NUCLEAR ENERGY AGENCY'S CONSENSUS POSITION ON THE IMPACT OF CYBER SECURITY FEATURES ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY AT NUCLEAR POWER PLANTS – EVALUATION FRAMEWORK

I. GARCIA[1]

[1]U.S. Nuclear Regulatory Commission (NRC), Rockville/Maryland, U.S.A.

Abstract

A cyber security feature is a provision, control, or function specifically designed for cyber security purposes. Cyber security features and safety functions are implemented in digital Instrumentation and Control (I&C) systems at nuclear power plants to protect against cyber attacks and protect the plant from postulated initiating events, respectively, that could compromise safety. Specifically, cyber security features are implemented for the protection of digital I&C systems against unauthorized access. The safety functions and cyber security features should be designed and implemented to prevent them from compromising one another. The paper documents an evaluation framework intended to apply to all digital I&C systems important to safety, both hardware and software, and was derived from the ongoing work being performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC). The framework addresses the following areas associated with the platform qualification: (1) Cyber security requirements and safety requirements; (2) Qualification of cyber security features; (3) Vulnerabilities Assessment; and, (4) Maintenance and operational considerations. The methodology discussed by the paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators; instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not compromise one another.

1. INTRODUCTION

Cyber security seeks to prevent unauthorized accesses to information, software, and data in order to ensure that three attributes are met, namely: (1) The prevention of disclosures or access of information that could be used to perform malicious or misguided acts which could lead to an accident, an unsafe situation or plant performance degradation (confidentiality); (2) The prevention of unauthorized modifications that degrade a safety function (integrity); and, (3) The prevention of unauthorized withholding of information, data, or resources that could compromise performance of a safety function (availability) [1]. A cyber security feature is a provision, control, or function specifically designed for cyber security purposes [1]. Cyber security features and safety functions are implemented in digital Instrumentation and Control (I&C) systems at nuclear power plants to protect against cyber attacks and protect the plant from postulated initiating events, respectively, that could compromise safety. Specifically, cyber security features are implemented for the protection of digital I&C systems against unauthorized access. The safety functions and cyber security features should be designed and implemented to prevent them from compromising one another.

The paper documents an evaluation framework intended to apply to all digital I&C systems important to safety, both hardware and software, and was derived from the ongoing work being performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC). In this context, hardware includes industrial digital devices of limited functionality, for example, while software includes firmware and logic in any form, including supporting data; this includes, but is not limited to application, operational and pre-existing software and software tools, intellectual property cores, field programmable gate arrays, complex programmable logic devices, network equipment, and items intended for non-safety purposes with the potential to interfere with safety systems.

Security can also be compromised through supply chains, which are getting longer, more complex and more difficult to control. Therefore, the evaluation framework discussed herein may be applied to hardware and

software used along the supply chain that can affect the safety function, including items on which the supply chain products and services depend. This includes items used by contractors, vendors, technical support organizations and any other service provider. Relevant supply chain activities include software upgrades, patching, analysis using external tools, testing, system modifications, and transportation. .

2. DEFINITION OF TERMS

The following definitions are specific to the paper:

- Cyber attack: Attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Cyber attacks include targeted and non-targeted (e.g. malwares) attacks by digital means [1].

- Cyber security feature: Provision, control, or function specifically designed for cyber security purposes [1].

- Cyber security: Seeks to prevent unauthorized accesses to information, software and data in order to ensure that three attributes are met, namely: (1) The prevention of disclosures or access of information that could be used to perform malicious or misguided acts which could lead to an accident, an unsafe situation or plant performance degradation (confidentiality); (2) The prevention of unauthorized modifications that degrade a safety function (integrity); and, (3) The prevention of unauthorized withholding of information, data or resources that could compromise performance of a safety function (availability) [1][2].

- Control of access: The administrative control of access to safety system equipment, supported by provisions within the safety systems (access controls), by provision in the plant design (physical security) or by a combination thereof [3][4].

- I&C system: System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself [5].

- Item important to safety: An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or member of the public [6].

- Platform: Set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An I&C platform usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software [7].

- Qualification: Process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements [7]. (Note: Qualification of I&C systems is a plant- and application-specific activity while platform qualification relies to a large degree on qualification activities performed outside the framework of a specific plant design.)

- Security degree: Gradation of security protection with associated sets of requirements, assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance [8].

• Security zone: Concept for grouping computer-based I&C systems for administration, communication and application of protective measures [8].

• Threat: Potential cause of an unwanted incident, which may result in harm to a system or organization. Threats can involve items on which the safety function depends (components, supply chain and supporting systems or components). These threats use a variety of techniques such as: (1) Unauthorized access through items on which the safety function depends; (2) Unauthorized influence (such as provision of false information); (3) Unauthorized access or modification through supporting activities; and, (4) Other techniques identified by the licensee and/or the regulatory authority [8].

• Vulnerability: Feature, attribute, or weakness in a system's design, implementation, or operation and management that could render a critical digital asset open to exploitation or safety, security, and emergency preparedness function susceptible to adverse impact [9].

3. EVALUATION FRAMEWORK

FIG. 1 below shows the evaluation framework for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not compromise one another. As shown in FIG. 1, the framework addresses the following areas:

1. Cyber security requirements and safety requirements;
2. Vulnerabilities and threats assessments;
3. Qualification of cyber security features; and,
4. Maintenance and operational considerations.

Sections 3.1 through 3.5 below discuss some of the key takeaways from this framework. Specifically, these sections discuss the kind of information and considerations associated with the cyber security features for digital I&C systems that would need to be assessed as part of the evaluation. The acceptability of the overall evaluation of such cyber security features will be a matter for the regulatory body for the country in which the digital I&C systems are to be used.

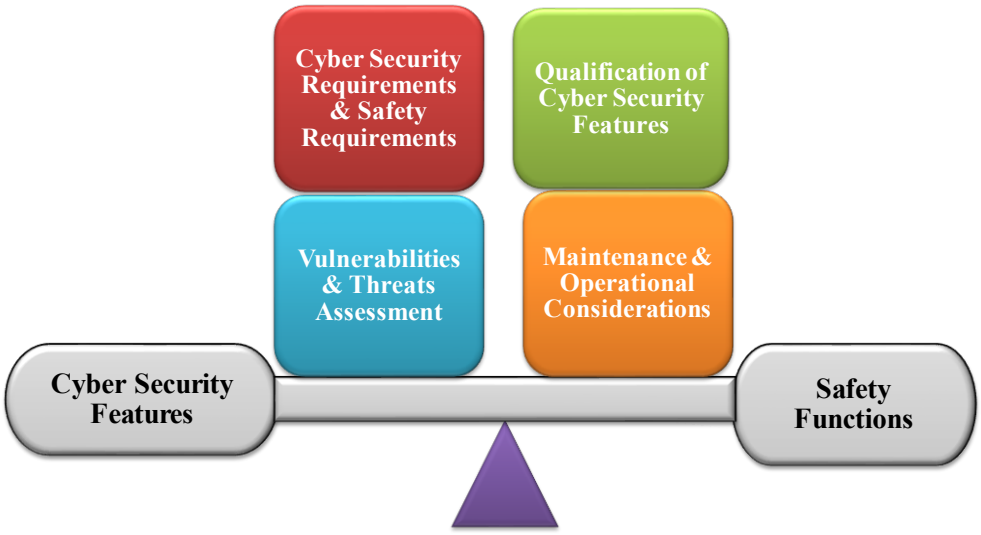


FIG. 1 Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants – Evaluation Framework

3.1. Cyber Security Features

A cyber security feature is a provision, control, or function specifically designed for cyber security purposes [1]. Cyber security features for digital I&C systems important to safety should be carefully evaluated and technically justified. Cyber security features should not adversely impact the required performance, effectiveness, reliability, or operation of safety functions. Therefore, the addition of cyber security features requires an evaluation to assess whether the gain in security from the features is worth any increase in complexity in the system, as well as accounting for any potential new failure modes that could be introduced due to the addition of such features. Examples of technical areas that would need to be addressed during such evaluation include:

1. Where cyber security features need to be implemented in displays and controls for digital I&C systems important to safety, they should not adversely impact the operating personnel's ability to maintain the safety of the plant; and,
2. A cyber security feature, when activated, should not inhibit, override or deactivate safety functions. For example, an antivirus software could unintentionally block or hinder the functionality of a digital I&C system important to safety.

3.2. Cyber Security Requirements and Safety Requirements

The architecture of individual I&C systems includes the allocation of system design requirements to functional units (e.g., divisions, processing units, human-system interfaces) and specifies the interactions between the functional units (e.g., communication links). The architecture design should factor in, among other things, the means for addressing the risk associated with remote electronic access to in-plant systems and networks from sources external to the plant. Design approaches and cyber security controls should ensure that digital I&C communication systems and networks are adequately protected against the potential hazards from physical and electronic access without adversely affecting the reliability and robustness of the systems [9]. Examples of design approaches and cyber security controls in the field of digital I&C systems communications include:

1. Data transmission between systems of different safety classes and security degrees should meet the constraints imposed by the appropriate industry standards [10]; and,
2. Secure control of communication pathways between a digital I&C system important to safety and any system external to the I&C architecture (e.g., the enterprise network) should be established.

As such, the architecture design for digital I&C systems important to safety should support both safety and cyber security objectives as reflected by the corresponding requirements. Specifically, cyber security requirements and safety requirements should be developed in a coordinated manner for the digital I&C systems under development throughout its lifecycle. This coordination should include, but not be limited to safety and cyber security demonstration, roles and responsibilities, policies, processes and procedures, plans, assurance and the management and content of operational and maintenance procedures. Such an approach avoids design-related issues such as the following:

1. Avoiding designs that will be difficult or impossible to adequately protect after their implementation; and,
2. Introducing new cyber security requirements later in the system development lifecycle, as they could introduce unintended consequences or vulnerabilities.

Therefore, requirements, including constraints, should be specified and controlled for cyber security features throughout the lifecycle (including system recovery) to protect against credible threats with the potential to degrade a safety function, based on the consequences of a successful cyber attack. Furthermore, requirements, including constraints, should be formulated to protect against intrusion or unauthorized modification during supporting activities such as testing, calibration (including update of calibration data), configuration, modification, loading software, other maintenance activities, and documenting the associated management activities. Sample technical areas that should be addressed by the requirements include:

1. Restricting or limiting access during the development, testing, use, and modifications of software development;
2. Protecting communication content;

3. Checking the software integrity (e.g., comparing software or data against its original source, stored independently);
4. Limiting interfaces and interactions;
5. Preventing unauthorized modifications;
6. Protecting boundaries between different security zones, by both logical and physical means; and,
7. Appropriately assessing procedures and equipment for transportation.

During the formulation of requirements, physical, logical, and administrative control of access to digital I&C systems important to safety should be included in the design (e.g., password or key lock access), while ensuring that they do not adversely impact the required performance, effectiveness, reliability, or operation of safety functions. Since security is continuously evolving, the effect on safety of any changes in cyber security features, including new security requirements, should be continuously evaluated. As such, cyber security requirements and safety requirements should be verified and validated throughout the lifecycle; thereby, providing assurance that both are implemented and coordinated correctly.

3.3. Qualification of Cyber Security Features

Cyber security features protecting digital I&C systems important to safety should be developed and/or qualified to the same level of safety classification as the system these features will secure. If not, evidence should be presented that the cyber security features cannot adversely affect the safety function. Any cyber security aspects not addressed during the qualification of a digital I&C platform to be used in systems important to safety need to be addressed during the system implementation [11].

Security testing and analysis (e.g., fuzz testing of network communication protocols, source code analysis) should be performed as part of the qualification exercise to identify if vulnerabilities are present in the system. Security testing and analysis should be done at the appropriate stage of the design or qualification and as early as possible. Any security testing from digital I&C systems installation onwards that could impact the safety functions should be avoided.

3.4. Vulnerabilities and Threats Assessments

Vulnerabilities can result from operational and resource requirements imposed by the safety systems or functions, but also from a poor development process, inadequate application of pre-developed software, or from infection with malware. All known vulnerabilities should be analyzed using a graded approach and mitigated either through eliminating the vulnerability or by requiring adequate protection by implementing a series of security controls [8][9].

To the extent feasible, digital I&C systems important to safety should not include design features that create vulnerabilities to known cyber threats. When included, these design features must offer a clear safety benefit and the designer should consider alternate or compensating measures to mitigate any resulting vulnerabilities [9]. Potential cyber security vulnerabilities should be considered for all software and hardware and during all stages of its lifecycle, including system's operation, maintenance, and modification.

3.5. Maintenance and Operational Considerations

Maintenance and/or operating conditions may require removing cyber security features or controls. Therefore, maintenance and operational procedures should contain the instructions for removing cyber security controls, applying any alternate cyber security controls, re-establishing the cyber security controls following maintenance, and confirming that the cyber security controls are effectively back in service (e.g., through post maintenance activities such as testing), as necessary.

To support a proactive safety management approach, nuclear power plants are enhancing the operating experience feedback processes by collecting more information on occurrences that are useful to address the early signs of declining performance and improve operational safety performance [12]. The establishment of an

effective tracking, monitoring, and reporting process may be used to streamline such efforts and ensure that major incidents and latent weaknesses are being addressed and that operating experience is treated according to its significance. Therefore, any event tracking, monitoring, and reporting process should also include events concerning adverse interactions between security and safety during operations. Such information could be used, for example, in support of modifying the cyber security features to ensure that they do not compromise the safety functions.

While operating experience alone does not provide enough evidence for the safety and security justification of a digital I&C system important to safety, it may provide, with proper documentation and under certain conditions, supporting evidence when applying this evaluation framework. Therefore, operating experience on cyber security features can provide valuable insights and should be considered during the evaluation. Such valuable insights could be factored into the cyber security training program. Specifically, the cyber security training should consider the appropriate level of knowledge, skills and experience to ensure that safety functions and cyber security features do not adversely affect one another.

4. CONCLUSIONS

There may be different approaches for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not compromise one another. The paper does not prescribe a particular approach but instead, provides a sample framework for ensuring that such an objective is met. Nonetheless, the approach taken for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not compromise one another should be justified for suitability for the particular important to safety application.

The methodology discussed by the paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators. Instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not compromise one another.

ACKNOWLEDGEMENTS

The paper was derived from the ongoing work being performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC), which I have the honor and privilege to serve as the Chairman. Specifically, the WGDIC is in the process of revising a previously published position [13] to address technical developments in the field of cyber security and safety. For additional information concerning the NEA/CNRA WGDIC visit: https://www.oecd-nea.org/nsd/cnra/.

(Note: The goal of the NEA/CNRA WGDIC is not to independently develop new regulatory standards. As such, the technical work develop by the NEA/CNRA WGDIC is not legally binding and do not constitute additional obligations for the regulators or the licensees. Instead, the technical work resulting from the NEA/CNRA WGDIC constitutes guidelines, recommendations, or assessments that the NEA/CNRA participants agree are good to highlight during their safety reviews of operating and new reactors. The development of technical guidance for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants follows the WGDIC examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents.)

REFERENCES

[1] International Electrotechnical Commission (IEC), "IEC 62859, Instrumentation and control systems – Requirements for coordinating safety and cybersecurity," https://webstore.iec.ch/publication/26131 (2016).

[2] Regulators Task Force on Safety Critical Software, "Regulators Task Force on Safety Critical Software (TF SCS), Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations," https://www.nrc.gov/reading-rm/doc-collections/nuregs/agreement/ia0463/index.html (2015).

[3] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Std. 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," https://standards.ieee.org/standard/603-2018.html (2018).

[4] IEEE, "IEEE Std. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," https://standards.ieee.org/standard/7-4_3_2-2016.html (2016).

[5] IEC, "IEC 61513: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," https://global.ihs.com/doc_detail.cfm?document_name=IEC%2061513&item_s_key=00378381 (2011).

[6] International Atomic Energy Agency (IAEA), "IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection," https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition (2018).

[7] IEC, "IEC 63084 TR: Nuclear power plants – Instrumentation and control important to safety – Platform qualification for systems important to safety," https://webstore.iec.ch/publication/34127 (2017).

[8] IEC, "IEC 62645, Nuclear Power Plants Instrumentation and Control Systems – Requirements for Security Programs for Computer-based Systems," https://webstore.iec.ch/publication/32904 (2019).

[9] U.S. Nuclear Regulatory Commission (NRC), "U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities," https://www.nrc.gov/docs/ML0903/ML090340159.pdf (2010).

[10] Nuclear Energy Agency (NEA), "NEA/CNRA/R(2019)2, CP-04, "Data Communication Independence," https://www.oecd-nea.org/jcms/pl_21460 (2018).

[11] NEA, "NEA/CNRA/R(2018)3, CP-14, Qualification of I&C Platforms for Use in Systems Important to Safety," https://www.oecd-nea.org/jcms/pl_21460 (2018).

[12] IAEA, "IAEA-TECDOC-1581, Best Practices in Identifying, Reporting and Screening Operating Experience at Nuclear Power Plants," https://www-pub.iaea.org/MTCD/Publications/PDF/TE_1581_web.pdf (2007).

[13] NEA, "Generic Common Position DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems," https://www.oecd-nea.org/mdep/common-positions/dicwg_8_rev_f.pdf (2012).

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

Nuclear Energy Agency's Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants – Evaluation Framework

Ismael L. Garcia
Senior Technical Advisor
Cyber Security and Digital Instrumentation & Control
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission (NRC)
Email: Ismael.Garcia@nrc.gov

Acknowledgements

- The evaluation framework discussed herein was derived from the ongoing work being performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC)

- For additional information concerning the NEA/CNRA WGDIC visit: https://www.oecd-nea.org/jcms/pl_21460/working-group-on-digital-instrumentation-and-control-wgdic

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Outline

- Introduction
- Evaluation Framework
  - Cyber Security Requirements and Safety Requirements
  - Vulnerabilities and Threats Assessment
  - Qualification of Cyber Security Features
  - Maintenance and Operational Considerations
- Closing Remarks/Take-aways

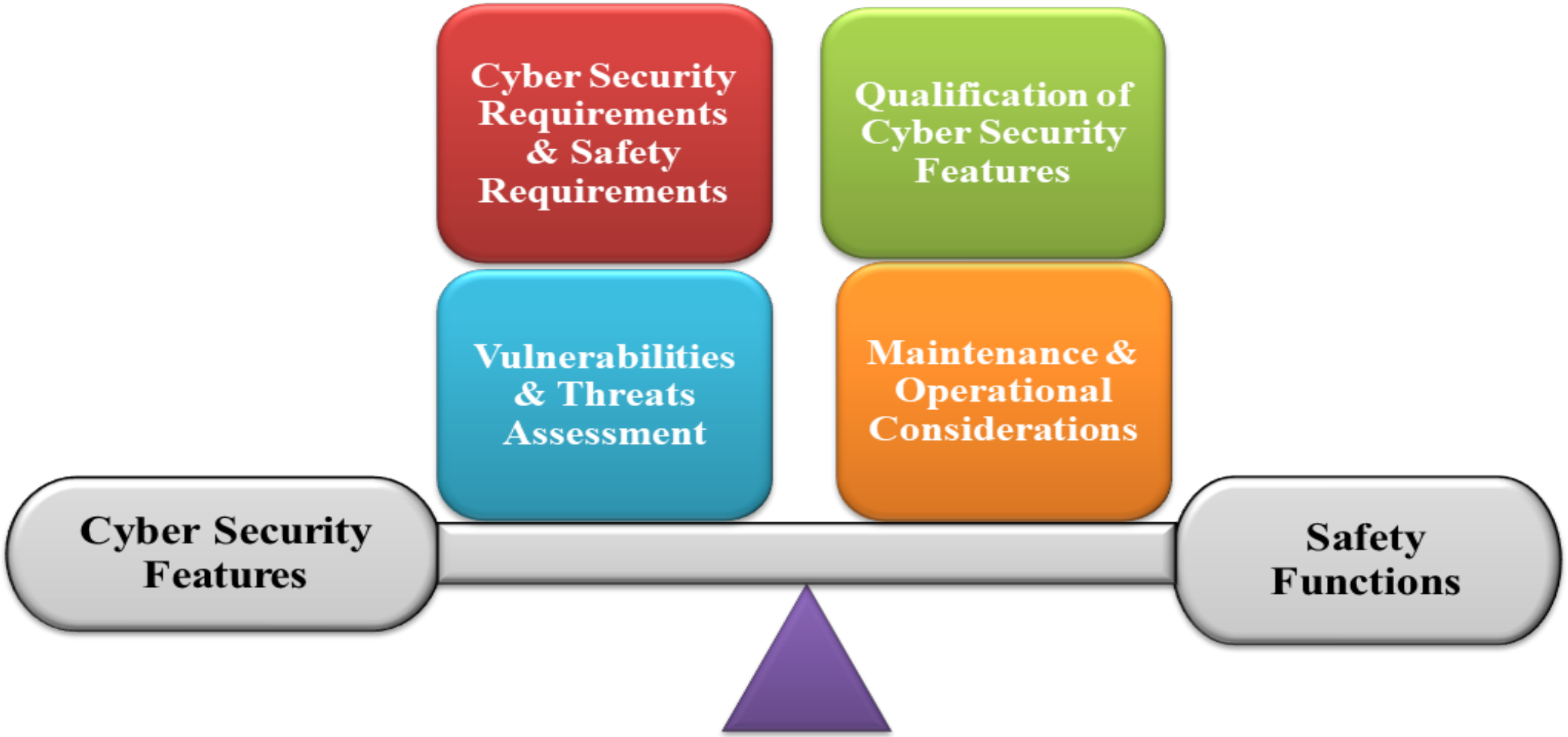
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Introduction

- Cyber security seeks to prevent unauthorized access to information, software, and data
- Safety functions and cyber security features should be designed and implemented in digital Instrumentation and Control (I&C) systems at nuclear power plants to prevent them from compromising one another
- The evaluation framework discussed herein applies to all digital I&C systems important to safety, both hardware and software

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Evaluation Framework



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Evaluation Framework – Cyber Security Requirements and Safety Requirements

- Cyber security/safety requirements should be developed in a coordinated manner for the digital I&C systems under development throughout their lifecycle
- Requirements and constraints should be:
  - Specified and controlled for cyber security features throughout the equipment lifecycle
  - Formulated to protect against intrusion or unauthorized modification
- Physical, logical, and administrative control of access to digital I&C systems important to safety should be included in the design

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Evaluation Framework – Qualification of Cyber Security Features

- Development/qualification of cyber security features should be at the same level of safety classification as the digital I&C systems these features will secure
- Security testing and analysis should be performed:
  - As part of the qualification exercise
  - At the appropriate stage of the design or qualification
- Any security testing from digital I&C systems installation onwards that could impact the safety functions should be avoided

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Evaluation Framework – Vulnerabilities & Threats Assessment

- All known vulnerabilities should be analyzed and mitigated
- Digital I&C systems important to safety should not include design features that create vulnerabilities to known cyber threats
- Potential cyber security vulnerabilities should be considered for all software and hardware and during all stages of the equipment lifecycle

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Evaluation Framework – Maintenance and Operational Considerations

- Maintenance and operational procedures should contain the instructions for actions such as
  - Removing cyber security controls
  - Applying any alternate cyber security controls
- Track/monitor events concerning adverse interactions between security and safety during operations
- The cyber security training should help ensure that safety functions and cyber security features do not adversely affect one another

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Closing Remarks/Take-Aways

- There may be different approaches for achieving the stated objective
- The approach taken should be justified for suitability for the important to safety application
- The methodology discussed herein is not to be construed as a requirement or regulation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment