SANDIA REPORT
SAND2021-14591
Printed September 2021

Sandia National Laboratories

Safety and Security Defense-in-Depth for Nuclear Power Plants

Andrew J. Clark and Michael T. Rowland

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

This report describes the risk-informed technical elements that will contribute to a defense-in-depth assessment for cybersecurity. Risk-informed cybersecurity must leverage the technical elements of a risk-informed approach appropriately in order to evaluate cybersecurity risk insights. HAZCADS and HAZOP+ are suitable methodologies to model the connection between digital harm and process hazards. Risk assessment modeling needs to be expanded beyond HAZCADS and HAZOP+ to consider the sequence of events that lead to plant consequences. Leveraging current practices in PRA can lead to categorization of digital assets and prioritizing digital assets commensurate with the risk. Ultimately, the culmination of cyber hazard methodologies, event sequence modeling, and digital asset categorization will facilitate a defense-in-depth assessment of cybersecurity.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

LIST OF ACRONYMS

Abbreviation	Definition
ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
DBE	Design Basis Event
DCS	Digital Control System
DCSA	Defensive Computer Security Architecture
DEG	Digital Engineering Guide
DID	Defense-in-Depth
EPRI	Electric Power Research Institute
FSF	Fundamental Safety Function
HAZCADS	HAZards and Consequences for Digital Systems
HSS	High-Safety-Significant
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
LBE	Licensing Basis Event
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LSS	Low-Safety-Significant
LWR	Light Water Reactor
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
O&M	Operation & Maintenance
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
RISC	Risk-Informed Safety Classification
SSC	Systems, structures, and components
TAM	Technology Assessment Methodology

Abbreviation	Definition
U.S.	United States

1. INTRODUCTION

Currently, cybersecurity defensive strategies for nuclear facilities rely largely on isolation and physical access controls, focused on containing the safety-related systems and assets. Such strategies provide few capabilities for detecting and responding to digital compromise where the adversary is able to gain access. The intent of this report is not to question prior strategies and evaluations. Rather, this report presents Defense-in-Depth (DID) strategies and evaluations showing how they can be leveraged for risk-informed cybersecurity. Cybersecurity programs are moving towards a risk-informed approach that integrates safety and security and demonstration of DID is a key component of that development. Throughout the industry, many cybersecurity programs already exist, however, the majority of those programs do not emphasize safety and security DID in the design, integration, and implementation of digital technology.

This report starts with contextual information – defining DID and providing historical background for DID. A Probabilistic Risk Assessment (PRA) primer is included that describes plant design requirements and many of the safety paradigms unique to nuclear power. Section 2 of this report describes two methods for risk informing approaches to determining DID requirements. Section 3 compares and contrasts DID frameworks for light water reactors (LWRs), non-LWRs, and international activities related to DID. Section 4 discusses the use of function-based assessments and Section 5 provides some concluding remarks.

1.1. Background

1.1.1. Safety Defense-in-Depth

Historically, safety defense-in-depth (DID) for nuclear power plants (NPPs) has considered deterministic evaluation of NPP designs. DID treatment considered a barrier approach where physical barriers were placed between radioactive material and the environment. Through design evolutions and maturation, NPP designs began to include active systems to respond to various design basis events (DBEs). The incorporation of active systems changed the risk assessment landscape. Prior to the development of modern PRA, NPP risk assessments were similar to "what if?" analyses that focused on evaluation of events that would challenge physical barriers. The incorporation of active systems and development of PRA created a new paradigm for DID evaluations. [1]

The majority of physical barriers are considered passive and include (but are not limited to): fuel itself (i.e., fission product holdup in fuel); fuel cladding; reactor vessel and reactor coolant system piping; and containment structures. Whereas passive structures do not rely on component response or operator actions, active systems do require operator actions and/or a multitude of systems, structures, and components (SSCs) to initiate on demand in response to some initiating event. Passive and automatic system responses are designed into many LWR technologies, but in many DBE scenarios, operator actions and active system responses are essential to preventing core damage.

Similar to safety assessments, the primary goal of cybersecurity plans and control method implementation is to protect the NPP from malicious attacks on safety systems. The subtlety of the safety and security function relationship should not be overlooked. Although cybersecurity requires unique tools, capabilities, and expertise, cybersecurity goals for NPPs share the goals of the safety assessments: ensure the plant can perform its fundamental safety functions (FSFs). Thus,

cybersecurity plans should leverage existing safety and risk assessments to the extent possible when developing cybersecurity strategies.

1.1.2. Risk Informed Assessments for Safety

This section presents some fundamental concepts for risk-informed assessment which will later be used to describe variations and evolutions in defense-in-depth concepts.

1.1.2.1. Probabilistic Risk Assessments for NPPs

In the U.S., every NPP has a PRA model for the plant. PRAs model the plant response to initiating events using fault tree and event tree models. Modeling success/failure of different systems to initiating events, plant consequences are modeled and quantified probabilistically. The probabilistic inputs come from basic events, which include operator actions/diagnosis events, SSC failure events, common-cause failure events, support system dependencies, plus many other types of events. PRA models are informed by Regulatory Guide 1.200, where Regulatory Guide 1.200 is developed in response to the ASME/ANS PRA Standards [2], [3]. Furthermore, PRA models are peer-reviewed by independent reviewers.

PRAs are used to develop risk-informed results and insights. Although PRAs are used in a risk-informed approach, qualitative analysis is often used with PRA to develop risk-informed results and insights. Code of Federal Regulations (CFR) 10 CFR 50.69 provides the regulations for NPPs and NEI 00-04 provides guidance for NPPs that wish to submit a risk-informed application [4], [5]. The benefits of a risk-informed application have been demonstrated across the industry by reducing/eliminating the need for nuclear quality assurance for SSCs that are not safety-significant. Examples of the cost-benefits of the risk-informed approach are provided in a "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors" [6].

1.1.2.2. Safety LBEs

The term "Licensing Basis Events" (LBE) is a term not formally used in NRC documents for LWR technologies, but colloquially the term LBE references the entire collection of events that a nuclear reactor could experience in the lifetime of the plant. The collection of LBEs also consists of internal/external hazards (e.g., internal fires/seismic events), different plant operating states (e.g., shutdown), and beyond design basis events (e.g., large loss-of-coolant-accident coinciding with a station blackout). One type of LBEs are DBEs where DBEs are events that a nuclear power plant must be designed to withstand and ensure functions of safety-related SSCs operate during postulated events [7]. For current LWR technologies, DBEs are identified deterministically and all plants of a specific technology and design must ensure they have sufficient capability to mitigate and/or prevent DBEs.

A key component of DBEs is the initiating event which represents an event that perturbs steady-state operation and could lead to an undesired plant condition [8]. The NEI 00-04 guidance for SSC categorization does address SSC events that directly or indirectly affect or are affected by initiating events. Nuclear power plant PRAs include extensive analysis for DBEs. The PRAs model the initiating event, the event sequences which model the success/failure of various SSCs and operator actions that must respond to the initiating event, and the end-state for each event sequence. In other words, PRA models provide a concise evaluation of DBEs and the consequences of various DBE event sequences

The existing collection of DBEs for current LWR technologies—disregarding advanced LWR technologies such as the AP1000 design—DBEs were established for safety and without security considerations. Identification of new security-related events is beyond the scope of this report, but it is envisioned that new security-related events may not align with existing DBEs. The purpose of this report is to demonstrate how cybersecurity hazard methodologies can be used commensurate with existing risk assessments.

1.1.3. Risk Informed Safety Categorization

NEI 00-04 [9] provides guidance for SSC categorization in alignment with 10 CFR 50.69 [4], illustrated in Figure 1 which utilizes both deterministic and probabilistic categorizations. The "safety-related" and "non-safety related" categories are based on deterministic approaches and the "safety significant" and "low safety significant" categories are derived from probabilistic evaluations. Following the risk-informed philosophy associated with 10 CFR 50.69, NEI 00-04 guidance also encompasses the principles of risk-informed by leveraging both probabilistic and deterministic approaches in the decision-making process. The guiding principles for risk-informed safety classifications (RISC) are:

- Use applicable risk assessment information.
- Deterministic or qualitative information should be used if no PRA information exists related to a particular hazard or operating mode.
- If PRA information is available, the categorization process should employ a blended approach considering both quantitative PRA information and qualitative information.
- The RG 1.174 principles of the risk-informed approach to regulations should be maintained [10].
- A safety-related SSC will be categorized as RISC-1 unless a basis can be developed for categorizing it as RISC-3.
- Attribute(s) that make an SSC safety-significant, and the basis for categorization as low-safety-significant (LSS), should be documented.

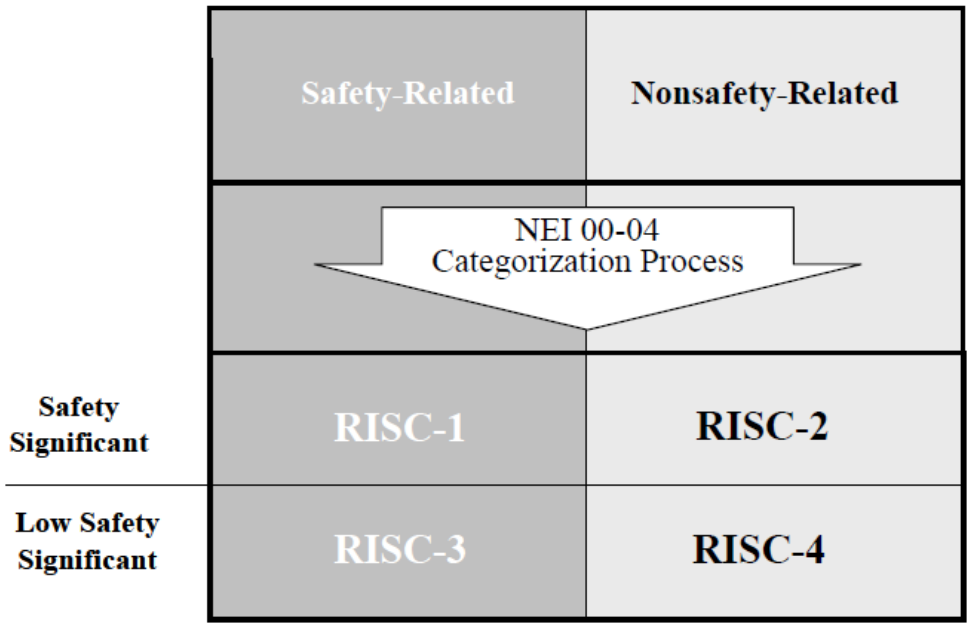

Figure 1. Risk-informed safety classifications [5].

The categorization process described in NEI 00-04 leverages the plant-specific PRA and results in the identification of SSCs as high-safety-significant (HSS) or LSS. Determination of HSS and LSS is derived from importance measure[1] analysis related to core damage frequency (CDF) and large early release frequency (LERF). A summary of the NEI 00-04 categorization process is shown in Figure 2. The processes "Defense-in-Depth Characterization" and "Risk Sensitivity Study" in Figure 2 will be discussed in Section 2.2.

[1] Risk importance measures are indexes that are used to rank SSCs using risk-informed methods. These are quantitative values derived from the PRA models. Several types of importance measure may be used by PRA analyst.

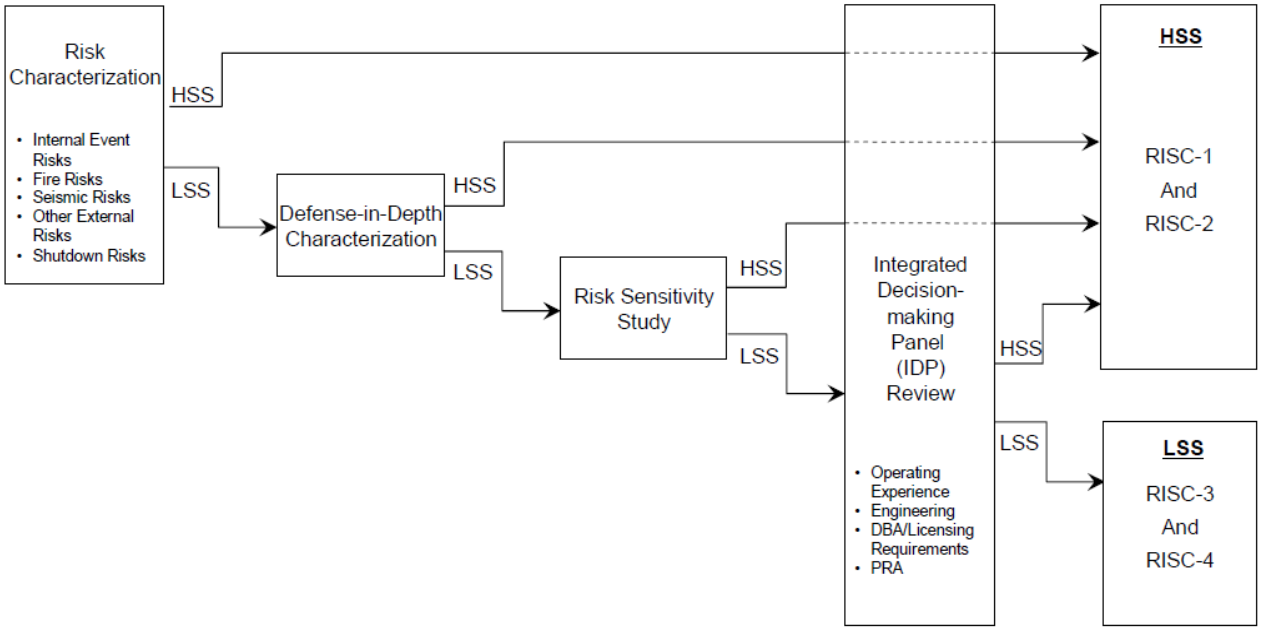

Figure 2. Summary of NEI 00-04 Categorization Process

1.1.4. Cybersecurity Defense-in-Depth

Although Sections 1.1.1 through 1.1.3 focused specifically on safety, the legacy of decades of nuclear safety engineering contribute significantly to cybersecurity. Nuclear PRA is an entire engineering discipline built to ensure that critical design principles are upheld. Cybersecurity plans can leverage plant designs that have been engineered with safety DID and strive to utilize the same design principles utilized by safety DID, that is, through a combination of redundant, diverse, and/or independent control methods. As new digital technologies are introduced, cybersecurity assessments need to ensure that new digital functionality maintains these design principles and does not introduce new, unexpected failure modes or result in common cause failures, even in the presence of cyber attacks.

Cyber security DID starts with existing safety DID. Safety PRA identifies safety significant events and the associated systems or collection of systems. Cyber security analysis considers how these events can be caused by an attacker. There are two possible paths for cyber events: 1) enhance the plant design such that cyber events are impossible or that the plant safety function is ensured even in the event of a successful attack or 2) design and maintain appropriate cyber security to prevent a successful cyber attack.

To prevent a successful attack cybersecurity DID should aim to implement multiple layers of controls (1) within or at the risk source (i.e., the system or device for which compromise can result in unacceptable risk), (2) to the environment or external to the risk source (e.g., physical access control to vital areas), and (3) to the personnel/organization (e.g., compulsory cyber awareness training).

1.1.4.1. Cybersecurity Management at NPPs

Regulatory Guide 5.71 provides guidance for NPPs to categorize systems and digital assets [11]. NEI 08-09 and NEI 13-10 provide guidance for implementing cybersecurity controls for systems and digital assets [12], [13]. Unlike the approach described in Section 1.1.3, categorization of digital assets is deterministic. While adequate, the guidance has generally resulted in over-conservative cybersecurity strategies and implementation of controls that are not commensurate with the safety-significance of the systems and SSCs that digital assets are meant to supervise and control.

Current cybersecurity management relies upon isolation and physical access controls to meet many of the requirements of the Regulatory Guide 5.71 or NEI 08-09. These controls are implemented to the operational environment that contains the systems and devices, which provides little capabilities for detecting and responding to compromise of these systems and devices where the adversary is able to gain access.

1.1.4.2. Risk Informed Assessments (Cybersecurity)

Several stakeholder engagements between NPP operators, the U.S. NRC, NEI, the Electric Power Research Institute (EPRI), to name just a few, are actively developing guidance and methods for risk-informed cybersecurity. One of the notable activities led by EPRI is the development of the Digital Engineering Guide (DEG) [14] which includes methodologies for hazard identification for digital systems (i.e., HAZards and Consequences for Digital Systems [HAZCADS] [15]) and mapping of hazards to cybersecurity controls (i.e., Technology Assessment Methodology [TAM] [16]). Thorough discussion of the DEG, HAZCADS, and TAM is beyond the scope of this report, but various comments will be made in reference to these methodologies throughout this report.

2. RISK-INFORMED CYBERSECURITY CONSIDERATIONS

Establishing safety DID requires several different technical analyses before DID assessments are considered. As will be discussed in this section, several of the technical elements that contribute to DID assessment could be invalidated by cybersecurity. Thus, these safety technical elements of DID are discussed considering the potential impacts from cybersecurity. Section 2.1 discusses the process of selecting licensing basis events (LBEs) and design basis events (DBEs). Section 2.2 discusses the risk-informed categorization of SSCs. Both sections provide a background on existing approaches for safety as well as considerations for cybersecurity.

2.1. DBE Considerations

The historic development of DBEs has followed an inductive approach, where initiating events are hypothesized, and system responses and subsequent consequences are modeled. With respect to initiating events, it's possible that security-related initiating events could occur. Security-related initiating events may be unique and may have no corollary to existing initiating events. For example, a cybersecurity event could cause a loss of feedwater, an initiating event considered in PRAs, but a actuation of all ECCS functions is not considered by PRAs. However, they will extend from the plant capabilities established by the plant design. For cases where there is no corollary between a security-related event and an initiating event in the PRA model, there would be no pre-existing event sequences in the PRA that would be able to predict the consequences from security-related events.

Security-related initiating events that cannot be correlated to existing initiating events may require a separate accident scenario analysis.

For security assessments which assess malicious attacks to system functions, the accident scenarios and corresponding consequences follow a deductive approach, meaning security-related events are aligned to existing DBEs. The major assumption of deductive approaches for cybersecurity is that security-related DBEs will follow the same accident progressions identified in the PRAs. For example, if the PRA assumes that system 1 operates before system 2, then the deductive approach to security would also assume this order of operations. However, this assumption may no longer be valid for security-related events [17]. Sabotaging the order of system responses is possible and may require additional accident scenario analysis to predict the consequences.

Accident scenario assumptions in the PRA models may not follow the same accident scenarios during cyber attack events and will likely need to be revised.

In consideration of LBE, this report recommends a risk-informed defense-in-depth strategy to provide protection for these potential unanalyzed conditions, or analysis where the bounding assumptions have been invalidated.

2.2. Safety on SSC Categorization

Through identification of digital SSC dependencies with safety functions, an initial scoping assessment can be used to identify safety-significant SSCs. A risk analyst can argue that if the DID evaluation determines that a system is low-safety-significant (LSS) and that the digital modification does not reduce the baseline configuration, the digital SSCs may also be categorized as LSS.

Depending on the DID evaluation, it may be argued that an extensive cybersecurity hazard evaluation is not necessary. This is justified probabilistically as follows:

During the probabilistic assessment, the physical process component is assumed to always fail (i.e., the probability of failure equals 1.0). The PRA model is rerun with this assumption and the results indicate the importance of that SSC, where importance in the PRA domain is determined probabilistically. Thus, whether the failure mechanism of that SSC is digital or not is irrelevant because the PRA models assumes it always fails. Acknowledging that cybersecurity end-states are bounded by the functions that the SSC is intended to perform, the digital SSC can effectively adopt the same safety significance value as the physical process SSC.

Although cybersecurity analysis may be complex such that its difficult to bound the analysis, the cyber effects on the physical process may be bounded.

Although the effects on the physical process may be bounded, it's possible that digital connections exist between systems and components such that common cyber events could be experienced on multiple systems and components. In order to facilitate the assessment of common cyber events, it's necessary to extend the system boundaries to include all connecting digital assets, including network connections. Extending the system boundaries will require additional digital system information which generally includes:

- Identification of system functions, including digital Instrumentation and Control (I&C) subfunctions (this should consider systems associated with electrical systems, HVAC, etc.).
- System boundary definitions should be revisited; system boundaries need to consider the functions identified above.
- Relative mapping of digital I&C components to system functions and subfunctions.

Cybersecurity hazard methodologies, such as HAZCADS, should address each of these elements. When identifying the digital I&C subfunctions, each subfunction should be correlated to the overall safety function where applicable. Defining system boundaries will likely be achieved through the first steps in the cybersecurity hazard methodologies where digital network diagrams and process diagrams are combined—these diagrams will be referred to as "control structures" throughout this report. Implicit modeling of SSCs with system functions and subfunctions should be achieved, to some degree, through the system diagrams developed in the cybersecurity hazard methodologies. For completeness, the digital control system (DCS) relationships to system functions and process components should be explicitly documented.

Define system boundaries and functions such that DCSs are included and ensure digital system interfaces, interactions, and interdependencies are explicitly acknowledged.

A crucial element for SSC categorization of digital systems is to develop dependency matrices [18] between a collection of systems, system functions, and the DCSs responsible for the system functions. Upon completing the dependency matrices for a set of systems, the dependencies should be compared to the baseline configuration—that is, the configuration before digital SSCs were included.

The development of the control structures along with the dependency matrices provides a mapping of digital SSCs to the physical process SSCs (e.g., valves, pumps, heat exchangers, etc.). Noting that the vast majority of physical process SSCs are represented as basic events in the PRA models, risk analyst can quickly relate the digital SSC dependency matrices directly to the PRA models.

Develop dependency matrices between system functions and digital SSCs.

3. RISK-INFORMED DEFENSE-IN-DEPTH

The U.S. Nuclear Regulatory Commission (NRC) Website Glossary defines DID as, "An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures," [19].

The International Atomic Energy Association (IAEA) describes DID as, "…defence in depth ensures that no single human error or equipment failure at one level of defence, nor even a combination of failures at more than one level of defence, propagates to jeopardize defence in depth at the subsequent level or leads to harm to the public or the environment" [20]. The "levels" mentioned in the IAEA description correspond to progression of transients and accidents in a nuclear power plant and are summarized in Table 1 and depicted in Figure 3. The IAEA description of DID also highlights the importance of physical barriers[2] that prevent or limit the release of fission products. In the IAEA DID report, the culmination of the DID activities result in objective trees.

Table 1. IAEA Levels of Defense-in-Depth (adapted from [20]

DID	Objective	Essential means for achieving the objective
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-sire emergency response

[2] The physical barriers typically considered include the fuel matrix, fuel cladding, pressure boundary/reactor coolant system, and the containment or confinement.

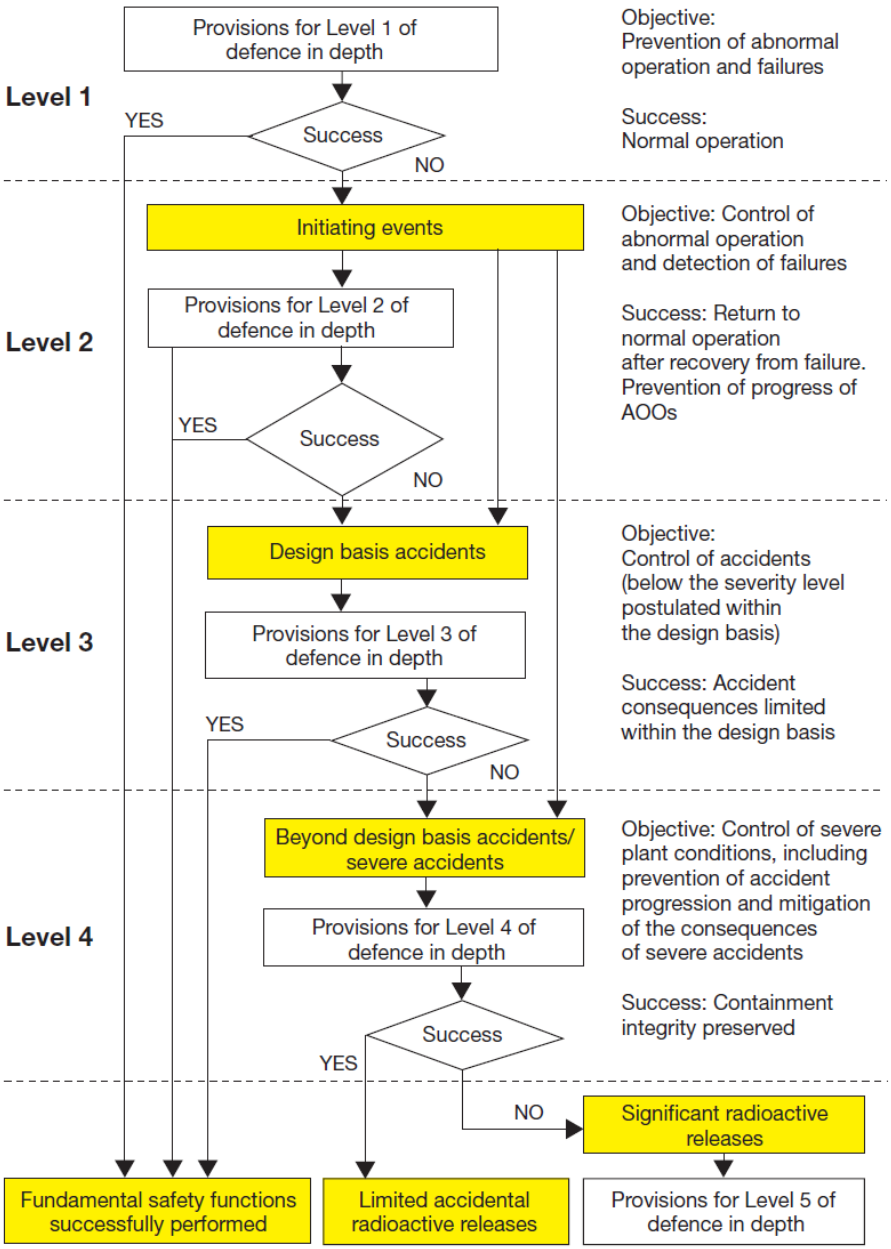

Figure 3. IAEA Flowchart for Defense-in-Depth [20]

The NRC and IAEA use of DID are similar but different. The NRC refers to the prevention and mitigation of accidents, which aligns with the IAEA DID philosophy. One of the major differences in the IAEA and NRC discussions of DID is that IAEA evaluates function significance deterministically whereas the NRC discussion has more emphasis on probabilistic evaluation—note that probabilistic models often include deterministic evaluations implicitly. IAEA does mention that future evaluations can be complemented by probabilistic analysis, but that is not formalized in the current IAEA publications.

The DID discussion differences are not necessarily a result of differences in DID philosophy—the philosophies are actually very similar—but rather how PRA[3] is performed in the U.S. PRAs cover the entirety of IAEA Levels 2 and 3 and different PRA models will incorporate Levels 1, 4, and 5 depending on the specific application [21]. NEI 18-04 has been endorsed by the NRC as one acceptable method for Non-LWR designers to use when preparing a risk-informed, performance-based application [22]. While developed with an intended audience of Non-LWR technologies, the principles and approaches can be applied to LWRs. One of the many reasons why LWR operators do not plan to adopt the NEI 18-04 approach is because of the prescriptive nature of LWR applications and the time spent developing complementary and satisfactory applications.

Figure 5 presents the "Framework for Establishing DID Adequacy," from NEI 18-04 which depicts a framework for establishing DID that includes probabilistic and deterministic assessment techniques using a combination of plant capabilities and programmatic controls. Plant capability DID generally relates to hardware and design and is provided by ensuring that SSCs are able to prevent and mitigate events, defend against common cause failures, include conservative design margins, and provide barriers to the release of radionuclides. Programmatic defense in depth includes measures to increase confidence in SSC performance during operation and throughout the life of a plant (e.g., quality assurance, testing, maintenance, and configuration control), operational procedures and training, and preparedness for emergency plan protective actions.

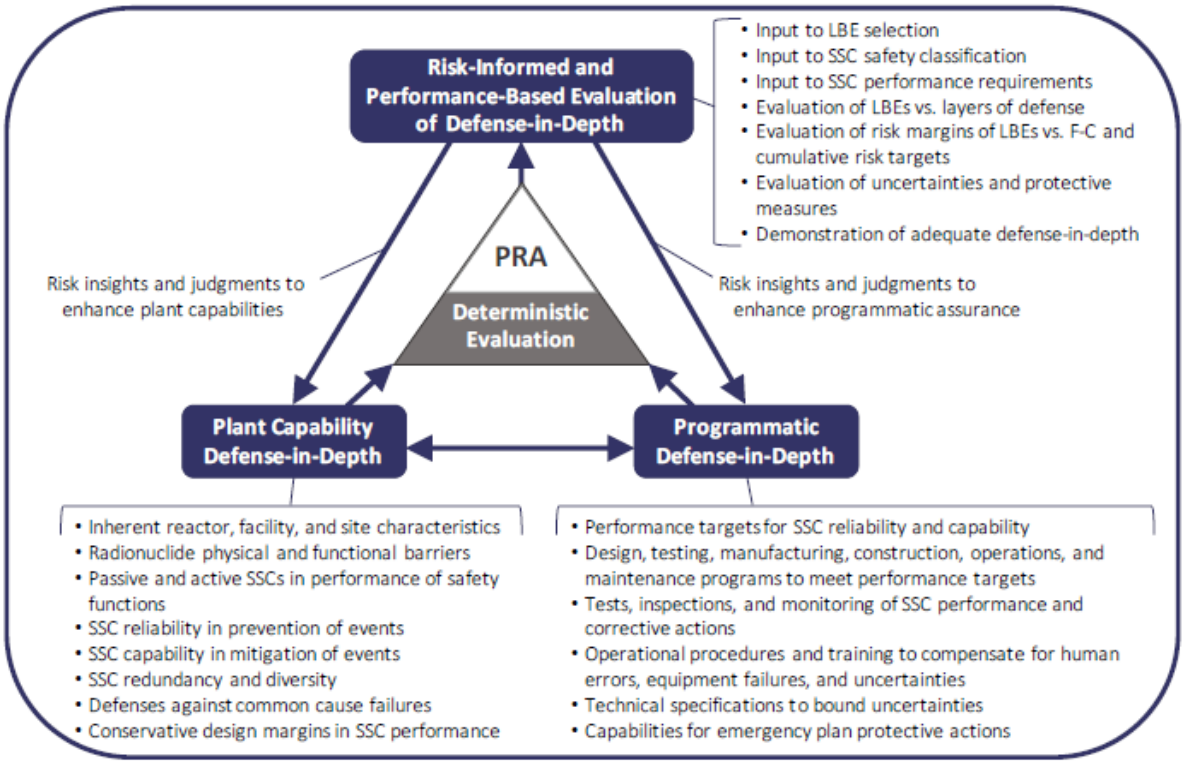

Figure 4. NEI 18-04 Framework for Establishing DID Adequacy [21].

[3] Internationally, PRA is referred to as Probabilistic Safety Assessment, or PSA.

3.1. Safety DID Considerations

Generally speaking, the U.S. LWR fleet has sufficient DID strategies established and DID has been adequately evaluated. The intent of this report is not to question prior strategies and evaluations. Rather, this report emphasizes how DID strategies and evaluations can be leveraged for risk-informed cybersecurity. Cybersecurity programs are hoping to move towards a risk-informed approach that integrates safety and security and demonstration of DID is a key component of that development. Throughout the industry, many cybersecurity programs already exist, however, the majority of those programs do not emphasize safety *and* security DID in the design, integration, and implementation of digital technology.

Using the insights from Section 2.1 for LBEs and Section 2.2 for SSC categorization, risk analysts can evaluate DID within processes utilized by both LWR and Non-LWR technologies. The safety significance for physical process SSCs is characterized and by use of the digital SSC dependency matrices, an initial approximation of the safety significance of digital SSCs can also be characterized.

Utilizing the important takeaways from Section 2.1 and 2.2, existing DID approaches may be applied for initial determinations of digital system DID.

Additional analysis may be required to thoroughly evaluate DID of digital systems, but these initial results can have substantial resource benefits for NPP operators. For example, through this initial DID evaluation, decision-makers can prioritize digital SSCs of highest safety-significance and systems that lack DID. By prioritizing these systems, designers can ensure security measures are commensurate with the risk to the public.

4. FUNCTION-BASED APPROACH TOWARDS I&C DESIGN

This report has presented different historical approaches to managing plant and cyber security risk and thus determining defense-in-depth requirements. Ultimately, however, defensive strategies are just part of the bigger goal of supporting and protecting critical plant safety functions.

4.1. Safety Functions and Features

From a safety perspective, most nuclear reactors rely on three primary safety functions: control reactivity and heat generation; control heat removal, including decay heat (i.e., long-term heat removal); confinement of radioactive material. NEI 18-04 [23] considers these safety functions fundamental, thus, they are called fundamental safety functions (FSFs)—this terminology is also adopted throughout the remainder of this report for simplicity. The FSFs are common to all reactor technologies, including LWRs. The design, construction, and operation & maintenance (O&M) has worked towards ensuring multiple layers of defense for each FSF. Types of defense may consist of inherent SSCs, passive SSCs, active SSCs, operator actions, and confinement SSCs.

Inherent safety refers to characteristics of the reactor design that are physically intrinsic to the design. For example, PWR and BWR design have a negative temperature coefficient of reactivity, meaning as the temperature of the fuel increases, the reactivity of the fuel goes up, thus preventing a "runaway reaction". Note that this does not imply the reaction turns off, only that the reactivity due to fuel temperature is bounded and cannot increase indefinitely.

Passive safety refers to characteristics of the reactor design that are purposefully designed such that active responses by controllers or operators are not required. For example, natural circulation occurs in reactors when steam/water mixture circulates throughout the reactor due natural thermalhydraulic phenomenon. The primary driving force for natural circulation is derived from heat removal and boundary conditions, such as the heat in the secondary loop. Without adequate boundary conditions, this passive function may not work adequately, if at all. Unlike inherent safety, passive safety is dependent on auxiliary and environmental conditions.

Active safety refers to characteristics of the reactor design that respond from specific actions, which may activate from automatic (e.g., a controller) or manual (e.g., operator) actions. For example, during a loss-of-coolant accident (LOCA), backup injection systems must activate to supply coolant to the reactor to control heat removal. In order for coolant supply to be provided, valves must open, turbines must spin, pumps must turn on, plus many other SSC demands in order for the FSFs to be upheld. In the absence of specific sequence of activations or combinations of activations, the FSFs may be compromised. Most backup injection systems for PWRs and BWRs rely on active systems.

Operator actions are similar to active safety systems, but from a reliability perspective, require a different scientific approach to analyze. Across the spectrum of possible events, from normal conditions to beyond design basis accidents, operators will monitor and activate SSCs either from the control room or directly at the SSC itself, depending on the response of the SSC. For PWRs and BWRs, operator actions are essential in every event sequence and are thus, crucial to prevent consequences and managing risk.

Finally, there is the confinement SSCs that help prevent or mitigate the release of radioactive material. For LWR technologies, there are typically four barriers to the release of radioactive material: fuel itself, fuel cladding, coolant system boundary, containment buildings. Note that

depending on the reactor design and specific accident scenario/progression, some boundaries may be lost or other boundaries can be credited. For example, for PWRs, a break in a steam generator tube may create a bypass of the primary system boundary, but the secondary system boundary may provide another layer of defense. Conversely, in some reactivity transient events, localized fuel cladding damage may occur thus eliminating the fuel cladding boundary.

Understanding the layers/types of defense is necessary to follow the lines of conclusion that come later, particularly with respect to the risk-informed cybersecurity. *Cybersecurity is often considered its own discipline, but when considering the operational technology for high consequence systems, cybersecurity functions should be used in concert with safety functions. When evaluating cybersecurity defense-in-depth, each of the discussed safety functions and features will provide unique characteristics to risk-informed cybersecurity.*

4.2. Security Functions

IAEA Report, "Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants" provides an extensive review of the functional approach towards digital I&C [24]. In that report, a common way to subdivide I&C by functional group is the following:

- Sensors
- Operational control, regulation, and monitoring systems
- Safety systems
- Communication systems
- Human-system interfaces
- Actuators

Furthermore, the IAEA report notes that the functionality that is embodied in the I&C system architecture can be decomposed into several elements, for example, control, monitoring (see Page 9 of IAEA Report for complete list). As acknowledged in the IAEA report, security functions for nuclear power plants need to span both safety and security. Figure 5 of the IAEA report provides a functional overview of NPP I&C.

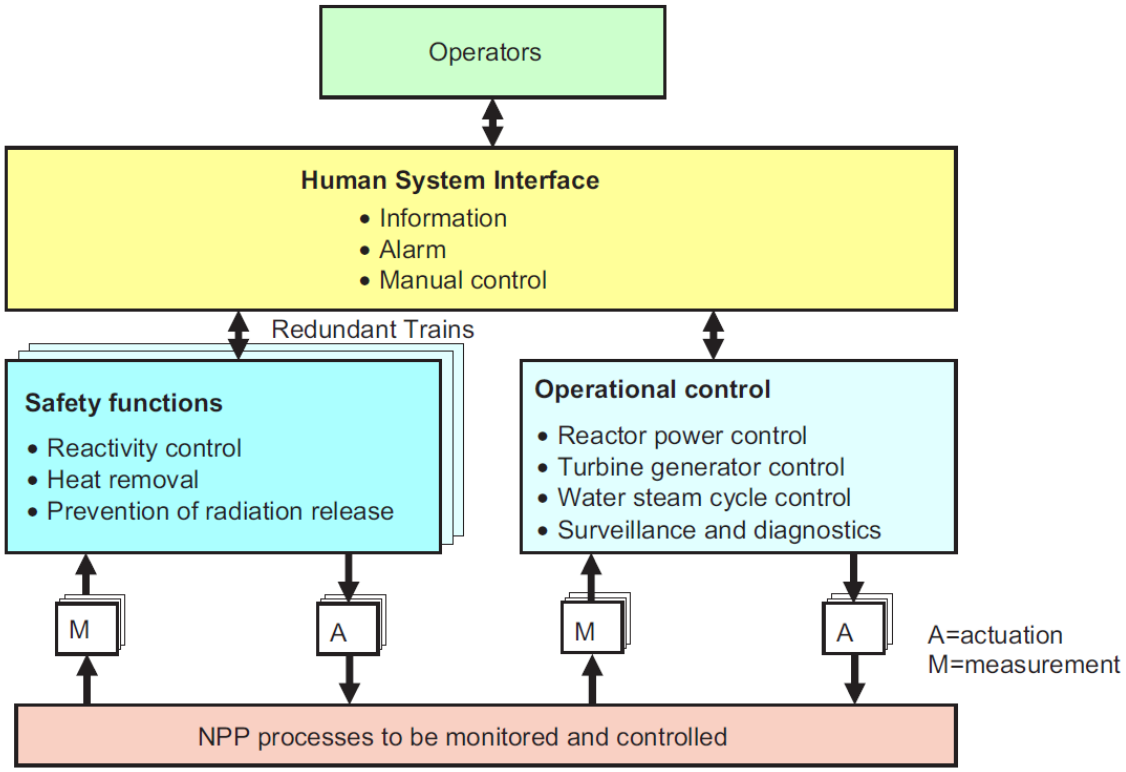

Figure 5. Functional overview of NPP I&C (Figure 5 [24]).

With respect to addressing an integrated safety and security approach, the first goal is to relate safety and security functions. Next, the goal is to identify how digital/cyber events can result in loss/degraded functions, or even an unexpected behavior related to that function. These relationships between digital/cyber are crucial to clearly articulate how threats result in consequences. Furthermore, any proposed method should be systematic and structured in order to facilitate a transparent assessment.

As stated in IAEA Report, software can fail in many different ways, whereas the hardware failures occur based on the laws of physics (e.g., stress corrosion cracking). It is daunting to consider having to address all permutations of software failure, especially when considering the software firmware patches, updates, and operating system updates that occur during a computer's lifecycle. Considering this, it is easy to understand why assessing failures of computers is difficult, perhaps even impossible for large Industrial Control Systems (ICS).

Despite the complexities of computer failure modes, the components that they are intended to control will fail or misbehave in predictive ways. For example, we can consider a Programmable Logic Controller (PLC) that is exploited by a cyber attack—we purposefully ignore the cyber scenario, attack vector, and complexity of the attack. Clearly, any cyber attack on a NPP is undesirable, and it is acknowledged that there are cyber control methods that can be implemented to prevent different types of attacks. Regardless of the near-unbounded problem of cybersecurity, the changes in the process that are feasible by the attack are predictive and are readily bounded. For example, assume that the PLC in question controls a valve and a pump in a water injection loop. The valve can only increase or decrease its position, resulting in more or less water, respectively,

being injected into the system. Similarly, a pump can only speed up or slow down, resulting in higher or lower flow speed/pressure. Dynamically, these same actions can be cycled, meaning the process components can increase position/speed up or decrease position/slow down many times over a given time period. In other words, despite the complexity or novelty of the attack, the process component behavior may be bounded. Downstream of the valve or pump failure/misbehavior, various SSC failures are possible, but the analysis of those SSC failures can be determined by experimentation and/or modeling and simulation.

Returning to the DID discussions in Section 3. The IAEA assignment of functions to security levels leverages the safety categorization (or system class). Computer security levels are the basis for a graded approach and broadly identify the security demands of the function. Due to the correlation between safety categorization and computer security levels, the security levels and safety defense in depth level are broadly equivalent. Significance of functions is determined almost entirely on the severity of the consequences associated with compromise of the function.

However, DID for cybersecurity requires the establishment of secure areas (e.g., IAEA computer security zones) and the arrangement of these zones to construct a defensive computer security architecture (DCSA). The IAEA and the NRC stress the importance of independent and redundant layers of defense. The IAEA computer security levels and function significance have importance in the specification of the DCSA requirements, with the higher security levels (i.e., 1 and 2) requiring protection from attacks initiated from systems assigned lower levels (i.e., 3, 4, and 5).

Essentially, the physical end states of a cyber attack may be bounded and safety assessments should be leveraged to the extent possible to ensure undue resources are not expended. Different methods have been developed that facilitate the conjunction of safety and security—see HAZCADS HAZOP+ for some examples. Regardless of the methodology employed, a given methodology must be able to bridge the gap between the digital I&C and the process components they are meant to control. By focusing on permutations of the process component behaviors, cybersecurity assessments are likely to be refined, focused, and—in cases where PRA models are readily available—be risk-informed.

5. CONCLUSIONS

Integrating safety and security for defense-in-depth is crucial to protecting nuclear power plants from cybersecurity events resulting in consequences. Achieving safety and security occurs through integrating security with the technical elements of a safety analysis. Risk-informed approaches for cybersecurity should at least consider how cybersecurity challenges the safety assessment of LBEs; SSC interfaces, interactions, and interdependencies; and existing DID design.

Cybersecurity assessment of LBEs can occur inductively or deductively. The inductive approach considers plant initiating events that are caused by a cybersecurity event which can lead to unique accident scenarios that had not been assessed previously by the safety assessment. In other words, the analyst must revisit elements of the risk triplet[4]: what can go wrong and what are the consequences. The deductive approach considers how accident scenarios already considered in the safety assessment may be challenged by cybersecurity events. For methodologies such as HAZCADS, the deductive approach results in new basic events being added to the existing safety assessment models.

The assessment of SSC interfaces, interactions, and interdependencies can be accomplished using a blend of current and advanced methodologies. Cyber hazard methodologies such as HAZCADS model the interfaces and interactions between digital and process SSCs. SSC interfaces and interactions are described using control structures which map control actions and feedback between digital and process SSCs. When performed on large, complex facilities, control structures also model the interdependencies between SSCs. In addition, cyber hazard methodologies predict how cybersecurity events at SSCs challenge and take advantage of the interfaces, interactions, and interdependencies to result in misbehavior of an SSC function. Identifying the digital and process SSC misbehaviors results in a bounded set of actions an adversary may take to compromise the nuclear power plant. Thus, cybersecurity analyst can take actions to protect, detect, respond and recover to these cybersecurity events in order to prevent consequences.

Finally, the culmination of assessing impacts to LBEs and SSC interfaces, interactions, and interdependencies allows an assessment of DID. First, the facilities need to consider existing DID design. Existing DID design should, at a minimum, not be compromised by the DCS design. For example, a single controller that controls three systems with proven DID safety design would result in bypassing of existing DID design. In these cases, security DID will need to undergo considerable assessment to demonstrate that this configuration is adequate for the facility.

The approach described throughout this report discusses the major technical elements of a safety assessment that should be considered to achieve a risk-informed cybersecurity approach—note, however, that several other PRA technical elements are not discussed in this report which require consideration for risk-informed cybersecurity. By utilizing the safety assessment during the digital and cyber design, "safety by design" can be achieved for cybersecurity.

Section 3 illustrates how safety DID is established through LBEs, SSC categorization, and risk-informed approaches. Through identification of digital SSC dependencies with safety functions, an initial scoping assessment can be used to identify safety-significant SSCs. A risk analyst can argue

[4] The question in the risk triplet, "how likely is it", is purposefully absent from this discussion. The reason for this absence is due to a lack of current consensus regarding the statistical nature of cyberattacks. Discussions surrounding, "how likely is it", are deferred to future R&D.

that if the DID evaluation determines that a system is low-safety-significant (LSS) and that the digital modification does not reduce the baseline configuration, the digital SSCs may also be categorized as LSS. Depending on the DID evaluation, it may be argued that an extensive cybersecurity hazard evaluation is not necessary. Future cybersecurity R&D should consider tiers of evaluation that would facilitate quick cybersecurity assessments to confirm LSS categorization.

The primary conclusion here is that with relatively simply digital system mapping to safety functions, existing PRAs can quickly and efficiently be used to identify digital SSCs that are low-safety-significant or high-safety-significant. For digital SSCs categorized as HSS, additional cyber hazard analysis and/or cybersecurity assessments will be necessary to ensure the digital SSC can perform its intended function.

REFERENCES

[1] T. R. Wellock, Safe Enough? A History of Nuclear Power and Accident Risk, Oakland, CA: University of California Press, 2021.

[2] American Society of Mechanical Engineers, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," The American Society of Mechanical Engineers and American Nuclear Society, 2008.

[3] U.S. Nuclear Regulatory Commission, "Regulatory Guide 1.200 Revision 2 An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," 2009.

[4] U.S. Nuclear Regulatory Commission, "10 CFR 50.69 Risk-Informed categorization and treatment of structures, systems and components for nuclear power reactors," 2008.

[5] Nuclear Energy Institute, "10 CFR 50.69 SSC Categorization Guideline," 2005.

[6] NRC, "10 CFR 50.69 Risk-informed categorization and treatment of structures, systems, and components for nuclear power reactors," 19 November 2012. [Online]. Available: https://www.nrc.gov/docs/ML0414/ML041470460.pdf.

[7] U.S. Nuclear Regulatory Commission, "NUREG-0800, Chapter 15: Standard Review Plan for the Review of Safety Analysis Report for Nuclear Power Plants: LWR Edition - Transient and Accident Analysis," 2007.

[8] U.S. Nuclear Regulatory Commission, "NUREG-2122 Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking," 2013.

[9] Nuclear Energy Institute, "NEI 00-04 (Rev 0) 10 CFR 50.69 SSC Categorization Guideline," Nuclear Energy Institute, WASHINGTON, 2005.

[10] U.S. Nuclear Regulatory Commission, "Regulatory Guide 1.174 An Approach For Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," 2018.

[11] U.S. Nuclear Regulatory Commission, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities," 2010.

[12] Nuclear Energy Institute, "NEI 08-09 Rev. 6 Cyber Security Plan for Nuclear Power Reactors," 2010.

[13] Nuclear Energy Institute, "NEI 13-10 Rev. 5 Cyber Security Control Assessments," 2017.

[14] Electric Power Research Institute, "Digital Engineering Guide: Decision Making Using Systems Engineering," EPRI, 2021.

[15] Electric Power Reserach Institute, "HAZCADS: Hazards and Consequences Analysis for Digital Systems - Revision 1," EPRI, 2021.

[16] Electric Power Research Institute, "Technical Assessment Methodology (TAM) Revision 1," EPRI, 2019.

[17] International Atomic Energy Agency, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," Vienna, 2018.

[18] International Atomic Energy Agency, "COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES," IAEA, Vienna, 2017.

[19] NRC Web "Glossary", "Defense in Depth," U.S. Nuclear Regulatory Commission, 26 June 2020. [Online]. Available: https://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html. [Accessed 17 November 2020].

[20] International Atomic Energy Agency, "Assessment of Defence in Depth For Nuclear Power Plants," Safety Report Series No. 46, Vienna, 2005.

[21] Nuclear Energy Institute, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development, Revision 1," NEI 18-04, August 2019.

[22] U.S. Nuclear Regulatory Commission, "Draft Regulatory Guide DG-1353 Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors," April 2019.

[23] Nuclear Energy Institute, "Risk-Informed Performance-Based Technology Guidance for Non-Light Water Reactors," NEI, 2019.

[24] International Atomic Energy Agency, "Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants," IAEA, Vienna, 2011.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	01977	sanddocs@sandia.gov

Email—External [redacted]

Name	Company Email Address	Company Name
Rebecca Onuschak	rebecca.onuschak@nuclear.energy.gov	DOE-NE Cybersecurity R&D Program Manager
PICS NE	n/a (upload into PICS Website)	DOE-NE Cybersecurity R&D

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.