U.S.A. REGULATORY EFFORTS FOR CYBER SECURITY OF ADVANCED REACTORS

I. GARCIA[1], J. JAUNTIRANS[2], M. ROWLAND[3]

[1]U.S. Nuclear Regulatory Commission (NRC), Rockville/Maryland, U.S.A.
[2]U.S. NRC, Rockville/Maryland, U.S.A.
[3]Sandia National Laboratory, Albuquerque/New Mexico, U.S.A.

Abstract

Small Modular Reactors / Advanced Reactors (SMR/ARs) are expected to provide safe, secure, and economical power that have the potential to support initiatives aimed at combating climate change. Current proposed SMR/ARs involve diverse technologies that include next generation modular pressurized water reactors, high temperature gas cooled reactors, molten salt reactors, and liquid metal cooled fast reactors. These diverse technologies each have a unique set of functions and systems that support both nuclear safety and security. To address these challenges, the U.S. Nuclear Regulatory Commission (NRC) is moving toward a risk informed, performance based and technology-neutral regulation and associated regulatory guides. The U.S. NRC, supported by cyber security experts from DOE national laboratories and U.S. universities, has undertaken efforts to develop a regulatory guide (RG), to provide an advanced reactor licensee with an acceptable approach for meeting the requirements of the proposed cyber security rule for advanced reactors, 10 CFR 73.110, "Technology neutral requirements for protection of digital computer and communication systems and networks." The RG aims to provide a process that accounts for the differing risk levels within advanced reactor technologies while providing reasonable assurance of adequate protection of public health and safety and promoting the common defense and security and protecting the environment. As such, a key RG outcome will be to provide the licensee with a risk-informed approach that would allow for the design and implementation of a cyber security program to meet demands for protection against the unacceptable consequences from a cyber attack. The RG is expected to leverage both the outcomes of the safety and security analyses performed for the associated reactor design.

1. INTRODUCTION

Current proposed ARs involve diverse technologies, and each have a unique set of functions and systems that support both nuclear safety and security. Examples of functions and systems supporting safety and security may include reactor trip, emergency core cooling, intrusion detection, and communications. To address these challenges, the U.S. Nuclear Regulatory Commission (NRC) is moving toward a risk-informed, performance-based, and technology-neutral regulation and associated RG. Section 2 below discusses the efforts associated with the development of the cyber security requirements for advanced reactors, while Section 3 discusses the efforts associated with the companion RG development. The proposed cyber security requirements and companion RG are aimed to enhance safety of the advanced reactors by: (1) protecting safety functions and systems from the adverse consequences resulting from potential cyber attacks; and, (2) ensuring that cyber security features for digital I&C safety systems at nuclear power plants are designed and implemented so that they do not compromise safety functions.

2. DRAFT CYBER SECURITY REQUIREMENTS FOR ADVANCED REACTORS

2.1. Background

The cyber security requirements for the legacy power reactors are found in Title 10 of the Code of Federal Regulations (CFR) 73.54, "Protection of digital computer and communication systems and networks" [1]. These requirements are based on the function digital assets perform. Specifically, licensees must protect digital assets associated with: (1) Safety, security, and emergency preparedness functions; and, (2) Support systems which, if compromised, could adversely impact safety, security, or emergency preparedness functions. Licensees must ensure these systems are protected from cyber attacks up to an including a Design Basis Threat that would: (1) Adversely impact integrity/confidentiality; (2) Deny access to systems, services, or data; and (3) Adversely impact operations.

2.2. Proposed New Cyber Requirements

For ARs, the NRC staff is developing a transformative regulatory framework via the development of a Title 10 of the CFR Part 53, which builds on a strong foundation of Commission policies and decisions and evolves existing requirements into a modern, risk-informed, performance-based approach. Specifically, 10 CFR Part 53 will provide technology-inclusive, risk-informed, performance-based approaches to safety that include scaling the requirements for licensing and regulating a variety of advanced reactor designs and technologies. The overall principles associated with this effort include: (1) Leveraging the best of the past and developing new tools for the future; (2) Crediting technological advancements which could provide operational flexibilities with increased margins of safety; and, (3) Prioritizing risk-informed and performance-based approaches that accommodate various advanced reactor technologies. The NRC is periodically making available the preliminary proposed rule language for public comment. The NRC staff is listening to all stakeholders and has made changes to the preliminary proposed rule language in response to stakeholder feedback.

The proposed rule will contain a new section in Part 73 titled: "Technology Neutral Requirements for Protection of Digital Computer and Communication Systems and Networks" [2] to address cyber security, which will implement a graded approach based on consequences to determine the level of cyber security protection required for digital computer and communication systems and network technologies. A graded approach based on potential consequences is intended to facilitate risk-informed approaches, results, and insights for the wide range of reactor technologies to be assessed by the NRC. The rule will recognize the more significant role that may be played by those digital computer and communication systems for future reactor designs. This proposed rule leverages the operating experience and lessons learned over the past 12 years from the power reactors' implementation of the current cyber security regulations.

As shown in FIG. 1 below, 10 CFR 73.110 will require licensees to protect systems associated with functions, such as those dealing with safety, security, and emergency preparedness, using a graded cyber security program commensurate with potential consequences from cyber attacks. The first consequence deals with radiological sabotage or scenarios where a cyber attack adversely impacts the functions performed by digital assets which may lead to offsite radiation hazards that would endanger public health and safety by exceeding established dose criteria. The second consequence deals with physical intrusion or scenarios where a cyber attack adversely impacts the functions performed by digital assets used to maintain physical security.

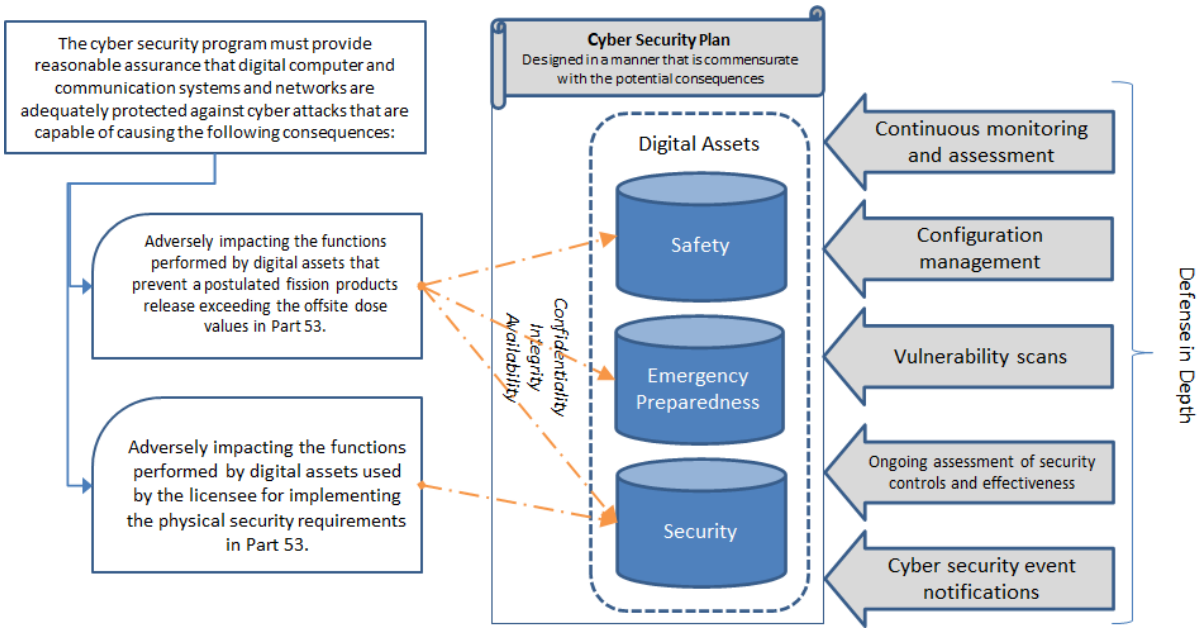


FIG. 1 New Cyber Security Approach - 10 CFR 73.110

Licensees would be required to: (1) Analyse the potential consequences resulting from cyber attacks and identify those assets that must be protected; and, (2) Establish, implement, and maintain a cyber security program, as defined in the cyber security plan, to protect the assets identified by applying defence-in-depth protective strategies to ensure the ability to detect, delay, respond, and recover from cyber attacks capable of causing the stated consequences. In addition, licensees would be required to: (1) Implement security controls commensurate with safety/security significance via a graded approach; (2) Mitigate adverse impact of cyber attacks capable of causing the stated consequences; and, (3) Ensure functions of protected assets are not adversely impacted due to cyber attacks capable of causing the stated consequences.

The NRC staff continues to develop this preliminary proposed rule, and its companion regulatory guidance discussed in Section 3 below, and seek public comments or feedback. The NRC staff plans to submit its proposed rule in February 2023 for Commission approval.

3. DRAFT RG CONCEPTS

This section discusses the companion guidance development for the new cyber security requirements being developed by the NRC staff.

3.3. Draft RG Development

The U.S. NRC, supported by cyber security experts from the Department of Energy national laboratories and U.S. universities, has undertaken efforts to develop a RG, to provide a commercial nuclear reactor under a 10 CFR Part 53 license with an acceptable approach for meeting the requirements of 10 CFR 73.110. In order to accommodate the wide range of commercial nuclear plant technologies to be assessed by the NRC under 10 CFR Part 53, a new cyber security analysis approach is being implemented via this draft RG while factoring in the following:

1. Commercial nuclear plant designs include increased reliance on digital systems, emerging technologies, passive safety features and other novel design features.

2. Novel use cases such as remote monitoring and autonomous operations are planned, which demand reassessing legacy systems isolation paradigms.

3. This effort is being informed by national and international standards and approaches supporting security concepts having a high degree of expert acceptance, including security design features, customized control catalogues and performance-based objectives.

4. The increasing capabilities of attackers, with a corresponding increase in sophistication and Operational Technology focus - dictates a broader approach to software supply chain attacks including both technical and administrative defensive measures.

This draft RG will provide an acceptable method that applies risk-informed, performance-based, technology neutral approach to account for the differing risk levels within commercial nuclear plant technologies to meet demands for protection against the unacceptable consequences from a cyber attack. This draft RG will describe, among other things, the elements required in a cyber security plan, including a cyber security plan template, and contain cyber security controls while leveraging the content in RG 5.71 guidance, “Cyber Security Programs for Nuclear Facilities,” [3] which was developed for the legacy nuclear power plants. This effort will also leverage the information from IAEA and IEC publications. The follow-on sections provide a high-level overview of the risk-informed, performance-based, technology-neutral approach concept being developed as part of this draft RG.

3.4. Three-Tier Analysis Approach

This draft RG will implement a three-tier approach via analyses at the Facility Level, Function Level, and at the System Level. At the Facility Level, the intent of the analysis is to rely on existing safety and security assessments to determine if the plant's design basis and existing physical protection systems are sufficient to effectively prevent the potential consequences from a cyber attack. At the Function Level, the intent of the analysis is to understand the adversary's access to attack pathways that allow for the compromise of plant functions resulting in the unacceptable consequences defined in 10 CFR 73.110. At the System Level, the intent of the analysis is to identify protective measures including system-level cyber security controls to prevent or mitigate the impact to compromised plant functions.

Both the Functional Level and System Level analyses will employ the use of a graded approach to determine the level of cyber security protection commensurate with potential consequences from a cyber attack. The intent of this approach is to ensure that analyses are performed until it is demonstrated that a cyber attack cannot result in the consequences listed in 10 CFR 73.110. This may result in a single tier of analysis being performed, two tiers of analysis being performed (i.e., first and second tier), or all three tiers of analysis being performed. The follow-on sections provide a more detailed explanation of how this three-tier analysis approach is being implemented in the draft RG.

3.5. Important Terminology

The analysis approach discussed herein employs the following two terms:

- CEAS: Cyber-Enabled Accident Scenario, which refers to postulated accidents that are used to assess the potential radiological sabotage consequences resulting from a cyber attack. The CEAS development leverages the safety-related analysis performed for a given advanced reactor design.

- CEIS: Cyber-Enabled Physical Intrusion Scenario, which refers to postulated scenarios that are used to assess the potential physical intrusion consequences that are enabled or result from a cyber attack. In other words, the assessment of CEIS allows for insights into mitigations to cyber attacks associated with the potential to result in unacceptable physical intrusion consequences.

3.6. Overview of Draft RG Performance-based/Risk Informed Approach

The analysis approach shown in FIG. 2 through FIG. 4, which is being implemented as part of the RG development, is intended to ensure that only systems that perform or rely upon functions that can contribute to the 10 CFR 73.110 consequences are assessed and protected.

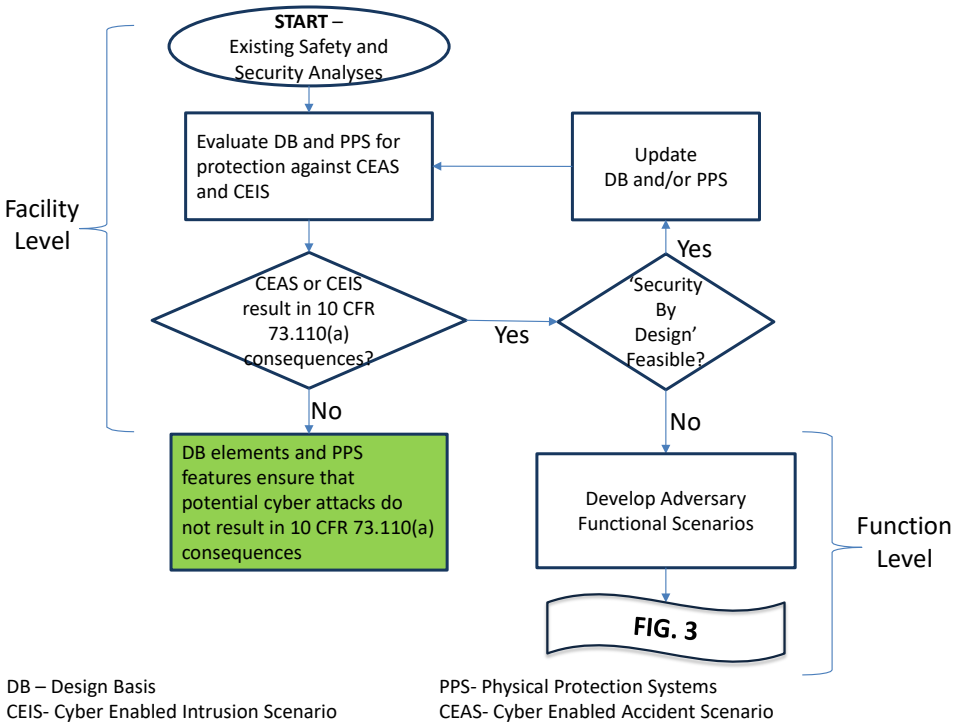


FIG. 2. Performance-based/Risk Informed Analysis Approach – Part 1.

As part of the Facility Analysis listed in FIG. 2 above, the existing results of safety and security assessments are used to analyse the impact of the loss or compromise of a plant function resulting in the unacceptable consequences defined in 10 CFR 73.110. The focus for this portion of the risk assessment is to evaluate potential cyber attack consequences considering the plant design basis and physical protection system. CEAS and CEIS, or the two terms discussed in Section 3.5 above, help identify those cyber security sequences of scenarios linked or having the potential to result in the consequences defined in 10 CFR 73.110 that must be protected against potential cyber attacks.

If a cyber attack results in the 10 CFR 73.110 consequences then, enhancements or improvements to the design basis and/or physical protection system mitigations should be considered, if allowed by a 'Security by Design' approach. A 'Security by Design' approach refers to the considerations for safety and security requirements together in the design process such that security issues (e.g., newly identified threats of adversary attacks) can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with no or minimal reliance on human actions. If a cyber attack does not result in the 10 CFR 73.110 consequences then, the licensee documents the design basis elements and physical protection system features which ensure that potential cyber attacks do not result in those consequences.

If the preceding analysis shows that a cyber-enabled scenario results in the 10 CFR 73.110(a) consequences and 'Security by Design' is not feasible then, the licensee proceeds with the Function Level Analysis or the next tier of analysis by developing Adversary Functional Scenarios as shown in FIG. 3, which is aimed at managing functional risks. The intent of this analysis is to assess whether and how an adversary can affect the functions via a cyber attack, thus leading to radiological sabotage or physical intrusion scenarios that result in unacceptable consequences.

Based on the outcome of the Adversary Functional Scenarios, the licensee is able to manage functional risks by specifying prohibitive Cyber Security Plan elements, such as prohibiting the use of wireless for certain plant applications, and passive/deterministic Defensive Cyber Security Architecture elements, such as a data diode, to protect against from cyber attacks. The Adversary Functional Scenario Analysis helps identify incident scenarios to inform design, development, and implementation of Defensive Cyber Security Architecture and other common, facility-wide elements that provide a plant capability (e.g., resilience) that can be leveraged to provide

protection against cyber attacks, specifically, those associated with unacceptable consequences as defined in 10 CFR 73.110.

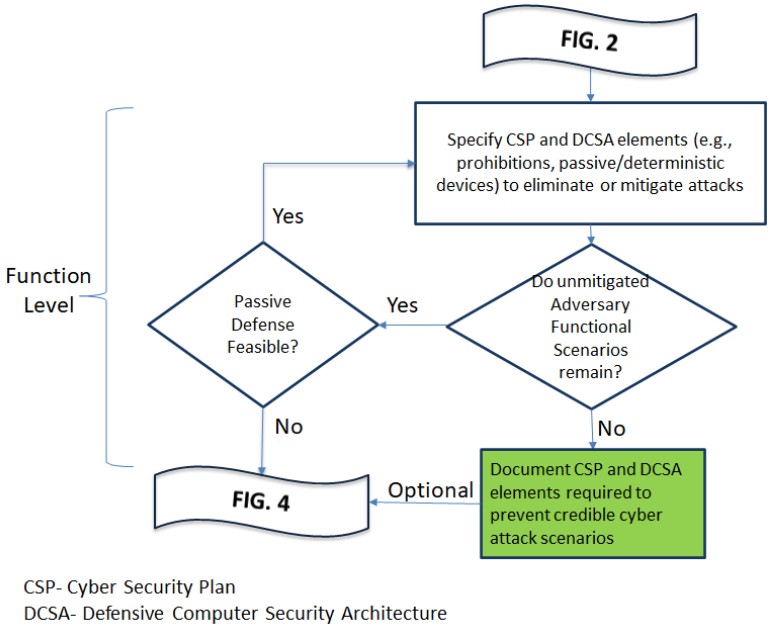


FIG. 3. Performance-based/Risk Informed Analysis Approach – Part 2

If the analysis results reveal that there any remaining unmitigated adversary functional scenarios and the implementation of passive defence features, such as those discussed herein are not feasible then, the licensee proceeds to perform the System Level or the third tier analysis as shown in FIG. 4 below. For cases where there are no remaining unmitigated adversary functional scenarios, proceeding with the next tier of analysis would be optional as licensees may decide to do so to increase or further enhance their defence-in-depth posture against cyber attacks.

As part of the System Level analysis depicted in FIG. 4, the licensee needs to identify the critical functions and associated systems via the use of a graded approach. Critical functions are those that are associated with a CEAS or CEIS. Critical Systems may be categorized into most critical or least critical allowing for a graded approach to be applied in the selection and implementation of cyber security control measures.

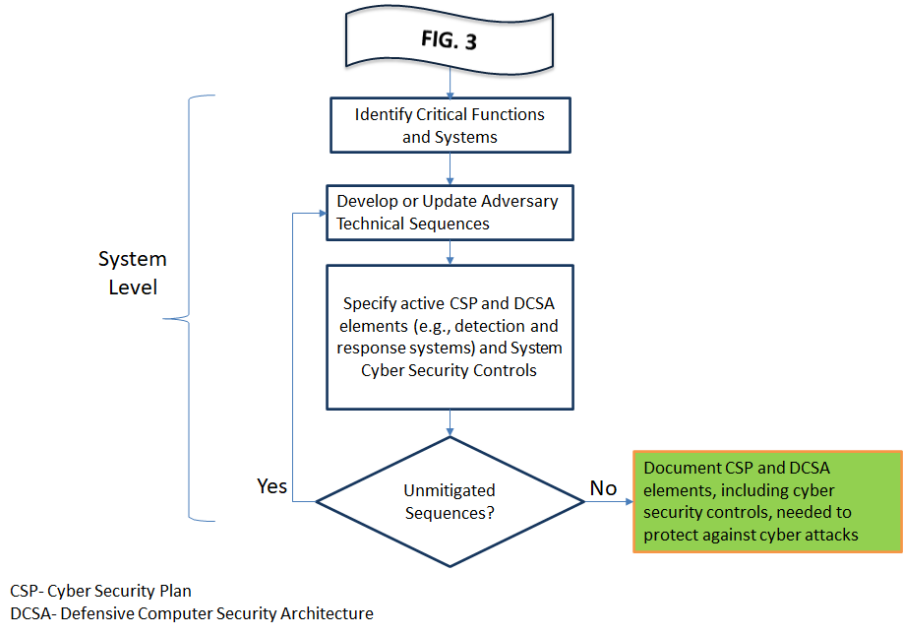


FIG. 4. Performance-based/Risk Informed Analysis Approach – Part 3

Adversary Technical Sequences are sequences of adversary tactics, techniques, and procedures that the licensee should protect against. Frameworks such as MITRE ATT&CK [4] can be used to develop Adversary Technical Sequences that are consistent and reproducible. The outcome of the Adversary Technical Sequences approach helps identify cyber security control measures and controls on system design and operation to protect critical function(s) via the application of a graded approach and implementation of defense-in-depth approaches for prevention, detection, and response against cyber attacks.

As shown in FIG. 4, this iterative analysis proceeds until all Adversary Technical Sequences are mitigated. Once this objective is achieved, the licensee would need to document the Cyber Security Plan and Defensive Cyber Security Architecture elements, including cyber security controls, needed to protect against cyber attacks.

3.7. Future Work

In terms of the future work associated with the proposed cyber requirements and its companion RG, the NRC staff plans to continue working on topics for inclusion in the document such as: (1) Developing sample Accident and Physical Intrusion scenarios; (2) Providing guidance for using a performance-based approach for the selection of cyber security measures; and, (3) Providing specific guidance for emerging technologies such as remote operation of reactors, and autonomous operation. These efforts will support finalizing the proposed cyber requirements and draft RG for inclusion in the Part 53 rulemaking package to be submitted in February 2023 for Commission approval.

REFERENCES

[1] U.S. Code of Federal Regulations (CFR) 73.54, “Protection of digital computer and communication systems and networks,” Title 10, “Energy,” (2009), https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

[2] U.S. CFR, “Physical Protection of Plants and Materials,” Part 73, Section 110, “Technology neutral requirements for protection of digital computer and communication systems and networks,” Title 10, “Energy,” (2022), https://www.nrc.gov/docs/ML2212/ML22125A000.pdf.

[3] U.S. NRC RG 5.71, “Protection of Digital Computer and Communication Systems and Networks,” (2010), https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

[4] MITRE Corporation, “MITRE ATT&CK for Industrial Control Systems: Design and Philosophy,” (2020), https://attack.mitre.org/.

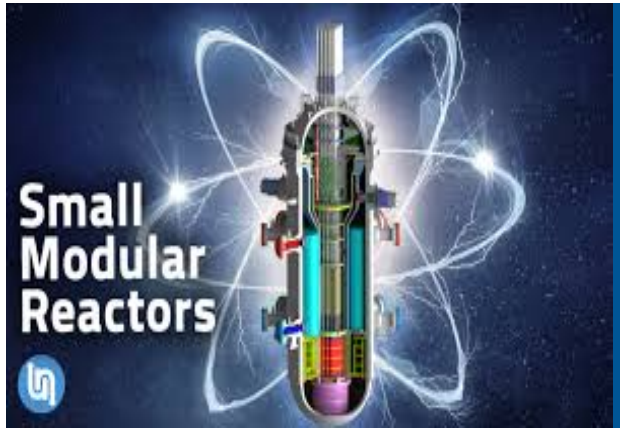
International Conference on
Topical Issues in Nuclear Installation Safety: Strengthening Safety or Evolutionary and Innovative Reactor Designs
18-21 October 2022

U.S.A. Regulatory Efforts for Cyber Security of Advanced Reactors

Juris Jauntirans
Cyber Security Specialist
U.S. Nuclear Regulatory Commission

Ismael Garcia
Senior Level Advisor, Cyber Security and Digital Instrumentation and Control
U.S. Nuclear Regulatory Commission

Michael T. Rowland
Sandia National Laboratory



Draft Cyber Security Requirements for Advanced Reactors

Background – Power Reactors Cyber Requirements

- Found in 10 CFR 73.54
- Protect digital assets that perform specified functions
- Protect from cyber attacks up to an including a Design Basis Threat

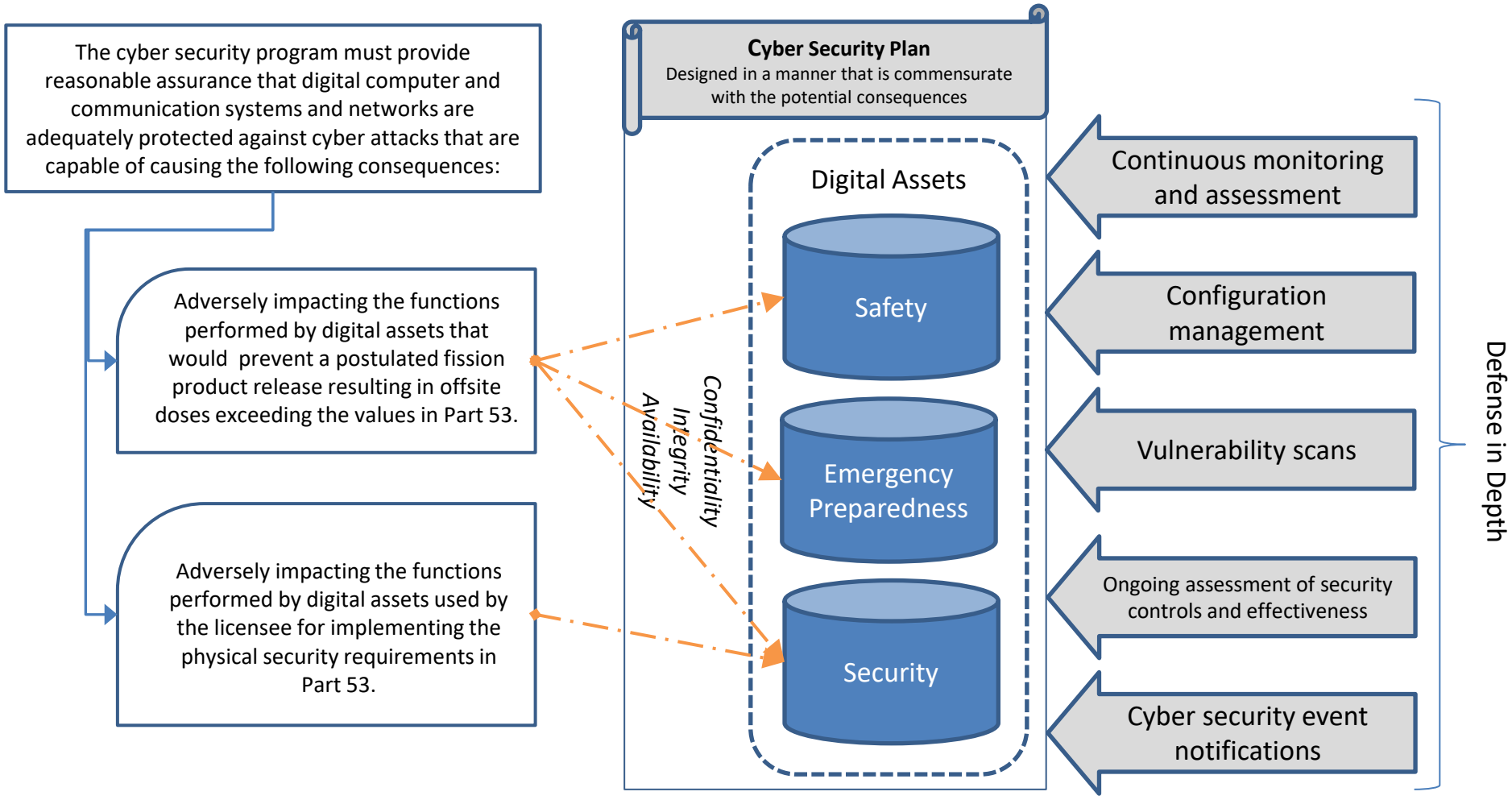
Proposed New Cyber Requirements

10 CFR Part 53 development for Advanced Reactors

Preliminary Proposed Rule Language Publicly Available

New Cyber Requirements in Proposed Rule

Preliminary Proposed Cyber Requirements



Reference: Part 73.110, "Technology Neutral Requirements for Protection of Digital Computer and Communication Systems and Networks," ADAMS Accession Number : ML22125A000

10 CFR 73.110 – Draft Regulatory Guide Concepts

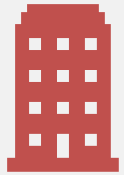
Draft Regulatory Guide Development

An acceptable approach for meeting the 10 CFR 73.110 requirements

Effective guidance to support a performance-based regulatory framework

Leverage IAEA and IEC security approaches

Draft Regulatory Guide – Three-Tier Analysis Approach



Facility Level

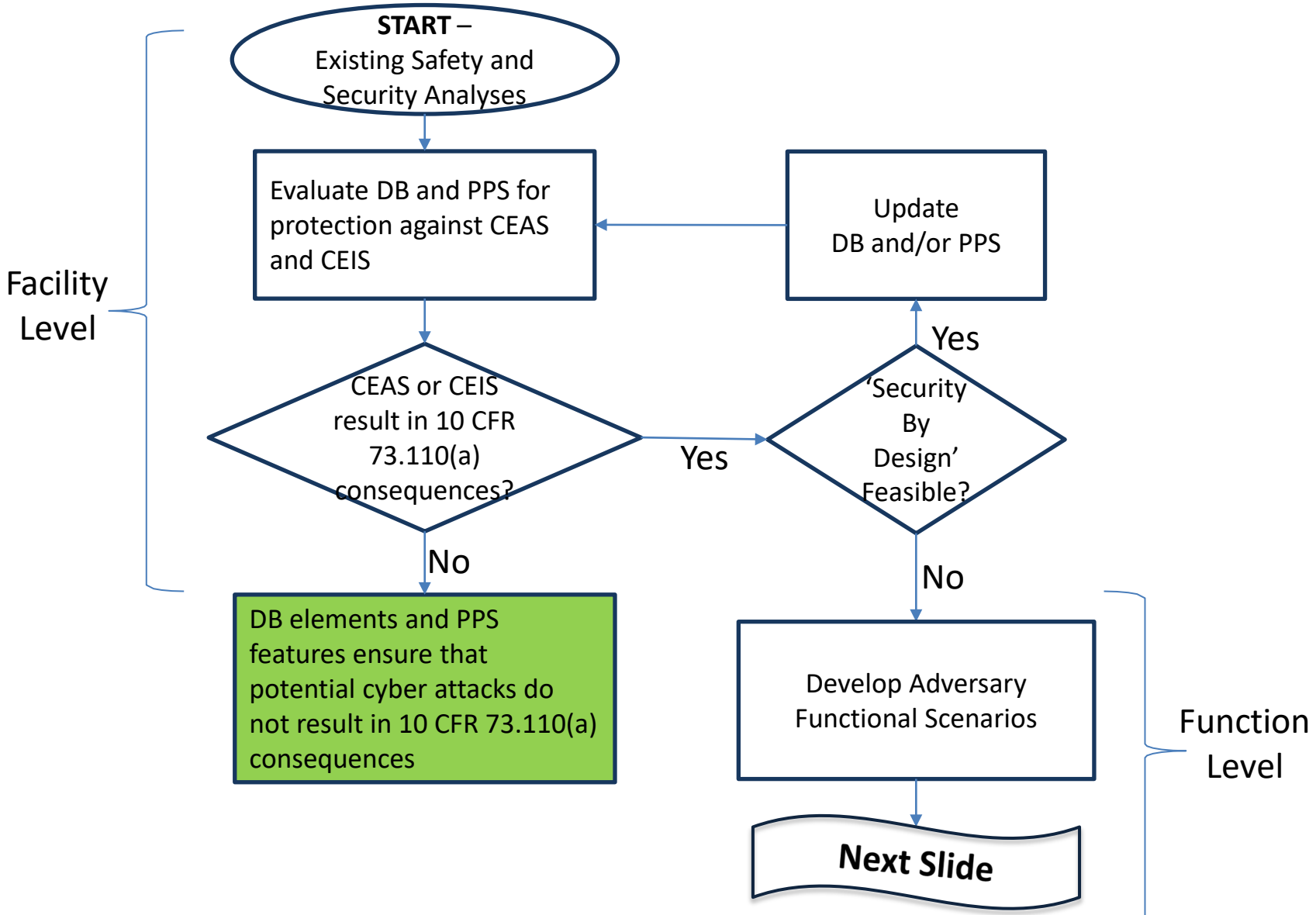
Function Level

System Level

Important Terminology

- CEAS: Cyber-Enabled Accident Scenario
- CEIS: Cyber-Enabled Intrusion Scenario

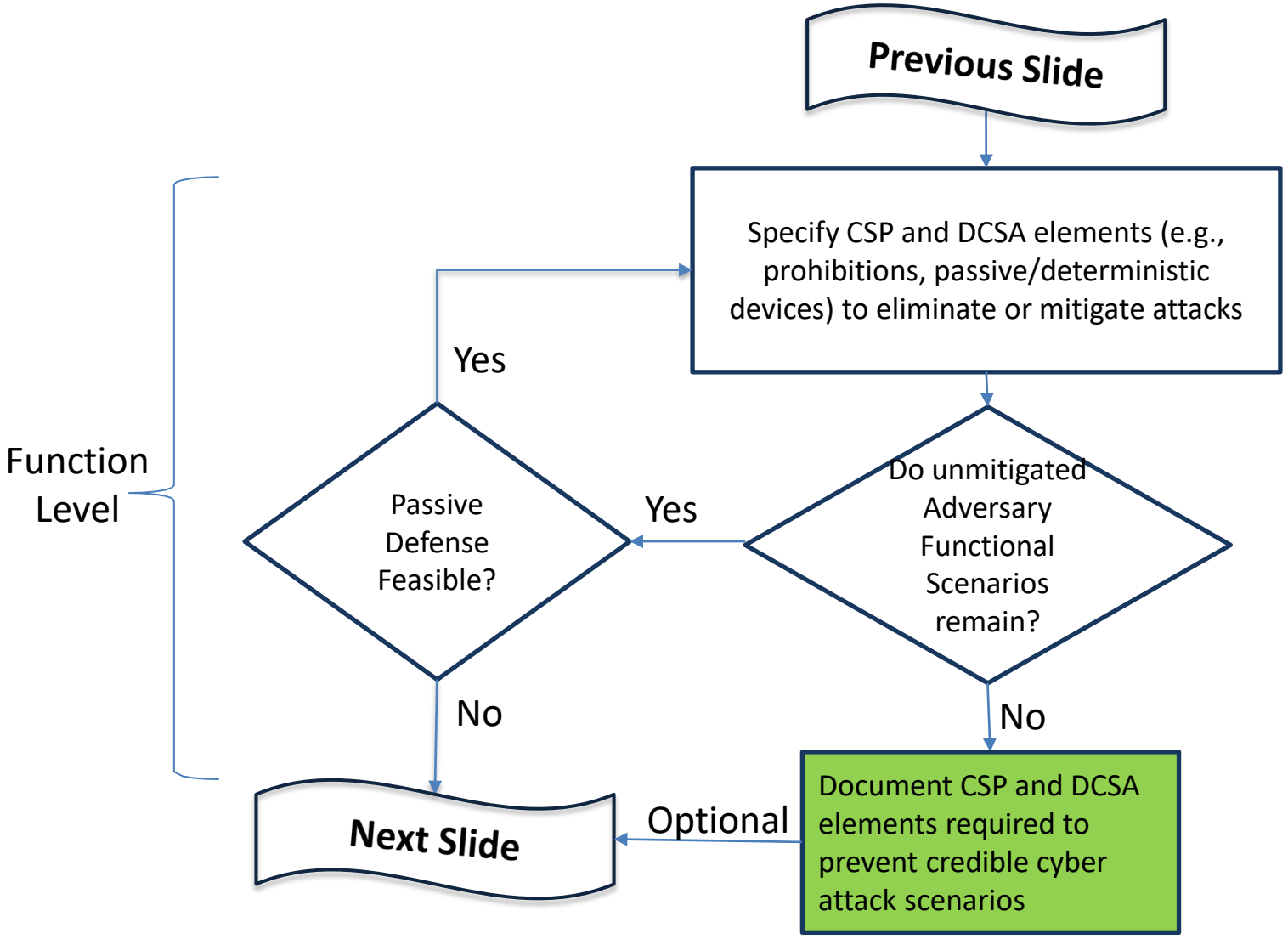
Overview of Draft Regulatory Guide Performance-based/Risk Informed Approach



DB – Design Basis
CEIS- Cyber Enabled Intrusion Scenario

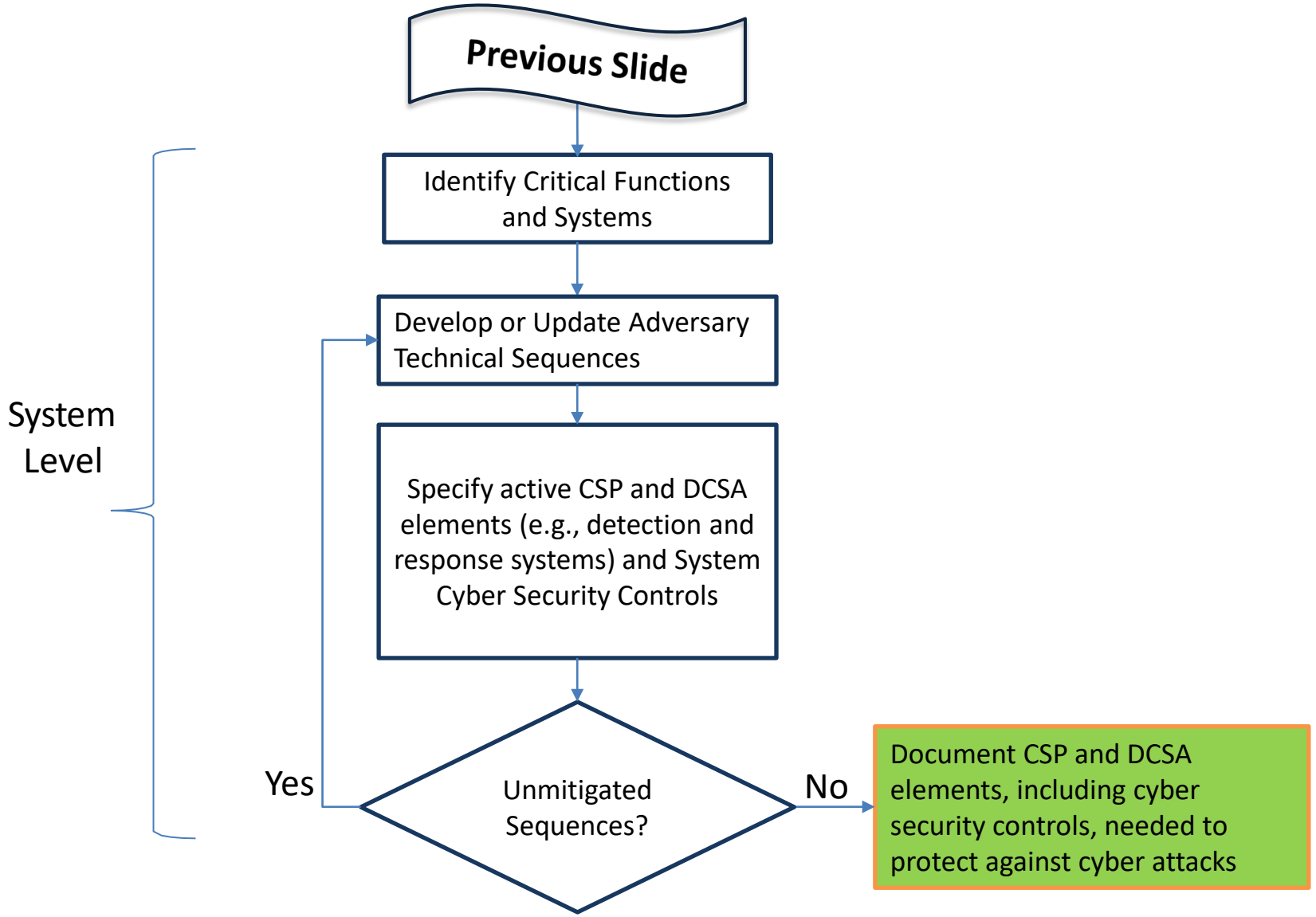
PPS- Physical Protection Systems
CEAS- Cyber Enabled Accident Scenario

Overview of Draft Regulatory Guide Performance-based/Risk Informed Approach (Cont.)



CSP- Cyber Security Plan
DCSA- Defensive Computer Security Architecture

Overview of Draft Regulatory Guide Performance-based/Risk Informed Approach (Cont.)



CSP- Cyber Security Plan
DCSA- Defensive Computer Security Architecture