if it can be demonstrated that the system of controls implementing that model or type of hardware has a documented reliability that is so high as to preclude its failure within the time frame needed to perform its protective functions, then it may be considered for all practical purposes to be independent. For instance, the use of the same process chemical analyzer for both controls that have a common mode failure component with a Mean Time Between Failure (MTBF) of less than 2000 hours would have a low reliability and high likelihood of failure, in comparison with two controls each making use of a simple thermocouple with a common mode failure component with a MTBF of greater than 100,000 hours.)
5. Two engineered controls that rely on the same source of essential utilities to perform their protective actions (e.g., electricity, instrument air, compressed nitrogen, water).
6. Two engineered controls that are co-located such that credible internal or external events (e.g., structural failure, forklift impacts, fires, explosions, chemical releases) can cause both to fail.
7. Administrative or engineered controls that are susceptible to failure due to presence of credible environmental conditions (e.g., two operator actions defeated by corrosive atmosphere, sensors rendered inoperable due to high-temperature or weather-related incidents).

The presence of any of these conditions does not necessarily mean that the redundant or multiple IROFS cannot be considered independent, but additional justification demonstrating the absence or extremely low likelihood of common-cause failure should be discussed within the license application or made available for inspection. The likelihood of such conditions in relation to the overall likelihood of a hazardous event sequence should be factored into making the determination of how significant the common-cause failure is.

Diversity is the degree to which protection is provided by IROFS which perform complementary safety functions, such that different types of failures of the IROFS are required before the complete loss of protection is possible. Diverse controls may consist of controls on different parameters or different means of controlling the same parameter. When choosing multiple controls for mitigating the same accident sequence, preference should be given to diverse means of control, because they are generally less susceptible to common-cause failure. However, it is still necessary to consider all credible failure modes of the system when evaluating the overall likelihood of failure. Diversity of controls may also be achieved through the use of different model digital processors, different software, and different engineering teams developing the design.

Vulnerability to Common-Cause Failure

Diverse means of control should be provided whenever practicable to minimize the potential for common-cause failure. For example, NUREG-1520, Section 5.4.3.4.4(7)(a), states that for criticality protection, a two-parameter control should be considered preferable to two controls on one parameter. Where a two-parameter control is not practicable, diverse means of controlling a single parameter should likewise be considered preferable to two redundant controls on that single parameter.

It is not possible to provide absolute assurance that IROFS are independent. However, if the cumulative likelihood of all common-cause failures of a system of IROFS is significantly less than the independent failure of the system of IROFS, (see Staff Guidance, below) then the IROFS may be treated for all practical purposes as independent.

If the potential for credible common-cause failures cannot be eliminated as discussed above, then they must be considered in evaluating the overall accident sequence likelihood. A likelihood evaluation method (whether quantitative or qualitative) that correctly treats dependent failures should be used when such failures are present. Guidance for performing such evaluations is contained in Appendix A of Chapter 3 of NUREG-1520.

Staff Guidance

The following guidance is for reviewers of license applications and amendments. This guidance is to be used in evaluating the licensee's or applicant's assessment of likelihood of potential common cause failure contribution (for example, where a licensee or applicant proposes to use multiple or redundant controls as IROFS for event risk reduction measures.)

Subpart H of 10 CFR 70 requires licensee and license applicants to perform an Integrated Safety Analysis for their facilities. Licensees are required to assure that each credible high consequence event is rendered highly-unlikely, and that intermediate consequence events are unlikely. To demonstrate that these performance-based requirements are met, licensees are required to identify all potential internal and external credible hazards for their facilities, and to provide a definition of unlikely, highly unlikely, and credible, as used in the evaluation of their safety analysis. To estimate the reliability of the control measures used to achieve the highly-unlikely, unlikely, and credible consequence occurrence, modeling is performed using qualitative and/or quantitative methods.

One method of assessing overall reliability for a set of engineered control measures used for mitigation or prevention of a particular identified hazard is known as the "index method." This method involves using a summation of the indices approach to estimate the probability of failure on demand for individual engineered control measures being assessed. Such individual engineered control measures may consist of a set of component sensors, a logic solver, and an output to a controlled device. It is possible that multiple safety instrumented functions may be used as IROFS or systems of IROFS to accomplish facility safety functions, including nuclear criticality prevention. Each component of these control measures has its own probability of failure on demand, which can be combined via appropriate modeling for a particular engineered control measure to achieve an overall figure for the likelihood of failure on demand for the combination of engineered control measures. Alternatively, qualitative assessments of likelihood of failures may be used and then combined to arrive at an overall estimate of IROFS failure on demand.

For this index methodology to remain an accurate estimate of the overall likelihood of occurrence for a particular event, functional independence of control mechanisms serving as individual IROFS applications has been assumed in the model. If these control measures are not, in fact, sufficiently independent, then the overall calculation of event likelihood is questionable.

It is the NRC staff position that if the combined sum of the likelihoods of all potential common-cause failures which can occur for a system of IROFS is significantly less than the independent failure which can occur for a system of control measures serving as IROFS, then the IROFS

may be treated in the index methodology analysis for all practical purposes as independent. It is also the NRC staff position that "significantly less" means that the likelihood of the cumulative effect of the common-cause failures should be at least two orders of magnitude (1E-2) (preferably three orders of magnitude) less than the estimate for the independent failures within the system of IROFS. (That is, the common cause failure contribution to the total likelihood of failure is no more than an additional 0.1% (0.001) -to-1.0% (0.01) of the estimate of total likelihood of failure for the combination of presumably independent control measures.) Qualitatively, when using the index method of likelihood evaluation, this means the likelihood of the common-cause failure should be sufficiently low that it does not change the index score for the likelihood of occurrence of the accident or hazard consequence for the system of IROFS preventing it.

This means that in most event sequences analyzed there must be no identified credible common-cause failures, however, in a few cases, dependent (common cause) failures may be unavoidable. For those unavoidable cases, licensees and license applicants need to analyze them appropriately, and where the analysis demonstrates that they are at least two (and preferably three) orders of magnitude less likely than a failure of the independent IROFS (i.e., they add at most 1.0% contribution to the overall event sequence likelihood) they may be considered negligible. Example: Suppose the event analysis demonstrates that a risk reduction factor of at least 1E-4/yr is required, and a proposed system of IROFS using two controls, each with a likelihood of failure of 0.01/year. The common cause failure for these two controls should be not credible. However if it is credible, to be considered negligible, it should be no more likely than 1E-6/year (since the two controls, if independent, would provide a risk reduction of (0.01)(0.01), or 1E-4, and the common-cause failure contribution of 1E-6 should be two orders of magnitude smaller.

Practical Considerations Regarding the Evaluation of Potential Common Cause Failure Conditions for Control Systems

When applying digital control systems as IROFS for achieving the performance goals of 10 CFR 70.61, there are a number of considerations to be evaluated before one can safely conclude that a particular potential common-cause failure's contribution to the total likelihood of failure is no more than an additional 1% (0.01) of the estimate of total likelihood of failure for the combination of individual digital control system control measures being applied. For IROFS used as control measures to prevent criticality, there must be no credible common cause failure which could affect both independent control measures. A clarification to this, however, is that for those cases where it can be demonstrated that resulting process condition due to the failure of either control measure leg of the double contingency is such that the process remains sub-critical, including margin, then the performance requirements of 10 CFR 70.61 are still being met. For this to occur, there must be evidence demonstrating that consistent known faulted states of the control system are being achieved when any likely form of control system failures occur, and that these known faulted states result in the safe application of controls to prevent criticality. (See discussion below regarding "Identification of All Potential Failure States of a Control System") No change in process condition should occur through any form of likely potential failure of the control, and no criticality condition should occur even when both legs of the control measure have reached their known faulted states.

This would imply that systems of IROFS whose failure condition is always in the "safe state" so as to prevent the occurrence of the postulated event consequence, would be considered acceptable for meeting the double contingency requirement. If such "fail-safe" state control systems are proposed for use, however, there must be a confirmation in the license application

that the availability and reliability of such a system of IROFS will be ensured by appropriately scheduled periodic functional testing, maintenance, and a high quality alarm system to indicate its failure. There should also be an independent mechanism not subject to the same common cause failure as the fail-safe system of IROFS, through which an operator can take action to place the process in a safe state in a timely manner in the event that he has evidence that a failure of the control has occurred, but for some reason he cannot confirm that the process has automatically been put into its safe condition. "Timely" here means that a licensee analysis demonstrates that the process can be repeatedly placed into its safe state by an operator using that mechanism before an event sequence can propagate into an unsafe condition. Periodic functional test programs must be able to demonstrate that each individual IROFS can be consistently shown to respond to its individually analyzed and defined "fail safe" condition when tested. For certain systems of IROFS, there may not be a clearly-defined "fail safe" state. For these systems, evaluations must be made by the system designers to determine the best or "safest" condition they deem the facility should be placed assuming that the most likely mode of failure for the IROFS has occurred.

Identification of All Potential Failure States of a Control System

Recent nuclear facility events have occurred during which failures have occurred within digital control systems that had previously been evaluated to fail into a known state, but the control system instead failed into a state that was previously unknown or unanticipated under the facility conditions experienced. One of these events was for a facility for which it had been anticipated that when the control system failed, certain valves would be commanded by the fail state of the control system to travel to their "full-open" positions. During this event, when power was momentarily lost to the control system, the valves did indeed go to their programmed "open" position. However, when power was restored to the control system, the controllers reverted to their last known operating state ("full closed") which was not a safe condition for the mode of operation of the facility at the time of the momentary control system power failure. Upon investigation of the root cause of this incident, it was learned that an inadequate evaluation of the performance of the control system led to an incomplete or incorrect specification of the modes of operation of the controllers, resulting in undesired facility conditions.

In another incident, power to the controller was continuously available; however the communications between the local controller and its unit server was temporarily interrupted when an update of the server was occurring. Upon restoration of the communications, however, the local controller went into a re-initialization mode, during which time the processors read a momentary "zero-state" of its inputs and commanded all its outputs to go to an "off" state, which was not a desired condition for the mode of operation in which the facility was operating. The re-initialization process experienced by the controller had been an unknown mode of operation of the controller to the systems designers, so it had not been accounted for in the design of the facility.

Since examples of events such as these are known to have occurred, extreme care should be used by systems designers when identifying failure modes and failure states of the control systems used in safety applications to be accommodated. It should not be automatically assumed that "obvious" failure modes of a control system are its only possible failure modes. License reviewers should evaluate applications for evidence that the applicant has performed a thorough evaluation of all potential failure modes for the control systems being proposed, including the incorporation of a thorough search of industry operating history for the proposed version of the controller, and that there is reasonable assurance that the applicant has performed a diligent analysis of the proposed failure modes for the system.

Design Compensating Measures for Common Cause Failures

In lieu of the requirement to quantitatively demonstrate that potential common cause failures are sufficiently unlikely, the following coping mechanisms may be used in conjunction with a system of IROFS consisting of channels of digital I&C equipment, logic solvers, and control outputs:

- One active engineered control under configuration management whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure, plus a second active engineered control from a separate and, if possible, diverse automatic control system under configuration management whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure. For example, a digital control channel could be used for one control and a hard-wired set of hardware could be used for the other channel.
- One active engineered control under configuration management controls whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure, plus one passive control under configuration management.
- One active engineered control under configuration management controls whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure, plus one enhanced administrative control in which the instrumentation and devices included in the administrative control are subject to periodic functional testing and maintenance, and the operator action is performed routinely or reinforced by periodic drills and training.
- One active engineered control under configuration management controls whose reliability is ensured by periodic functional testing, maintenance, and an alarm to automatically indicate its failure, plus one simple administrative control in which the reliability of the administrative control is ensured through appropriate procedural layers of redundancy.

It is the NRC staff's position that the nature and estimated likelihood of occurrence of the potential common cause failure must be thoroughly evaluated and compared with the likelihood of failure of the individual digital control functions being applied. In addition, common cause failures identified by the control system vendor as indicated in a validated database of operating history for the particular model of digital platform being applied must be validated for use in analyses of their potential contribution to common cause or common cause failure. Examples of such evaluation considerations are provided below:

Software Common-Cause Failure Considerations

The worst-case common cause failure of a control system would be one in which two presumably independent digital control functions using a common control system platform experience an undetectable failure within their common application system or operating system software features, or suffer a failure due to the inadvertent introduction of inappropriate code entered into their systems through their common system maintenance terminal. Such an undetectable failure could occur whether the platform was actually shared by the independent control functions or whether they were implemented in two separate, but otherwise identical digital platforms. In this instance both control functions could cease to be available to prevent the process from reaching a hazardous condition. (The assumption is made here that the latent

software failure that occurs was not the type of failure that could have been discovered during integrated hardware and software module testing or factory acceptance or installation and start-up testing.) For the evaluation of likelihood position described above to be valid, one must be able to demonstrate and document, in quantitative and/or qualitative terms, exactly what is the likelihood of occurrence of such a condition, and that the likelihood is at least two orders of magnitude less likely to occur than the combination of faulted conditions from each independent control measure. For a control system with significant operating history it may be possible to assess the likelihood of potential common cause software failure occurrence based on a thorough evaluation of operating history data for that system.

For a proposed control system that is relatively new, or one for which there is a lack of documented operating history, there is not likely to be sufficient data to support the estimate of software common cause failure likelihood, since, if a digital control system vendor was aware that such a software faulted condition could occur, he would presumably have developed modifications to that software that would prevent that fault from occurring in the first place. Further, if the control system being proposed has been typically applied in industrial applications for which it is not common practice to carefully document operating history, it may be difficult to ascertain the conditions under which the control system has been in use, which would enable the system designers to better estimate the likely performance of the system in the facility being licensed. Where limited operating history is available on which to base estimates of performance reliability, it may be necessary to apply engineering judgment regarding the design of the system being proposed for use, and its similarity to the designs of systems for which reliability data is known. The reviewer should evaluate the judgments made, and if necessary, request the licensee or license applicant to provide additional supporting information to justify his assumptions and validate his conclusions.

One might argue that in the event of hardware or software failures, each independent control measure digital control system output would revert to its “faulted-state” or “safe-state” condition. In order to make this argument, however, one must have had previous knowledge that for the type of software fault that occurred, there is evidence that 100% of the time the logic outputs all changed to known “faulted conditions” or “safe states.” Since this software fault was previously not made manifest, however, this would be virtually impossible to prove.

To resolve this problem, there are two design attributes that are sufficient to eliminate consideration of the software common cause failure. The first involves use of diversity in design of the independent control functions. The second requires thorough testability of the various fault states for the software installed. The testing option, however, requires that the software be simple enough so that all of the states can be appropriately modeled.

(1) Diversity - Where sufficient diversity exists in the control measures, common cause failures within the independent channels can be considered to be fully addressed without further action.

Example: A control measure in which each safety function is implemented such that one independent function is served by one type of highly reliable digital system and the other uses a diverse highly reliable digital system. A diversity analysis is then performed using the guidance contained in NUREG/CR-6303 to determine that the two diverse digital systems are not subject to a common cause failure mechanism.

(2) Testability - A digital system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses. If it is not possible to test every possible combination of failure states, then identify and test the combinations that are most likely to fail in a manner that could result in an event of high or intermediate consequence.

In assessing the system states, the guidance provided in NQA-1-2008 regarding computer system testing, should be addressed. Computer system qualification testing should be performed with the computer functioning with software and diagnostics representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This testing should be accomplished in addition to the software lifecycle coverage testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance requirements related to safety functions have been met. The software and diagnostics should be representative of the software used in actual operation to a degree that provides assurance that the system states produced by the actual system will be tested during the equipment qualification process.

License application and amendment reviewers should evaluate what constitutes "sufficient diversity" on a case-by-case basis, considering design and process attributes that preclude or limit certain types of common cause failures.

Power Supply Distribution/Common Cause Failure Considerations

One of the most frequently-experienced common cause failures affecting multiple control functions within a control system is the loss of a power source. In addition to a thorough evaluation of the control system design to verify that its power supply distribution has been adequately partitioned such that no single failure of an ultimate power source, an uninterruptible power supply, or an individual rack power supply will result in the loss of a protective function, licensees should be considering other, non-obvious control system responses. Systems are often designed such that when either power or communications with remote servers or other controllers is restored to a controller, a re-initialization of control system parameters will occur to validate programmed values on re-start and to verify that no new commands or instructions were sent to it during the loss of power condition. Recent events have occurred during which the output states of digital controllers changed from their last-known conditions to their fault-condition or safe-states upon re-initialization following power or communications restoration. It is critical that new applications for such control systems have considered the consequences of these start-up re-initialization sequences, and that they appropriately factor in the control system responses in a manner that precludes the possibility of a loss of preventive or mitigation measure.

Common Cause Failures due to Environmental and Physical Conditions

Independence also applies to the appropriate analysis of physical and environmental events which could affect redundant subsystems of IROFS. Controls that are required to be redundant to increase the reliability of the system of IROFS should not be located within the same

environmental envelope or within the same vicinity that they could both potentially be affected by a simultaneous physical hazard event. For example, two redundant controls should not be located such that they can both be flooded by an overhead fire sprinkler that leaks or fails catastrophically. Similarly, redundant controls that require facility heating or cooling to maintain their operating temperature to within manufacturer-specified temperature conditions should not be located within the same HVAC system boundary. Redundant controls should not be located such that they may be exposed to the same excessive electromagnetic interference environment, or could be physically damaged simultaneously by the same potential fork-lift accident.

Evaluation of Vendor-Indentified Digital Control System Failure Alert Notices

Vendors of digital control systems typically applied for use in safety applications make provisions for notifying their customers and stakeholders within the public to apprise them of known failure modes that have occurred through field operating experience (10 CFR Part 21-type notifications.) After in-house testing to model and duplicate the failure mode and validating the conditions under which they can occur, a product alert notice will be published to warn users of these newly discovered fault conditions. In many cases these published product alert notices warn users of failure modes for digital output states that can occur and which were not previously known to occur nor were they planned for in the design. It is imperative that where an applicant is planning for the use of a digital control system of the same design as those for which these product alert notices have been published, that he carefully review them for applicability to his proposed design. Once a system has been implemented in the facility, aspects of the 10 CFR Part 21 program pertaining to the vendor's quality program, the system integrator's quality program, and the facility's own quality program remain in effect well past the "planning for use" stage through to the "retirement" phase.

Implementation of Safety Control Systems

Safety Control Systems or Safety Instrumented Systems are specially-designed systems consisting of sensors, logic solvers, and actuators for the purpose of taking a process to a safe state when predetermined analytical setpoints are exceeded. The logic solvers for such systems are typically certified by third-party certifying organizations to be able to achieve a specific risk reduction value through an analysis of their inherent design features and a thorough analysis of their failure modes and effects. Such certification is provided by the organization in terms of a limited or specific set of boundary or safety design or installation conditions. It is imperative that the user of such logic solvers verify that when implementing such systems within his facility, that the conditions described within the certification statement or "safety manual" for that equipment have been satisfied.

Regulatory Basis

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," including Section 70.4, "Definitions," and Subpart H – "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," including Section 70.60, "Applicability," Section 70.61, "Performance requirements", Section 70.62, "Safety programs and integrated safety analysis," Section 70.64, "Requirements for new facilities or new processes at existing facilities."

Technical Review Guidance

The reviewer should use the information contained in this ISG, as applicable, to evaluate whether a licensee or applicant has described in his application appropriate management measures. Such measures will ensure that digital equipment performing IROFS functions or supporting functions are designed, implemented, and maintained such that they are reasonably protected against common cause failures. This will help to ensure that IROFS are available and reliable to perform their function when needed. Further, the reviewer should make the determination that the application provides reasonable assurance of adequate compliance with the technical requirements of Subpart H of 10 CFR Part 70. In particular, the reviewer should use the information contained in this ISG, as applicable, to evaluate whether a license application or license amendment request demonstrates that digital control and instrumentation systems used as IROFS or systems of IROFS meet the requirements for independence as described herein.

Recommendations

This guidance should be used to supplement the guidance contained in NUREG-1520 with regard to providing management measures to ensure that IROFS or systems of IROFS are available and reliable when called upon to perform their required safety actions.

References

1. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility," NUREG-1520, Final Report, March 2002
2. U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards, Fuel Cycle Facility Interim Staff Guidance Document FCSS-ISG-01, Rev. 0, "Qualitative Criteria for Evaluation of Likelihood," June, 2005
3. U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards, Fuel Cycle Facility Interim Staff Guidance Document, FCSS-ISG-03, Rev. 0, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle," February 17, 2005
4. ANSI/American Nuclear Society Standard 8.1, "Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors." (ANSI/ANS-8.1) September,1998
5. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Interim Staff Guidance DI&C-ISG-02, "Diversity and Defense-in-Depth Issues," January 31, 2008

Digital Communications

Issue

Guidance is needed in reviewing the adequacy of license applications and amendments which concern the protection of digital communications. At fuel cycle facilities, such communications occur among instruments and logic processors that are required to perform integrated safety analysis (ISA)-identified safety functions (i.e., IROFS) and between instrumentation and operator interface stations (workstations).

Introduction

In reviewing a license application, renewal application, or license amendment for a fuel cycle facility, the staff must determine whether there is reasonable assurance that the facility can and will be operated in a manner that will adequately protect the health and safety of workers, the public, and the environment. To carry out this responsibility, the staff evaluates the information that the applicant provides and, through independent assessments, determines whether the applicant has proposed an adequate safety program that is compliant with regulatory requirements. To assist the staff in carrying out this responsibility, a Standard Review Plan clearly states and identifies those standards, criteria, and bases that the staff will use in reaching licensing decisions.

Key design goals stated in 10 CFR Part 70 associated with the use of instrumentation and control systems in fuel cycle facilities pertain to the use of such systems in the prevention and/or mitigation of identified hazards or potential accident sequences. Digital control systems used to mitigate such events are designated as items relied on for safety (IROFS). Licensees are required to implement management measures to ensure that such controls are available and reliable when called upon to perform their intended functions. One management measure which can be applied to assure that such digital IROFS are available and reliable is to provide assurance that such control systems are designed, implemented, and maintained such that they are protected against the effects of potential communications errors which can degrade or prevent the proper performance of the digital safety controls.

The use of digital system technology for use in safety applications requires an appropriate evaluation of the potential for new modes of control system failures, as well as the risks associated with the occurrence of natural phenomena, electromagnetic or other induced environmental phenomena, human error, hardware/software performance issues, or inadvertent challenges due to previously unanalyzed interactions with other plant equipment.

This Interim Staff Guidance (ISG) provides guidance for the review and evaluation of license applications, renewals, or amendments pertaining to fuel cycle facilities. This ISG provides an acceptable approach for demonstrating reasonable assurance that digital systems and networks relied upon to protect the health and safety of the public and to protect the environment, will not become compromised due to potential communications errors that can degrade the safety functions performed by those systems and networks. This guidance specifically addresses issues related to interactions among instruments and processors designated as IROFS and between such processors that communicate with operator work stations and network interface equipment.

Discussion

An IROFS that makes use of digital instrumentation and control systems equipment may consist of a set of equipment that is composed of a sensor, a hard-wired or digital communications path to a "logic solver" (e.g., a programmable logic controller (PLC) or a distributed control system (DCS)), an output driver, and a solenoid valve. In some complex control schemes, it may be necessary for a logic processor to communicate with a second logic processor to complete a system of IROFS needed to protect against an identified postulated event. For example, if the consequence of the event being prevented or mitigated by the control system IROFS is sufficiently high, (indicating that a high degree of risk reduction is required to be performed by the IROFS), one method of implementing a management measure may be to include in the design an independent, redundant IROFS or an independent diverse IROFS (or one that is both redundant and diverse) that independently monitors the process and communicates with an independent logic solver, output driver, and solenoid valve to provide added assurance that the total system performance will be sufficiently reliable for the facility to meet the performance requirements.

Such redundant systems of IROFS may need to communicate to a third logic processor that performs a logic decision to initiate a safety action or may communicate with an annunciator panel or with an operator work station in a control room that is remote from the process. Independence of redundant IROFS improves the reliability of achieving a protective measure. A redundant IROFS is one which is separate (independent) from but performs essentially the same safety function as another IROFS. Redundant IROFS may be either diverse or non-diverse; it is not necessary for them to consist of identical equipment. However, when redundancy is provided by identical equipment or operator actions, it is important to ensure that they are sufficiently independent from one another such that no credible common-cause failures exist that could adversely affect both redundant IROFS.

In modern control systems traditional control panels, with their assorted gauges, indicating lights, control switches, annunciators, etc., are being replaced by computer-driven consolidated operator interfaces, for which:

- The primary means for providing information to the plant operator is by way of computer driven display screens mounted on consoles or on the control room walls.
- The primary means for the operator to command the plant is by way of touch screens, keyboards, pointing devices or other computer-based provisions.

It is anticipated that license applications for new fuel cycle facilities will describe the intent to use such designs, in part because the technology currently offered by control systems vendors make extensive use of this design technology.

The term "channel" or "instrument channel" as used throughout the remainder of this ISG refers to a collection of sensors, transmitters, signal conversion devices, communications paths, logic processors, and human-machine interface devices which function collectively to perform a single sensing and control function. The term "redundant channel" refers to a set of such devices that perform an action that is functionally redundant to the "channel" or "instrument channel" under discussion, so as to provide for an improvement in reliability or a higher likelihood of facility control action being completed upon demand, because it would require a coincident failure of both redundant channels to occur before the intended control action would be rendered inoperable. The term "IROFS channel" refers to those instrument channels that

perform functions that are relied on to accomplish safety actions needed to control the facility such that the performance requirements of 10 CFR 70.61 are continually met.

The term “communications channel” hereinafter refers to the logical pathway needed for process or control data to be transmitted among process sensors, transmitters, signal conversion devices, logic processors, output control devices, and human-machine interface devices, to perform a single process measurement and/or process control function.

A digital workstation is in essence just one device. Unlike a conventional control panel, there is no way for its many functions to be independent of or separated from one another, because they all use the same display screen, processing equipment, operator interface devices, etc. Functions that must be independent must be implemented in independent workstations.

This ISG also describes how the signals from selected controls and indications from local processors with IROFS functional requirements can be combined into a single non-IROFS integrated workstation while maintaining separation, isolation, and independence among redundant IROFS. This ISG does not alter the need for maintaining separate workstations of safety-related controls and displays to support manual execution of safety functions.

Staff Guidance

For independence to be maintained between redundant or diverse IROFS certain key design criteria must be maintained. Among these is the need to prevent the introduction of common communications errors into independent, diverse, or redundant IROFS. Another is the need to assure that the functions served by independent digital systems-based IROFS are not influenced by common errors emanating from non-IROFS instrument channels, which have a lower standard for reliability performance, and therefore are likely to be classified and qualified to lesser quality design requirements.

Interim Staff Guidance pertinent to the review of license applications and amendment requests has been developed to facilitate the review of applications for future fuel cycle facilities and amendments to existing facilities. This ISG covers the following areas:

a) Inter-channel Communications. Whereas fuel cycle facilities typically do not make extensive use of facility shutdown systems composed of multiple redundant safety “channels” similar to that of power reactor facilities, there is nevertheless a need for maintaining independence among systems of IROFS that function together to mitigate or prevent identified hazardous events from propagating such that the safety performance requirements for the facility will not be met. Therefore, guidance has been provided to identify important criteria needed to protect the integrity of independent IROFS channels from potential communications errors.

b) Multichannel Control and Display Stations. Similar to the requirement for communication between independent, diverse, or redundant IROFS equipment, a need exists to protect the IROFS channels that communicate with Operator Interface Stations from any possibility of failure to perform required IROFS functions based on data or commands originating from channels transmitting lesser qualified non-IROFS related information when these channels converge at Operator Interface Stations.

Communications Criteria for Protecting Independence among IROFS

Bidirectional communications between independent processors serving as IROFS and between processors of IROFS functions and non-IROFS functions is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety functions. The review of systems--which includes the review of communications among IROFS processors and/or bidirectional communications between an IROFS processor and non-safety processor--should follow the guidance described in the remainder of this section. Typically, the materials submitted with the application or amendment request will not permit an evaluation of the design criteria described below in sufficient detail to permit verification of their incorporation into the design. However, during in-office and vertical slice reviews, it should be apparent that the criteria described in each point have been addressed by the applicant. A verification review should be performed that includes a review of the system configuration and software specifications. This verification reviwe and may also involve a review of selected software code.

1. A processor of IROFS functions should not be dependent upon any information or resource originating or residing outside its own independent channel to accomplish its safety function. This is a fundamental consequence of a requirement to maintain independent IROFS.
2. The IROFS function of each IROFS processor should be protected from adverse influence from outside the IROFS channel. Information and signals originating outside the channel must not be able to inhibit or delay the safety function. This protection must be implemented within the affected channel (rather than in the sources outside the channel), and must not itself be affected by any condition or information from outside the affected channel. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the IROFS channel.
3. A safety channel should not receive any communication from outside its own safety channel unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different channels may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Receipt of information from outside the channel, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one channel. The applicant should justify the definition of “significantly” used in the demonstration.
4. Commensurate with the degree of risk reduction required, the communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this

exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with quality design standards appropriate to the facility. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.
6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety channel.
7. Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.
8. Data exchanged between redundant safety channels or between safety and non-safety channels should be processed in a manner that does not adversely affect the safety function of the sending channels, the receiving channels, or any other independent channels.
9. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.
10. Safety channel software should be protected from alteration while the safety channel is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one channel at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.

"Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

11. Provisions for inter-channel communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its channel. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.
12. Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures." Examples of credible communication faults include, but are not limited to, the following:
    - Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
    - Messages may be repeated at an incorrect point in time.
    - Messages may be sent in the incorrect sequence.
    - Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
    - Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
    - Messages may be inserted into the communication medium from unexpected or unknown sources.
    - Messages may be sent to the wrong destination, which could treat the message as a valid message.
    - Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
    - Messages may contain data that is outside the expected range.
    - Messages may appear valid, but data may be placed in incorrect locations within the message.
    - Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
    - Message headers or addresses may be corrupted.
13. Communication that are needed to support a safety function, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

14. Communication that is needed to support a safety function should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the channel of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.
15. Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.
16. Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the IROFS channel can cause a safety communication protocol to stall or be flooded, either through deadlock, livelock, or broadcast storm. (Note: This is also considered a requirement of Independence. Although not a design requirement for fuel cycle facilities, IEEE 603-1991 “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” provides design criteria for assuring separation between control and safety functions and independence among redundant safety related instruments.) (Reference 4: NUREG/CR-6082, Section 3.4.3)
17. Pursuant to the requirement for maintaining availability and reliability of IROFS, the medium used in a safety communications channel should be qualified for the anticipated normal and post-event environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems will likely need susceptibility testing for Electromagnetic Interference and Radio Frequency Interference (EMI/RFI) and power surges and emissions testing to assure Electromagnetic Compatibility (EMC) with other devices in a highly integrated control room environment.
18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.
19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.
20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

Communications Criteria for Protecting IROFS Channels at the Operator Interface Panel

This section presents guidance concerning operator workstations used for the control of plant equipment in more than one safety channel and for display of information from sources in more than one safety channel. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety channel as the workstation.

Multichannel control and display stations addressed in this guidance may themselves be safety-related or not safety-related, and they may include controls and displays for equipment in multiple safety channels and for equipment that is not safety-related, provided they meet the conditions identified herein. Even though the use of multichannel control and display stations is relatively new to the nuclear industry, the concepts to maintain the plant safety contained in this guidance is in line with current NRC regulations.

NOTE: As used in connection with control and display stations, "control" refers to control provisions available to the plant operator by way of those stations. Such controls provide the plant operator with means to, for example, instruct the control system to open or close a particular valve. Control of safety-related plant devices (in the sense of the process of generating and transmitting safety-related control signals) must be accomplished by means of safety-related control equipment in the same safety channel or train as that of the plant equipment it is controlling. In some cases, a command originating from a control and display station outside the channel may be superseded by a higher-priority command. The manner of combining the commands from control stations outside a safety channel with the safety commands originating within the channel is addressed below. This guidance explicitly DOES NOT endorse the exclusive or direct control of safety related plant equipment by means of provisions outside the equipment's own safety channel.

Independence and Isolation

The following discussion is applicable to multichannel control and display stations. This guidance does not apply to conventional hardwired control and indicating devices (hand switches, indicating lamps, analog indicators, etc.).

1. Non-safety workstations receiving information from one or more safety channels: All communications with safety-related equipment should conform to the guidelines for inter-channel communications.
2. Safety-related stations receiving information from other channels (safety or non-safety): All communications with equipment outside the workstation safety channel, where applicable, whether that equipment is safety-related or not, should conform to the guidelines for inter-channel communications. Note that the guidelines for inter-channel communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.
3. Non-safety stations controlling the operation of safety-related equipment: Non-safety workstations may control (see note above) the operation of safety-related equipment, provided the following restrictions are enforced:

   A non-safety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the non-safety equipment. Further,
   - The non-safety station should be able to bypass a safety function only when the affected channel has itself determined that such action would be acceptable.
   - The non-safety station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety channel. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety channel is not acceptable because there would be no protection from inappropriate or accidental reset.)

- The non-safety station should not be able to bring a safety function out of bypass condition unless the affected channel has itself determined that such action would be acceptable.

4. Safety-related stations controlling the operation of equipment in other safety-related channels:

   - Safety-related stations controlling (see note above) the operation of equipment in other channels are subject to constraints similar to those described above for non-safety stations that control the operation of safety-related equipment.
   - A station must not influence the operation of safety-related equipment outside its own channel when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the channel of which those controls are a member. In addition:
     - The extra-channel (that is, "outside the channel") control station should be able to bypass a safety function only when the affected channel itself determined that such action would be acceptable.
     - The extra-channel station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety channel. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety channel is not acceptable because there would be no protection from inappropriate or accidental reset.)
     - The extra-channel station should not be able to bring a safety function out of bypass condition unless the affected channel has itself determined that such action would be acceptable.

5. Malfunctions and Spurious Actuations: The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, include but are not limited to the following:
   - Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multichannel control and display station.
   - Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.
   - Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.
   - No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should

be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond “do you want to proceed?” The operator should then be required to respond “Yes” or “No” to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.

- Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks.
- Multichannel control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the workstation is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. Diversity and Defense-in-Depth (D3) considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein.
- Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.
- The design should have provision for an “operator workstation disable” switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.
- Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, or in other unanticipated abnormal plant conditions.

Human Factors Considerations

Plant equipment required to prevent or mitigate identified hazards should have safety-related controls designated as IROFS, and, if operators are required by the analysis to perform safety actions, they must be furnished with displays designated as IROFS. For any safety-related equipment not having safety-related controls and displays, an applicant or licensee should demonstrate that safety-related controls and displays are not needed. The staff’s review in this regard should take into account the above discussion, and any applicable regulatory requirements.

Safety-related controls and displays may be provided via operator workstations, or they may be provided via hardwired devices such as switches, relays, indicators, and analog signal processing circuits. In either case, the safety-related controls and indications must consist of safety-related devices with safety-related software and must be dedicated to specific safety channels. Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems. Therefore equipment that is NOT classified as part of a safety system must NOT be used in support of safety functions. Therefore multichannel control and display stations must not be used to perform functions needed to support plant safety. The control of functions credited with the protection of the plant in the plant safety analyses must be performed utilizing safety-related resources.

The need for a plant operator to use alternative controls and displays under upset or accident conditions could pose Human Factors concerns, since the need to use less-familiar controls or displays would coincide with the need for maximum effectiveness and timeliness in operator actions. Such an approach could also result in confusion if the non-safety displays, as a result of lack of qualification and of lesser quality standards, present obsolete or erroneous information to the plant operator but fail to advise the operator of these potential inaccuracies. In addition, the presence on the non-safety workstations of controls and displays that are associated with safety functions could lead an operator to erroneously select those non-safety controls and displays, rather than the safety-related ones, when the safety functions are required.

An applicant would need to demonstrate that Human Factors considerations, including the foregoing considerations and also including consideration of operator response time and situation awareness, are consistent with the system design bases, operating procedures, and event sequence analyses and are both reasonable and adequate.

There are many other Human Factors considerations applicable to the design of operator workstations, whether multichannel or not. Such considerations are not addressed in this ISG, but are similar to those discussed in guidance for the design of power reactors, which may be found in Digital I&C ISG-05, “Highly Integrated Control Rooms—Human Factors Issues.”

Diversity and Defense-in-Depth (D3) Considerations

D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety-related. The guidance provided herein is not dependent upon such details. D3 considerations may also impose qualification or other measures or guidelines upon equipment addressed in this ISG. Refer to DI&C-ISG-02 for such guidance.

Regulatory Basis

10 CFR Part 70, “Domestic Licensing of Special Nuclear Material,” including Section 70.4, “Definitions,” and Subpart H – “Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material,” including Section 70.60, “Applicability,” Section 70.61, “Performance requirements”, Section 70.62, “Safety programs and integrated safety analysis,” Section 70.64, “Requirements for new facilities or new processes at existing facilities.”

Technical Review Guidance

The reviewer should use the information contained in this ISG, as applicable, to evaluate whether a license application or license amendment request demonstrates that digital control and instrumentation systems used as IROFS or systems of IROFS are sufficiently independent, as discussed herein. The reviewer should be satisfied that these digital control and instrumentation systems will not become degraded or rendered inoperable due to inadequate design, as this would have the potential to introduce digital communications errors. License reviewers should evaluate the materials provided in the application and make a determination whether it provides reasonable assurance of adequate safety, or reasonable assurance of adequate compliance with the technical requirements of Subpart H of 10 CFR Part 70.

Recommendations

This guidance should be used to supplement the guidance contained in NUREG-1520 with regard to providing management measures to ensure that IROFS or systems of IROFS are available and reliable when called upon to perform their required safety actions.

References

1. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility," NUREG-1520, Final Report, March 2002
2. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Interim Staff Guidance DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)," Revision 1 January, 2009
3. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Interim Staff Guidance DI&C-ISG-02, "Diversity and Defense-in-Depth Issues," January 31, 2008
4. U.S. Nuclear Regulatory Commission, NUREG/CR-6082, "Digital Communications," prepared by G. G. Preckshot, Lawrence Livermore National Laboratory, August 1993
5. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Interim Staff Guidance DI&C-ISG-05, "Highly-Integrated Control Rooms – Human Factors Issues," Revision 1, November 3, 2008

Software Quality

Issue

The occurrence of potential common cause software failures in fuel cycle facilities needs to be minimized. This guidance section pertains to reviewing the adequacy of license applications and amendments describing how high quality software design methods are used in digital I&C applications to help prevent software failures.

Introduction

In reviewing a license application, renewal application, or license amendment request for a fuel cycle facility, the staff must determine whether there is reasonable assurance that the facility can and will be operated in a manner that will adequately protect the health and safety of workers, the public, and the environment. To carry out this responsibility, the staff evaluates the information that the applicant provides and, through independent assessments, determines whether the applicant has proposed an adequate safety program that is compliant with regulatory requirements. To assist the staff in carrying out this responsibility, a Standard Review Plan clearly states and identifies those standards, criteria, and bases that the staff will use in reaching licensing decisions.

Key design goals stated in 10 CFR Part 70 associated with the use of instrumentation and control systems in fuel cycle facilities pertain to the use of such systems in the prevention and/or mitigation of identified hazards or potential accident sequences. Digital control systems used to mitigate such events are designated as items relied on for safety (IROFS). Licensees are required to implement management measures to ensure that such controls are available and reliable when called upon to perform their intended functions. One management measure which can be applied to assure that such digital IROFS are available and reliable is to provide assurance that such control systems are designed, implemented, and maintained such that they are protected against the potential effects of common cause software failures. This Interim Staff Guidance (ISG) provides review criteria for evaluating management measures that address acceptable means of achieving high quality software in digital I&C applications used for safety functions in fuel cycle facilities to assist in limiting the occurrence of potential common cause software failures. Title 10 of the Code of Federal Regulations (CFR) section 70.64 a (1) requires that “the design must be developed and implemented in accordance with management measures, to provide adequate assurance that items relied on for safety will be available and reliable to perform their function when needed” and that “Appropriate records of these items must be maintained by or under the control of the licensee through out the life of the facility.”

Management measures are defined as “the functions performed by the licensee, generally on a continuing basis that are applied to items relied on for safety (IROFS), to ensure the items are available and reliable to perform their functions when needed. The phrase “available and reliable,” as used in 10 CFR Part 70, means that, based on the analyzed, credible conditions in the ISA, IROFS will perform their intended safety function when needed to prevent accidents or mitigate the consequences of accidents to an acceptable level. Management measures will be implemented to provide reasonable assurance of compliance with the performance requirements, considering factors such as necessary maintenance, operating limits, common-cause failures, and the likelihood and consequences of failure or degradation of the IROFS and the measures. Management measures include configuration management, maintenance,

training and qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements." (Reference: 10 CFR 70.4)

The identification and selection of appropriate management measures may use a risk-informed process to ensure that the applications of controls in areas with the highest degree of potential risk to the health and safety of the public, or potential harm to the environment or to facility workers, offers adequate protection. When identifying the appropriate controls needed to mitigate or prevent identified hazards for the facility, 10 CFR 70.62(d) states that the management measures applied to a particular engineered control or control system may be graded, commensurate with the reduction of risk attributable to that control system. Thus, it is recognized that certain high risk applications may indicate the need for rigorous means of applying quality measures to achieve and maintain a high quality control system, while relatively low risk applications may employ less rigorous management measures.

Discussion

One of the most important results obtained from the performance of an Integrated Safety Analysis (ISA) is the identification of the controls needed to ensure the safe operation of the facility. These items relied on for safety (IROFS) are defined as structures, systems, equipment, components, and activities of personnel that are relied on to prevent potential accidents. The ISA process by itself cannot ensure the effective design and implementation of the controls and their proper operation. Instead, other elements of the licensee's safety program are relied on to provide this assurance. For example, as part of the measures used to ensure criticality safety, radiological safety, chemical safety, and fire safety, design criteria for relevant safety controls are established. (For example, one such design criterion applicable to the design of an active engineered safety control is to utilize two redundant and independent controls to accomplish key safety functions in order to achieve a high degree of reliability.) The design of the controls identified in the ISA Summary should then adhere to these criteria. Management measures should be applied to ensure that the safety controls implemented satisfy the design criteria. The application of such management measures may be graded in a manner that is commensurate with the required degree of overall risk reduction needed for the application being controlled, such that the highest risk reduction applications have the highest or most stringent management measures applied to assure the reliability and availability of controls. Applications for a license to possess and use special nuclear material in a plutonium processing and fuel fabrication plant are required to contain a description of the quality assurance program to be applied to the design of the facility, including a discussion of how the criteria of 10 CFR 50 Appendix B will be met. However for other Part 70 facilities, there are no special requirements pertaining to specific criteria that must be contained within quality programs. License applicants may propose to apply quality elements such that management measures are applied in a graded manner commensurate with the reduction of risk attributable to a particular control or control system.

High-Quality Software Design When a licensee or applicant selects the controls needed to protect against the occurrence of a particular event sequence, both the number and the effectiveness of such controls should be taken into account. For active engineered controls, the effectiveness of such controls may be demonstrated by selecting for use in achieving the required safety functions those components and systems which have been developed through processes that adhere to appropriate design criteria, and which are subsequently maintained, calibrated, and functionally tested to provide additional assurance that the controls are in place and are continually maintained in working order. However, once a software-driven safety system has been implemented, there is little in the way of software programming maintenance

that can be performed to make sure that the software will continue to function properly. Therefore, it is critical that the software for such control systems be **initially** of a very high quality in order to provide assurance that it will meet the facility performance requirements. A potential software functional design error or software programming error could result in a common-mode or common-cause failure of a redundant or "independent" set of control equipment, which could then be rendered inoperable due to this failure, thereby preventing the facility from meeting the performance requirements.

Graded Approach to Implementation of Management Measures Depending on the level of risk posed by the hazards to be mitigated for the facility as indicated in the results of the ISA Summary, a range of management measures may be applied governing the design and development of digital control hardware and software systems that are commensurate with the likelihood of occurrence and severity of consequences of the hazards identified in the Integrated Safety Analysis. Controls designed to mitigate high likelihood and high consequence events require high levels of quality design processes to assure that the control system will continually be available and reliable to achieve the safety functions required to mitigate or prevent those hazards. Such quality design processes should provide assurance that the controls cannot be compromised by a failure occurring within the control system itself, as well as failures that can occur external to the control system that could compromise the ability of the control system to achieve its required functional performance. Further, engineered controls designed to prevent hazards that are significant enough to warrant the use of functionally independent and redundant controls to achieve the required safety function should be designed such that they cannot be compromised by the occurrence of a possible failure originating within the control system that could be common to both sets of redundant controls, thereby rendering the active engineered control inoperable (i.e., a common cause failure.)

Depending on the level of risk to public health and safety associated with the worst-case identified hazard to be prevented or mitigated by the safety control system for the facility in order to meet its performance requirements, the facility may elect to implement one or more of several possible approaches to achieving an initial high-quality software design which provide varying degrees of assurance that the initial safety control system software will have a low likelihood of potential common-cause failures. The reviewer should evaluate the application to determine whether the applicant's proposed method for addressing and achieving adequate initial high-quality software represents a reasonable assurance of adequate safety for the facility, taking into account the potential level of risk reduction needed to mitigate or prevent the hazards identified in the facility ISA Summary to meet the performance requirements.

Possible approaches to achieve a high quality software design are described below. As discussed above, plutonium processing and fuel fabrication facilities are required to include in their applications a description of the Quality Assurance Program to be applied to the design of the facility, including a discussion of how the criteria of 10 CFR 50 Appendix B will be met. For Part 70 facilities other than these, formal Quality Assurance programs are not required. However, management measures are to be applied to items relied on for safety to ensure that the items are available and reliable to perform their functions when needed. Management measures include configuration management, maintenance, training, procedures, audits and assessments, and other quality assurance elements. License applicants may propose to apply quality elements such that management measures are applied in a graded manner commensurate with the reduction of risk attributable to a particular control or control system.

Possible Approaches to Achieve High-Quality Software for Safety Applications at Fuel Cycle Facilities

The four items below are listed in order of application for the highest level of risk reduction needed to that of the lowest risk reduction needed.

1. Nuclear Power Reactor (10 CFR Part 50) Appendix B Quality Assurance Software Lifecycle Development Process, following Regulatory Guide 1.152, Revision 2 "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," and US NRC Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants". Regulatory Guide 1.173 endorses the use of IEEE Standard 1074, "IEEE Standard for Developing Software Life Cycle Processes." Although the implementation of software development programs and processes that adhere to the requirements, recommendations, and guidance contained within these documents does not guarantee software that is free from potential common mode failures, compliance does ensure that practices, based on past experience and representing industry consensus on approaches for development of software for digital safety systems, will be incorporated into the development process to achieve a very high level of software quality.

2. Commercial Grade Dedication Process for Commercial Off-the-Shelf (COTS) Systems: EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" was prepared to address the need for installing digital upgrades in safety applications for nuclear facilities. This report melds together the requirements from other EPRI, IEEE, and NRC design standards and guidance for licensing digital upgrades and defining criteria for digital computers in reactor safety applications. Through the selection and use of high-quality commercial grade equipment originally developed for safety applications in non-nuclear facilities or for applications where successful mission completion needed to be assured to a high degree, work already performed in other industries to achieve high quality processes can be leveraged to make up for a dwindling supplier base and increased development costs for such software because it is spread out over a smaller market. It should be noted that this process does not actually add quality, but seeks to confirm that the commercial product already has adequate quality. Key components of this process are described in more detail below.

3. Use of Criteria and Processes Developed for Safety Instrumented Systems: ANSI/ISA Standard 84.00.01, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Hardware and Software Requirements" was developed in tandem with International Electrotechnical Commission Standard IEC-61511-1 (same name) to address the need for high quality controls and a consistency among design techniques used for development of safety controls for the Process Industries. The standard provides an approach for safety life cycle activities to achieve a required level of risk reduction identified through a formal hazards analysis process for a process facility. The standard defines three types of software development languages in use for process control systems in process industries: fixed program languages, limited variability languages, and full variability languages. The standard recognizes and primarily addresses software developed using fixed programming languages and limited variability languages, which are most commonly used in the application of safety control systems for process industries, and it focuses on attaining a level of software quality applicable for any type of safety application up to a Safety Integrity Level (SIL) of SIL 3.

The standard identifies methods, tools, and techniques for developing safety system software to achieve high assurance of high quality. The process steps are represented at a high level in the figure in Appendix A to this ISG. This ANSI/ISA standard also states that full variability languages should comply with IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety Systems-Part 3, Software Requirements."

4. Third-Party Certification Processes, Evaluations of Well-Documented Operating History, and other methods. Although these processes are less deterministic than the others described above, in certain instances there may be valid reasons for concluding that the degree of assurance of high quality afforded by these processes may be acceptable for low risk applications within fuel cycle facilities. In the discussion that follows, certain precautions are described for the review of license applications that make sole use of processes such as these.

The availability and reliability of digital I&C-based IROFS is largely dependent on the management measures that have been applied to assure that the software performing safety functions has been "designed, implemented, and maintained" using a high quality development process. However, within 10 CFR Part 70 there are no specific requirements for conducting processes that provide a high degree of assurance of software quality. The design evaluation processes described above that have been recognized by the NRC staff, as well as similar processes that are utilized by other industries in facilities that handle hazardous chemicals or petrochemical processes, can provide various degrees of assurance of high software reliability.

NRC Staff Review Criteria for Evaluating the Software Lifecycle Design Process For the level of risk applicable to the use of digital control systems in safety applications for power reactors, the NRC staff has determined that a high level of assurance can be achieved for the design of software required to accomplish safety functions through a rigorous, high-quality software development process. Regulatory Guide 1.152, Revision 2 "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," identifies IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" as a standard that specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations." This process described in IEEE Std 7-4.3.2 provides a means for incorporating quality design processes that have the potential for severely limiting the development of undetected common mode software problems. To achieve a high quality level in the software used in safety systems the complete lifecycle must be monitored and carefully controlled from its conceptual design through its ultimate retirement. Some standards, such as ANSI/ASME NQA–1-2008, "*Quality Assurance Requirements for Nuclear Facility Applications*" and IEEE Standard 1074-2006, "*IEEE Standard for Developing a Software Project Life Cycle Process,"* (although not required to be applied in 10 CFR Part 70) describe the software lifecycle as "the period of time that starts when a software product is conceived and ends when the software product is no longer available for routine use." The software life cycle typically consists of the following phases:

- Conceptual Design
- Requirements Specification
- Functional Design
- Detailed Implementation
- Testing
- Installation, Checkout, and Acceptance Testing

- Operations
- Maintenance
- Retirement

(Details describing the elements considered within each phase can be found in ANSI/ASME NQA-1-2008, Subpart 2.7 and IEEE-1074-2006.)

One means of assuring that such quality measures are applied is to verify that the software meets its intended functional requirements, and to validate it using appropriate standards of comparison or models known to have correct responses. Although there are no specific standards identified within Part 70 that define requirements for such a process, appropriate verification and validation processes for software codes are described in Subpart 2.7 of ASME NQA-1-2008 and supporting materials. Whichever methods are used, the licensee should provide a description of the methodology or process utilized to develop and program safety related software in a manner that provides a reasonable assurance that digital control systems performing safety related functions would reliably and satisfactorily perform these functions when required. Although not required per 10 CFR Part 70, one such method that would be acceptable to the NRC staff would be to implement the requirements of NQA-1-2008, Subpart 2.7 as they apply to computer software used to produce or manipulate data, which is used directly in the design, analysis, and operation of structures, systems, and components.

Alternative Means for Demonstrating Control System Software Design Quality Other means of verifying that the software will meet its intended functional requirements are permitted, provided that these means meet certain acceptance criteria. One criterion is that the verification process should include a formal evaluation of well-documented, significant, incontrovertible evidence of successful software development and operating history of identical versions and types of application logic and operating system software in similar applications of safety controls for facilities as the ones proposed. Another criterion is that the verification process should include an evaluation of how the control system responds to likely scenarios of potential failure modes for the digital controls based on the use of the software proposed. The documentation of operating history should be for facilities with equivalent or greater degrees of risk to the health and safety of the public as the facility or upgrade to a facility whose license is being reviewed. In determining whether such other means are adequate to assure the required protection for the facility, critical characteristics of the software development/design, evaluation, and testing process should be addressed. Such characteristics should include factors such as whether the proposed software was developed using a high-quality design process; whether significant testing and verification of the software and its integration with the platform being proposed has been well-documented; whether the testing process identified requirements for further software and/or hardware and software integration improvements and whether those improvements have been successfully tested, and what additional measures have been proposed by the applicant to assure that the proposed software will reliably perform its intended functions to allow the facility to meet the performance requirements. Examples of such additional measures include the use of third-party certifications of the ability of the integrated control systems to reliably perform safety functions using acceptance criteria for safety performance in accordance with industry standards for safety instrumented systems that have been deemed adequate for the applications being considered in the license application; as well as testing of the installed hardware and software system in an off-line manner prior to start-up to verify the response of the system to likely failure scenarios. In addition, management measures should include the performance of stimulus-to-response tests of the system, and simulation of failure modes deemed most likely to occur as common mode software failures to assure that the anticipated response to these simulated failures do not prevent the safety objectives from being achieved.

Use of Commercial Off-the-Shelf Applications Where an applicant for a new or amended license has proposed the use of a commercial-off-the-shelf (COTS) control system to accomplish a safety function, a distinction needs to be made between the responsibilities of the dedication organization who applies the product to a specific safety related application versus the designer of that item. For issues involving the use of COTS, and more generally, the design of software used in digital I&C-based systems at Part 70 facilities, NRC Reviewers need to be familiar with various terms defined in 10 CFR Part 21, "Reporting of Defects and Noncompliance." The relevant 10 CFR part 21 defined terms are discussed below.

For Part 70 facilities, a "basic component" is a structure, system or component, or part thereof, used in designing the facility, that (1) affects a safety function and is directly procured by the licensee; and (2) is one in which a defect or failure to comply with any applicable regulation, NRC order, or NRC license could create a substantial safety hazard.

A "commercial grade item" is an item that is: a) not subject to design or specification requirements that are unique to Part 70 facilities or activities; b) used in applications other than Part 70 facilities or activities; and c) ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description or catalog.

"Dedication" is an acceptance process undertaken to demonstrate reasonable assurance that a commercial grade item to be used as a "basic component" will perform its intended safety function. As applied to Part 70 facilities, "dedication" occurs after receipt when the "commercial grade item" is designated for use as a "basic component."

Commercial-grade dedication for a generic class of service cannot absolve the application designer of the responsibility for making a safety case for specific applications of the dedicated COTS item. In this respect, COTS software is no different than a dedicated commercial-grade hardware item, such as a relay; the product received must still be shown to be the product specified, and the design using the item or the method of application must still be shown to be correct and consistent with the terms of the dedication under design control and quality assurance measures required by 10 CFR Part 70. Industry guidance, such as that contained in EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" provides an acceptable means of achieving this confidence. Further, NQA-1-2008 Part II, Subpart 2.7, Section 302 provides additional relevant discussion pertaining to acquired software that was not developed using industry standard processes pertinent to the application for which it is being proposed. For such software evaluation it is required to demonstrate that the limitations and capabilities of the software intended for use are tested and bounded. That is, the conditions under which the software will be used are not outside the bounds of that which has been previously proven in use, or which has been evaluated and found to provide adequate assurance of high quality as part of a commercial grade dedication process or qualified third-party certification process.

Software prepared for use in safety applications at fuel cycle facilities should use quality processes throughout its design lifecycle. The NRC staff has found that one means of applying such quality processes is to implement the discussion in Subpart 2.7 of ANSI/ASME NQA-1-2008, "*Quality Assurance Requirements for Nuclear Facility Applications*," pertinent to software quality. Where commercial grade equipment is being used for safety applications, that equipment should be of a high quality, and the commercial dedication process for digital I&C equipment as described in EPRI TR-106439 should be followed. That process requires the implementation of specific technical and management measures to provide additional assurance that the software processes are of sufficient high quality to be relied upon when

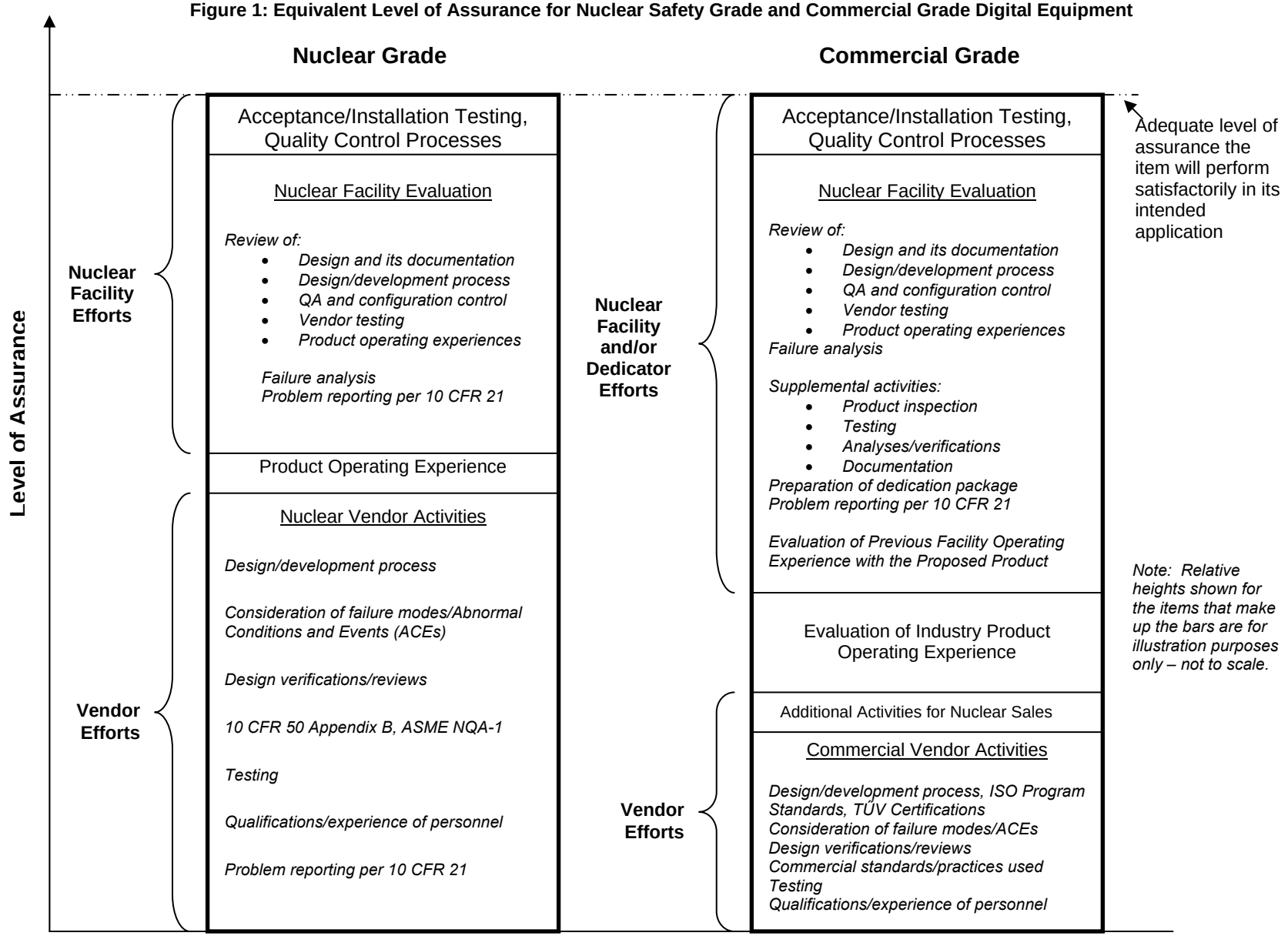
called upon to perform safety actions. Chapter 7 of NUREG-0800, the Standard Review Plan for the review of license applications for power reactors contains guidance on the review of the use of computer-based control systems that have been procured and implemented for use through a commercial dedication process. Such guidance may be utilized for the review of license applications for fuel cycle facilities as well, recognizing however that other approaches to high quality software design may also be appropriate.

To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system analysis software. Elements of the process may be tailored to be commensurate with the safety significance of the control measure being applied.

The fundamental function of software quality guidance is to demonstrate that the facility and equipment, the operating procedures, the processes to be performed, and other technical requirements provide reasonable assurance that the applicant/licensee will comply with the regulations of 10 CFR Chapter 1, and that public health and safety will be protected. The license application or license amendment request should describe the quality assurance measures that have been applied to the applicable life-cycle activities. Information should be available to the reviewer for inspection during the course of his review of the license application or amendment that describes the system requirements and demonstrates how the design of the system is intended to meet these requirements. System implementation should focus on component and system requirements, design outputs, verification, validation, and equipment qualification, based on type testing. Facility systems making use of digital components to perform safety actions, should provide additional focus on demonstration that the life cycle activities for the platform and for the application or configuration were disciplined and documented, applying a set of high quality life cycle processes. Further, the digital safety system software development process should also address potential security vulnerabilities in each phase of the digital safety software system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Figure 1 (next page) compares the general elements needed to achieve an equivalent level of assurance for a safety grade system that has been designed and developed specifically to meet “nuclear safety grade” requirements and one which has been developed for use as high-quality, commercial grade equipment. When applying or dedicating commercial grade equipment for use in safety applications, in addition to evaluating the historical operating experience of the components under consideration, licensees should evaluate the quality controls and design processes utilized by the control system vendor to develop the software used to perform the logic operations and supervisory diagnostics needed to accomplish required safety functions and monitor the status of system operability. In the area of software development, this includes a review of the vendor’s design and documentation processes, configuration management process, corrective action process, and other elements of quality design. The effort put into this evaluation should be commensurate with the level of safety significance required by the facility application.

Figure 1: Equivalent Level of Assurance for Nuclear Safety Grade and Commercial Grade Digital Equipment



Staff Guidance

Reviewers should evaluate license applications and license amendments for evidence that the licensee has successfully conducted and completed efforts to provide reasonable assurance of the adequacy of design, implementation, and maintenance programs for IROFS identified in the ISA Summary, to ensure that they are available and reliable to perform their function when needed. Further, the reviewer should make the determination that the application provides reasonable assurance of adequate compliance with the technical requirements of Subpart H of 10 CFR Part 70. In particular, reviewers should evaluate evidence provided by the licensee that digital equipment used to accomplish safety functions has been evaluated against appropriate requirements for availability and reliability, including the design of the system architecture and the software incorporated into it. Such characteristics cannot be assessed through a process of inspection and testing alone, but rather it is necessary to understand how the control system vendor or systems integrator has configured the design, performed the software design process, documented this process, and identified any vulnerabilities of the system to faults and failures, especially those defining how the system might respond in the presence of a fault or failure of the software which has the potential of acting as a common-cause failure to redundant or potentially "independent" IROFS, or the failure of a sole IROFS. A goal of the review is to identify and credit, where applicable, all evidence that the licensee has achieved a highly reliable and available design. License applications or license amendments submitted for review that describe the use of digital control systems in process or utility applications as Items Relied on for Safety (IROFS) should demonstrate reasonable assurance that the performance requirements of 10 CFR 70.61 will be met for the facility. The management measures and acceptance processes providing the required assurance should be selected and applied based on the level of risk to the health and safety of the public (and facility workers) and to the environment applicable to the facility functions to be achieved by the digital control system.

As stated in the "Introduction" section at the beginning of this Interim Staff Guidance document, an ISA Summary must include, pursuant to 10 CFR 70.65 (b) (4) a description of the management measures. An ISA Summary must also identify, pursuant to 10 CFR 70.65 (b) (8), all IROFS that are the sole item mitigating or preventing an accident sequence for which the consequences could exceed the 10 CFR 70.61 performance requirements. For evidence that high-quality processes have been applied in the design of such IROFS, the reviewer should ascertain how the licensee has assessed the overall quality and reliability of the software and its integration with the hardware that is inherent in design of the IROFS with respect to the risk mitigation or prevention level required for the application requirements. For example, the license application should address quality controls utilized in the acceptance process for the selection of the design, including:

- An evaluation of the operating experience history for the hardware and software in relevant applications
- An evaluation of the design of the hardware and software, including an analysis of the documentation of the design, the programming code, test procedures utilized and test results experienced by the designers
- An evaluation of any identified system design or performance vulnerabilities
- An evaluation of the processes, procedures, and practices used in the development review, testing, and maintenance of the hardware and software
- An evaluation of the qualifications and similar project experiences of the personnel responsible for the design, testing, and development of the hardware and software

To be effective, such evaluations should have identified whether the licensee or applicant has defined objective acceptance criteria for specific digital system requirements related to reliability and availability. In lieu of such objective criteria being identified by the licensee or applicant, the licensee or applicant may have taken credit within his evaluation that adequate documentation is available to demonstrate that such reviews have been conducted and successfully completed by qualified third-party certifying organizations. When reviews by such organizations are referenced, however, a demonstration should be made by the applicant that the third party review was conducted for the specific equipment model and type proposed for use in the applicant's facility and that the software version tested or evaluated is identical to the one proposed. In addition, any bounding parameters or certification conditional statements made by the certifying organization should be evaluated, found to be applicable for the intended design, or accommodated in the applicant's final design.

When evaluating how licensees have addressed the application of engineered control systems software, there should be evidence that the licensee has applied appropriate quality controls during the conceptual design stage and the functional/safety requirements specifications stage for the facility's safety control systems, as well as for the installation, checkout, acceptance testing, operations, and maintenance of the control system, once it has been delivered. In addition, there should be evidence that the licensee has considered, and found to be adequate, vendor quality controls for the following key software lifecycle activities for the vendor and/or systems integrator scope of work: conceptual design; functional and safety requirements specifications; detailed design and implementation; software unit testing, validation and verification processes, software configuration management processes, documentation adequacy, and factory testing; installation, checkout, and acceptance testing; operational considerations; and maintenance requirements.

As a minimum, a set of characteristics associated with key phases of the software lifecycle activities should be evaluated, and should include the following:

Software Requirements Specifications: For each IROFS implemented via a digital component or system, the ISA should provide the definitive requirements for the specific safety functional performance required to be implemented by the hardware and software. If needed for clarity, software safety plans and software design requirements specifications should be prepared in sufficient detail to identify the performance requirements for each IROFS for each mode of operation (e.g., standby, normal operations, initial start-up/re-boot, etc.) required. Requirements specifying the use of pre-developed software and systems (e.g., reuse software and commercial off-the-shelf systems) should address the vulnerability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

Software Design: The software design should demonstrate that the requirements set forth in the ISA are met, and that the most likely failure modes and effects are evaluated, fail-safe design practices are implemented, and independence among IROFS for meeting the single failure or double contingency requirements has been achieved. In addition, the design should demonstrate that the digital safety system development process addresses potential security vulnerabilities in each phase of the digital safety system lifecycle. The development process should include considerations of software security to ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications. COTS systems are likely to be proprietary and generally unavailable for review. It is likely that there is no reliable method to determine security vulnerabilities for Operating

systems (for example, Microsoft and other operating system suppliers do not provide access to the source code for operating systems and callable code libraries). In such cases, unless such systems are modified by the application developer, the security effort should be limited to ensuring that the features within the system do not compromise the security requirements of the system, and the security functions should not be compromised by the other system functions.

Installation: The licensee should have demonstrated that the software installed meets the requirements of the design by testing the most likely failure modes and demonstrating that the IROFS is functional by performing a stimulus-to-response test that simulates, as closely as possible, the actual conditions and configuration that will be experienced once the control system starts actual operations in the facility. In addition, it should be verified that the software will allow the system to respond to the process requirements with a response time that is in conformance with the ISA hazard mitigation or prevention requirements.

Operations and Maintenance: The licensee should demonstrate that a program is in place to perform periodic surveillances and/or preventive maintenance that demonstrates that the hardware and software is performing properly, with a periodicity consistent with that which has been identified as required by the ISA analysis. In addition, a program for performing timely corrective maintenance, when needed, is in place.

Generic Guidance for Review of Software Quality in Applications for Safety Systems relying on the use of Digital Control Systems

The following standards should be used to assist the reviewer in evaluating whether the applicant has addressed appropriate criteria such that the proposed design will achieve a high quality assurance for a software program, regardless of whether it is using application-specific or COTS software.

IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," provides an overview of which specific standards should be considered when implementing an efficient V&V program.

When reviewing the methodology used in the validation and verification of software the staff should:

- Identify the safety function the software must perform;
- Identify the characteristics the software must possess in order to accomplish the safety functions;
- Verify that the characteristics are implemented in an acceptable manner.

IEEE 1012-2004, "IEEE Standard for Software Verification and Validation," defines the concept of validation and verification (V&V) and could be used as a supporting document to provide a reviewer with background information on the V&V process. This standard establishes a common framework for V&V processes, activities, and tasks in support of all software lifecycle process, (i.e., acquisition, supply, development, operation, and maintenance processes). This also defines the V&V tasks, required inputs and outputs; and the content of a software V&V plan. V&V processes provide an objective assessment of software products and processes throughout the software lifecycle. Annex C of IEEE 1012 also provides a framework for applying software quality measures using a graded approach, commensurate with the degree of importance to safety, via application of "Software Integrity Levels" or SILs.

IEEE 1074-2006 "IEEE Standard for Developing a Software Project Life Cycle Process," provides a generic approach to develop processes for safety system software.

IEEE 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," describes a method of acceptable means to achieving high functional reliability and design quality in software used in safety systems. The software requirements specification is an essential part of the record of the design of safety system software. Software requirements specification should exhibit characteristics, such as correctness and completeness that will facilitate the implementation of a carefully planned and controlled software development process.

IEEE 829-1998, "IEEE Standard for Software Test Documentation," defines software test documentation and specifies its form and content.

IEEE 1008-1987 "IEEE Standard for Software Unit Testing," provides *"an integrated approach to systematic and documented unit testing. The approach uses unit design and unit implementation information, in addition to unit requirements, to determine the completeness of the testing. This standard describes a testing process composed of a hierarchy of phases, activities, and tasks and defines a minimum set of tasks for each activity. Additional tasks may be added to any activity.*"

IEEE 828-2005, "IEEE Standard for Software Configuration Management Plans," provide guidance for planning and executing a software configuration management program.

IEEE 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology."

IEEE 1042-1987, "IEEE Guide to Software Configuration Management." (Archived)

Guidance for Review of Software Quality in Applications for Safety Systems relying on the use of Digital Control Systems based on High-Quality Commercial Grade Equipment

For a commercial-grade element of the system, there should be evidence that an acceptance process has been applied to determine that there is reasonable assurance that the equipment will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under either a quality assurance program applicable for the facility or consistent with the management measures applied to the design and development of items relied on for safety that are appropriate to the facility. The acceptance process itself should address applicable key quality elements described in such programs or management measures. This process might vary depending on the specifics of the particular commercial-grade equipment and its intended application; however, it must establish the required assurance. One process for doing this is described in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," which was found acceptable by the NRC staff in a safety evaluation, dated July 17, 1997.

The steps of the dedication process may vary significantly depending on the vendors, components, and applications. Detailed specific information, in addition to the information provided in examples within EPRI TR-106439, is needed to perform an actual commercial dedication. Other EPRI guidance documents, such as EPRI TR-107330, "Generic Requirements Specification for Qualifying A Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants"; EPRI TR-107339, "*Evaluating Commercial Digital*

Equipment for High Integrity Applications - A Supplement to EPRI Report TR-106439"; EPRI TR-1001045, *"Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants,"* and EPRI TR-1011710, "*Handbook for Evaluating Critical Digital Equipment and Systems,"* may be useful in providing additional information on the qualification, analysis, and use of commercial grade dedicated equipment. When reviewing license applications where high quality, commercial grade equipment has been proposed, the reviewer should evaluate the descriptions of the alternatives selected and any deviations that were taken from the guidance document pertinent to the acceptance process. The dedication process may be applied in a "graded" manner according to safety significance and complexity.

The processes within EPRI TR-106439 are based on EPRI NP-5652, "Utilization of Commercial Grade Items in Nuclear Safety Related Applications," which discusses four methods for use in commercial-grade dedication. (Note: EPRI NP-5652 was conditionally endorsed in NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products." Further clarification of the guidance for use of EPRI NP-5652 is contained in NRC Generic Letter 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs.") These methods are (1) special tests and inspections; (2) commercial grade survey of the supplier; (3) source verification; and (4) acceptable supplier/item performance record. No one method will suffice by itself for typical applications. Method (4) must not be used as the only method for acceptance; however it may be used to support the conclusions reached by the application of one or more of Methods (1), (2), or (3). Method (2) should not be used as the basis for accepting items from suppliers with undocumented commercial quality programs or with programs that do not effectively implement their own necessary controls. Also, Method (2) should not be employed as the basis for accepting items from distributors unless the survey includes the part manufacturers as well, and the survey confirms that adequate controls are implemented by both the distributor and the part manufacturers. Depending on the application and the product, additional verification activities may be needed. Engineering judgment must be documented sufficiently to allow a comparably qualified individual to make the same conclusions.

Dedicated software items should not be updated to new revision levels without prior evaluation to determine whether the modified design is compatible with the functional safety requirements intended. Commercially dedicated items should not be operated in a configuration that is inconsistent with the original dedication.

This approach is based on the use of the existing commercial grade item dedication process, with supplemental guidance provided to help the user address digital specific issues. This approach emphasizes identification of appropriate critical characteristics with subsequent verification through some combination of review of operating experience, inspection, testing, analysis, and vendor quality program assessments. Therefore it is recommended that the reviewer use guidance from the following documents when evaluating the application to indicate that the licensee or license applicant has implemented some form of evaluation process when applying commercial grade digital equipment and software for use in safety applications:

EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,"

EPRI TR-107339, "Evaluating Commercial Digital Equipment for High Integrity Applications - A Supplement to EPRI Report TR-106439"

Regulatory Basis

10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," including Section 70.1, "Purpose," Section 70.4, "Definitions," Section 70.21, "Filing," Section 70.22, "Contents of applications," Section 70.34, "Amendment of Licenses," and Subpart H-Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material, Sections 70.61 through 70.76, with an emphasis on Section 70.62 and paragraph 10 CFR 70.64 a (1).

10 CFR Part 21, "Reporting of Defects and Noncompliance," including Section 21.1, "Purpose," Section 21.2, "Scope," and Section 21.3, "Definitions."

Technical Review Guidance

The reviewer should use the information contained in this ISG, as applicable, to evaluate whether a fuel cycle facility licensee or applicant has described in his application appropriate management measures to ensure that digital equipment performing IROFS functions or supporting functions has been or will be adequately designed, implemented, and maintained. The reviewer should also evaluate whether high quality processes have been followed in the development of software used in digital I&C applications for safety functions. The use of such high quality processes assists in limiting the occurrence of potential common cause software failures, in accordance with the requirements of 10 CFR 70.64 a (1), and provides a reasonable assurance that the control system using this software will perform its intended safety function, thus achieving the safety performance goals stated in 10 CFR 70.61. If the applicant is using NUREG-1520 or NUREG-1718, the reviewer should use the guidance in this document to evaluate the adequacy of the applicant's ISA Summary. The purpose of the ISA Summary review is not to verify the correctness of the software, but to verify whether the applicant has an acceptable methodology such that there is reasonable assurance of maintaining an adequate safety basis over the facility lifetime, by ensuring that the methodology results in limiting the occurrence of potential common cause software failures. License reviewers should evaluate the materials provided in the application and make a determination whether it provides reasonable assurance of adequate safety, or reasonable assurance of adequate compliance with the technical requirements of Subpart H of 10 CFR Part 70.

Recommendations

This guidance should be used to supplement the guidance contained in NUREG-1520, Chapter 11, "Management Measures," Appendix A, "Check List for Procedures," and Appendix B, "Records." This guidance may also be used to supplement the guidance contained in NUREG-1718, Chapter 11, "Plant Systems," Chapter 15 "Management Measures," and Appendix G, "Checklist for Evaluating Acceptance of Quality Assurance Elements."

References

1. U.S. Code of Federal Regulations, Title 10, Energy, Part 70, "Domestic Licensing of Special Nuclear Material."

2. U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility.” NRC: Washington, D.C. March 2002.
3. U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1718, “Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility.” NRC: Washington, D.C. August 2000.
4. U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1513, “Integrated Safety Analysis Guidance Document,” NRC: Washington, D.C. May 2001
5. ANSI/ASME NQA-1a-1995 Addenda to ASME NQA-1-1994 Edition, “Quality Assurance Requirements for Nuclear Facility Applications”
6. ANSI/ASME NQA-1-2008 “Quality Assurance Requirements for Nuclear Facility Applications” (Revision of ASME NQA-1-2004), Part 1, Requirement 3, Article 800: Software Design Control; Part 1 Requirement 7, Article 700, Commercial Grade Items and Services; and Part 1, Requirement 11, Article 400, Computer Program Test Procedures.
7. IEEE 828-2005, “IEEE Standard for Software Configuration Management Plans.”
8. IEEE 1012-2004 “IEEE Standard for Software Verification and Validation.”
9. IEEE 830-1998, “IEEE Recommended Practice for Software Requirements Specifications.”
10. IEEE 7-4.3.2-2003 “IEEE Standard for Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
11. IEEE 1074-2006 “IEEE Standard for Developing a Software Project Life Cycle Process.”
12. IEEE 1008-1987 “IEEE Standard for Software Unit Testing.”
13. EPRI TR-106439 “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications” October, 1996
14. EPRI TR-107330, “Generic Requirements Specification for Qualifying A Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants” December 1996
15. EPRI TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications - A Supplement to EPRI Report TR-106439” December 1997
16. EPRI TR-1001045, "Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants," December 2000.
17. EPRI TR-1011710, “Handbook for Evaluating Critical Digital Equipment and Systems”, November 2005.
18. Mathew Chiramal, USNRC, “Application of Commercial-Grade Digital Equipment in Nuclear Power Plant Safety Systems,” IEEE Press, October 2001
19. U.S. Nuclear Regulatory Commission (U.S.)(NRC). NUREG/CR-6421, “A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications,” prepared by G.G. Preckshot and J. A. Scott, Lawrence Livermore National Laboratory, March 1996
20. ANSI/ISA Standard 84.00.01-2004, “Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Hardware and Software Requirements” Approved September 2004
21. U.S. Nuclear Regulatory Commission (U.S.) (NRC). Regulatory Guide 1.152, Rev. 2, “Criteria for use of Digital Computers in Safety Systems Nuclear Power Plants” January 2006
22. U.S. Nuclear Regulatory Commission, Generic Letter 89-02, “Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products,” March 21, 1989
23. U.S. Nuclear Regulatory Commission, Generic Letter 91-05, “Licensee Commercial-Grade Procurement and Dedication Programs,” April 9, 1991

Appendix

Typical Software Development Life Cycle Model (V-Model)

(Reference: ANSI/ISA 84.00.01 Part 1 / IEC 61511-1 Mod)