INL/MIS-21-61982-Revision-0

Cyber Risk Considerations for Nuclear Digital I&C Systems

January 2024

Shannon Leigh Eggers

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-21-61982-Revision-0

Cyber Risk Considerations for Nuclear Digital I&C Systems

Shannon Leigh Eggers

January 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CHAPTER 5

Cyber risk considerations for nuclear digital I&C systems

Shannon L. Eggers
Idaho National Laboratory, Idaho Falls, ID, United States

Contents

5.1 Introduction

All but two of the operational nuclear power reactors in the United States began commercial operation prior to 1997 [1]. Since most of these reactors were designed with the 1960s and 1970s technology, modernization efforts are underway to replace analog instrumentation and control (I&C) systems with digital equipment. Additionally, it is anticipated that new advanced reactors (e.g., generation III+ and IV reactors, small modular reactors, and microreactors) will rely primarily on digital I&C. Traditional plant safety analysis (i.e., probabilistic risk analysis (PRA)) relies on known historical data for functional failure and accident analysis. However, while traditional nuclear PRAs often model the failure of an operator to perform an action required in an abnormal or emergency procedure, PRAs have limitations in modeling other unintentional or deliberate human actions. Additionally, it is challenging to model digital device failures in a PRA as these devices can fail by unexpected means.

https://doi.org/10.1016/B978-0-323-91152-8.00003-X

Given that digital technology will remain a key feature of reactor I&C design, how can the risks associated with this digital transformation be properly identified in safety analysis? Furthermore, how can these cyber risks be effectively evaluated and treated? The answers to these questions have been studied as part of the U.S. Department of Energy Office of Nuclear Energy (DOE-NE) Cybersecurity Crosscutting Technology Development program. The remainder of this chapter provides an overview of digital assets and digital I&C systems used in nuclear reactors, describes key attributes of cyber risk management, and discusses best practices for including Cyber-Informed Engineering (CIE) throughout the systems engineering life cycle.

5.2 Digital assets and I&C systems in nuclear reactors

A digital asset is a programmable device consisting of hardware, firmware, and/or software that executes internally stored programs and algorithms [2]. As shown in Fig. 1, hardware includes microelectronic components, such as integrated circuits, that are further manufactured or assembled into larger hardware devices (e.g., microprocessors, memory chips, and logic chips) or other peripherals (e.g., expansion drives and communication controllers). Firmware is the bridge between hardware and software; it runs higher-level operations and controls the basic functionality of the device, including communication, program execution, and device initialization. The software includes various operating systems, platforms, and packages used for I&C process control, Human-Machine Interfaces (HMI), terminals, and application programming interfaces (APIs). I&C systems may include proprietary, commercial, and open-source software including third-party services or libraries.

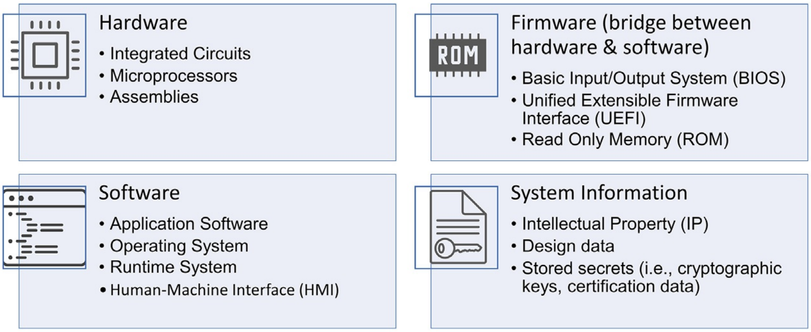
Hardware
• Integrated Circuits
• Microprocessors
• Assemblies
ROM
Firmware (bridge between hardware & software)
• Basic Input/Output System (BIOS)
• Unified Extensible Firmware Interface (UEFI)
• Read Only Memory (ROM)
Software
• Application Software
• Operating System
• Runtime System
• Human-Machine Interface (HMI)
System Information
• Intellectual Property (IP)
• Design data
• Stored secrets (i.e., cryptographic keys, certification data)

Fig. 1 Elements of a digital asset.

Often overlooked with digital assets is system information. System information is the complete record of information regarding a digital system or component. This record may include system-level and component-level information and/or data, such as requirement specifications, design documentation, fabrication, assembly, or manufacturing details; validation and verification documentation; operation and maintenance manuals; stored secrets, such as credential, authentication, or cryptographic information; and product life cycle plans.

Digital assets installed in nuclear reactors include equipment for monitoring and control, such as intelligent sensors and transmitters, programmable logic controllers (PLCs), digital data recorders, actuators, indicators, computers, and display devices. An example of an intelligent transmitter is illustrated in Fig. 2. These devices monitor and transmit process parameter data (e.g., temperature, pressure, flow, and level) by receiving analog process signals, converting them to a digital signal for mathematical transformation, and then converting the results to a 4–20 mA output signal. As illustrated by the notional block diagram in Fig. 2, these transmitters may include many subcomponents (i.e., hardware, firmware, and software) in the full digital bill of materials (DBOM).

Digital assets in U.S. nuclear power reactors are classified as critical digital assets (CDAs) if they are components in systems (or support systems) providing safety-related, important-to-safety, security, or emergency preparedness functions [2,4,5]. On average, a power reactor in the U.S. nuclear fleet contains 2000 installed CDAs [6].

While digital assets may be used as standalone devices, they are often assembled into larger, complex control systems. Nuclear digital I&C systems include reactor protection systems (RPS), engineered safety feature actuation systems, distributed control systems, feedwater control systems, turbine control systems, and emergency diesel generator systems. A simplified hierarchy of an RPS is illustrated in Fig. 3.

5.3 Cyber risk management

Despite improvements in flexibility, performance, and reliability [7], using digital I&C in a nuclear reactor adds additional risk due to cyber concerns, such as common cause failures and cyber-attacks. This cyber risk can be addressed using a risk management process. As illustrated by Fig. 4, risk management typically includes three steps—risk analysis, risk evaluation, and risk treatment.

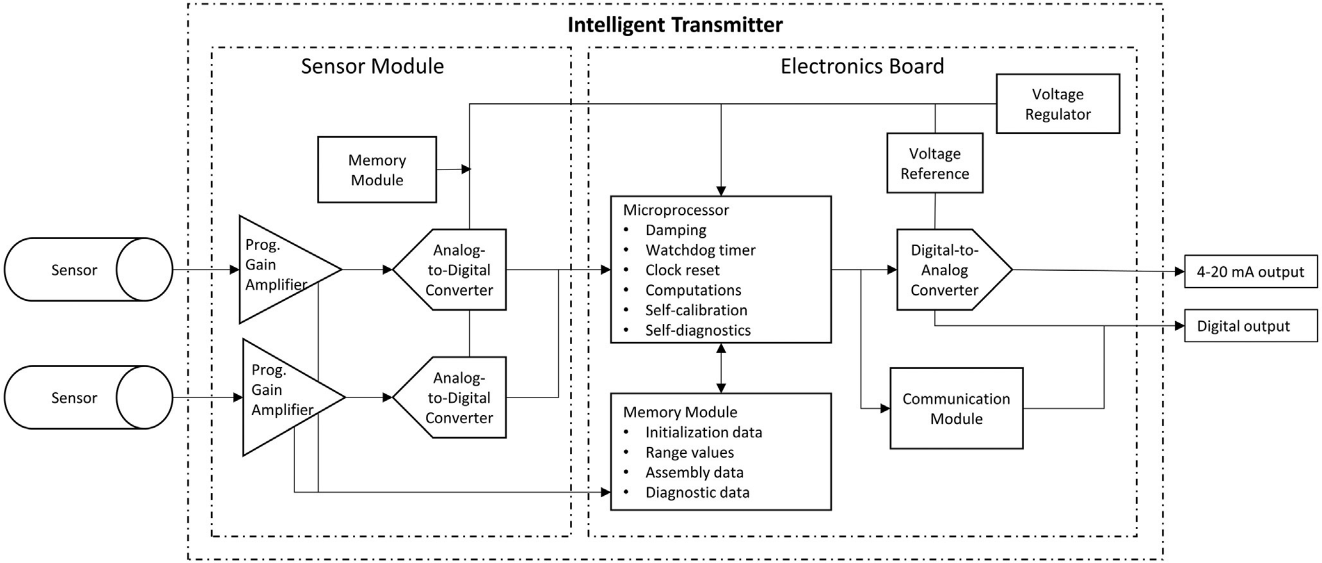

Fig. 2 Notional block diagram of an intelligent transmitter illustrating the number of subcomponents in a simple device. Not shown is the associated liquid crystal display, firmware, and software [3].

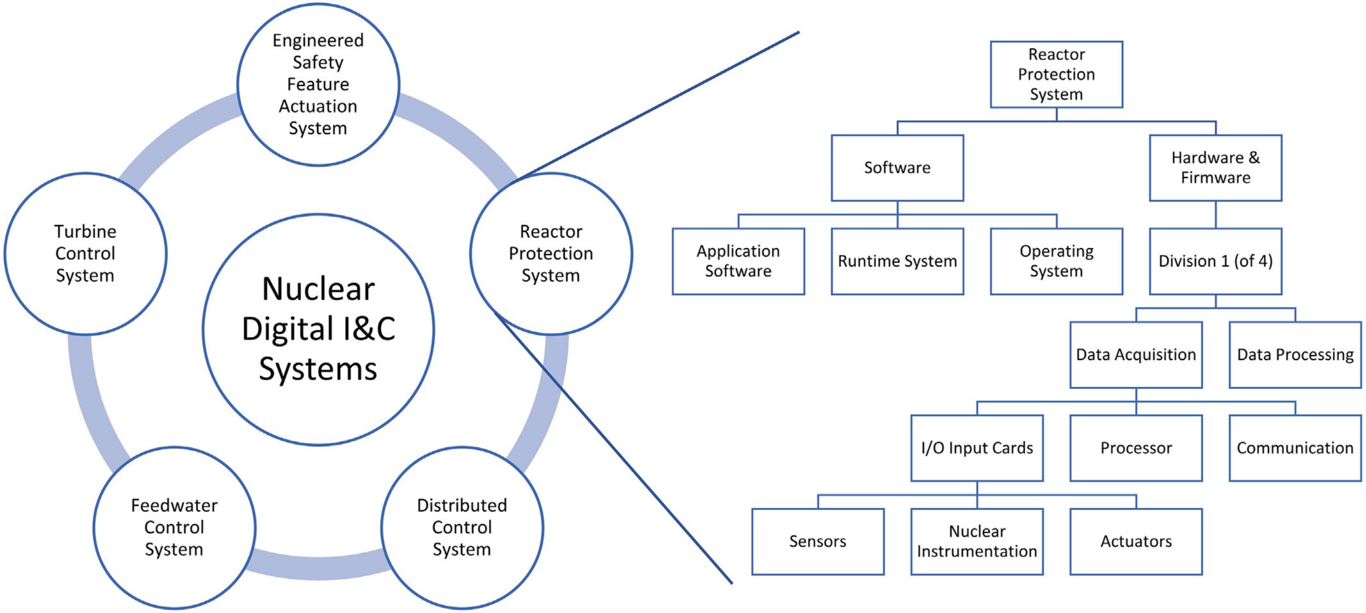

Fig. 3 Digital I&C system examples in nuclear power reactors, including a simplified hierarchy of an RPS.

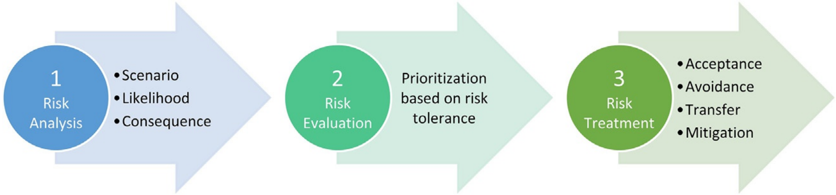

Fig. 4 Typical risk management process [8].

Risk analysis is the process by which an organization identifies what can go wrong, the likelihood that it will go wrong, and the consequences if it does go wrong [9]. Risk evaluation is the process by which an organization evaluates and prioritizes the identified risk based on their risk tolerance. Lastly, risk treatment is the process by which an organization responds to the identified risk, including acceptance, avoidance, transference, and mitigation practices.

5.3.1 Cyber risk analysis

In nuclear reactors, safety PRAs typically use data on functional failures (i.e., manufacturer failure analyses, historical plant, and industry failure data) along with known events (i.e., historical data on prior nuclear-significant events) in fault tree analysis and event tree analysis models to determine the likelihood of an event and the frequency of potential consequences. While this approach is commonly used for safety analyses, there are challenges for using it to evaluate cyber risk, such as:

1. The complete set of failure modes for digital assets and systems may be unknown as they can fail in unexpected ways.
2. Deliberate actions, such as intentional, intelligent, and adaptive actions by an adversary are challenging, if not impossible, to effectively model.
3. Threats and vulnerabilities are constantly evolving.

Whereas safety PRAs typically evaluate safety risk as a function of scenario, likelihood, and consequence, cyber risk analysis techniques often evaluate cyber risk as a function of threat, vulnerability, and consequence, including likelihood of scenario/incident success given these threats and vulnerabilities:

Threat
Vulnerability
Consequence
Likelihood of attack success

$$Cyber\ Risk = f(threat, vulnerability, consequence) \tag{1}$$

Threats include unintentional or hostile actions, vulnerabilities include unknown or known exploitable weaknesses, and consequences include the impact of the action. It is important to recognize that cyber risk is not simply the product of threat, vulnerability, and consequence, but rather a function of them. For example, a low-threat, high-consequence event resulting in fatalities will have a much different risk significance to an organization than a high-threat, low-consequence event despite potentially having the same mathematical result if multiplied together. Many different techniques for cyber risk analysis have been reported in literature. An in-depth survey of these techniques was performed by DOE-NE Cybersecurity program researchers to evaluate their use in the nuclear industry [8].

5.3.2 Consequence

Starting with the last term in Eq. (1), I&C cybersecurity objectives are usually described in terms of the C-I-A triad (Confidentiality, Integrity, and Availability) as illustrated in Fig. 5. Failure to meet these objectives could potentially lead to high-impact consequences, such as those shown in Fig. 6.

Loss of confidentiality, usually considered the least important consequence in digital I&C, includes loss of sensitive information that may be used to plan future, more damaging attacks. Loss of company or facility data may also cause financial damage or other harm to the organization.

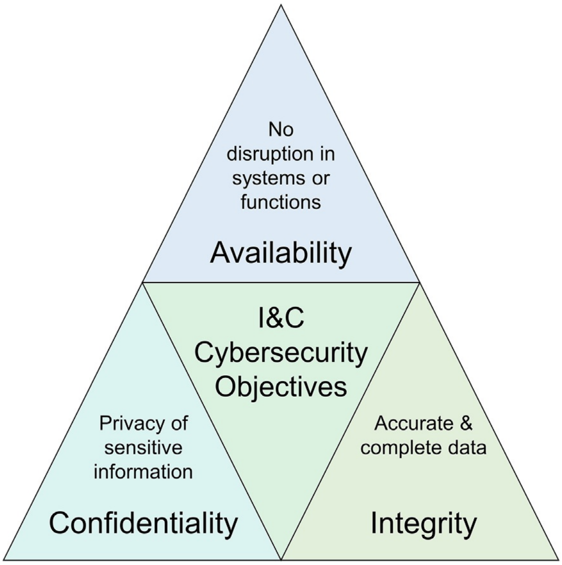
No disruption in systems or functions
Availability
I&C Cybersecurity Objectives
Privacy of sensitive information
Confidentiality
Accurate & complete data
Integrity

Fig. 5 I&C cybersecurity objectives [8].

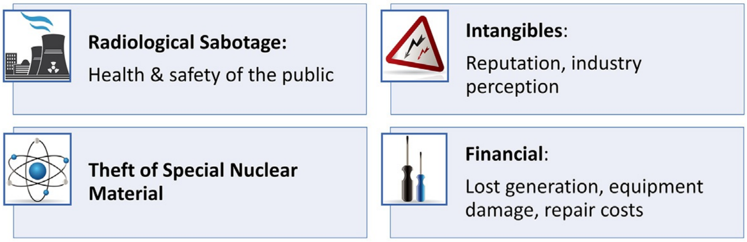
Radiological Sabotage:
Health & safety of the public
Intangibles:
Reputation, industry perception
Theft of Special Nuclear Material
Financial:
Lost generation, equipment damage, repair costs

Fig. 6 Potential high-impact consequences from a loss of C-I-A at a nuclear power reactor.

Loss of availability, which could occur from denial-of-service attacks, impacts data and communication flow in a system. Loss of integrity, which could occur from modification of data, logic or commands, impacts the truthfulness of a system. Both loss of availability and integrity may result in adverse system operation leading to safety-related (e.g., radiological sabotage, loss of life, and injury), financial-related (e.g., lost generation and equipment damage), or intangible-related (e.g., reputation and industry perception) consequences. Failure to maintain C-I-A in security systems may also enable theft of special nuclear material from a facility.

5.3.3 Threat

Threats, the first term in Eq. (1), can be classified as unintentional or deliberate. Unintentional threats are often due to human performance errors by individuals, such as misconfiguration, improper testing, and improper procedure adherence. In contrast, deliberate threats are due to adversarial or malicious intent to causing harm or damage to a facility or organization. Adversaries may also take advantage of unintentional actions by combining them with deliberate, malicious actions to cause greater harm. While adversaries may include recreational hackers, malicious insiders, and criminals, terrorist organizations and nation states have more resources (e.g., skilled personnel, funding, and time) and sufficient motivation (e.g., economic gain and military advantage) in which to launch a sophisticated attack against a nuclear reactor.

Adversaries intent on damaging critical infrastructure are becoming increasingly sophisticated. In fact, these attacks are often part of long-term offensive cyber campaigns planned and executed by nation states, such as Russia, China, North Korea, and Iran [10–15]. The Stuxnet, BlackEnergy3, and CrashOverride malware established that highly motivated and resourced adversaries (i.e., nation states and well-funded terrorist organizations) can

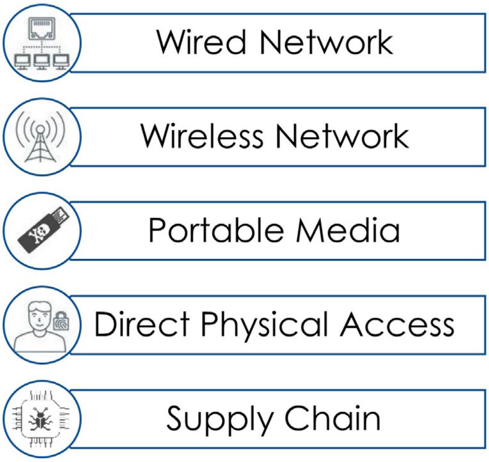

Fig. 7 Nuclear power reactor threat pathways.

maliciously cause physical equipment damage or mal-action via a cyber-attack [16–18]. Furthermore, the Triton malware attacks on Schneider Electric's Triconex Safety Instrumented System controllers demonstrated that adversaries can launch an attack against a safety control system, thereby adversely affecting safe shutdown of an industrial process [19].

As shown in Fig. 7, threat pathways at a nuclear reactor include wired and wireless networks, portable media (e.g., USB drives, maintenance laptops), direct physical access, and the supply chain. Additionally, attacks can be multi-dimensional and asymmetric—coordinated and hybrid attacks may combine multiple threat pathways and include both physical and cyber-attackers. Referring to the elements of a digital asset—hardware, firmware, software, and system information—adversarial threats can impact each of these individually, as identified in Fig. 8. Sophisticated adversaries will consider both digital asset and overall system functionality when developing an attack.

5.3.4 Vulnerability

Vulnerabilities, the second term in Eq. (1), are points or weaknesses on a digital asset or system at which an adversary can insert a compromise or extract information. Vulnerability analysis at a nuclear reactor begins with understanding the full breadth and scope of installed digital assets, including their functions, systems of systems interactions, information flows, and access points. It is impossible to provide adequate response to cyber risk if this digital

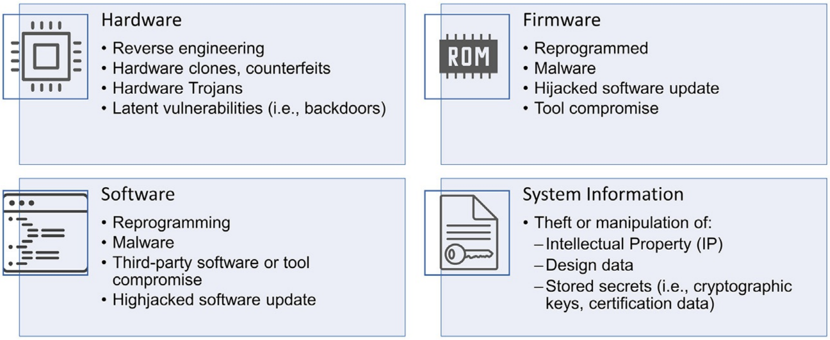
Hardware
• Reverse engineering
• Hardware clones, counterfeits
• Hardware Trojans
• Latent vulnerabilities (i.e., backdoors)
ROM
Firmware
• Reprogrammed
• Malware
• Hijacked software update
• Tool compromise
Software
• Reprogramming
• Malware
• Third-party software or tool compromise
• Highjacked software update
System Information
• Theft or manipulation of:
– Intellectual Property (IP)
– Design data
– Stored secrets (i.e., cryptographic keys, certification data)

Fig. 8 Impacts of cyber-attacks on the hardware, firmware, software, and system information of a digital asset.

asset inventory is unknown or incomplete. Known and unknown vulnerabilities in hardware, firmware, and/or software also leave the digital asset susceptible to unintentional failure modes or inadvertent human/operational error.

Vulnerabilities often increase as the digital footprint of the device or system expands, leading to a larger attack surface. While digital I&C provides increased flexibility, better performance, and improved reliability for a nuclear reactor [7], the resultant expanded cyber-attack surface increases cyber risk. Vulnerabilities may be identified by the manufacturer, industry, or plant personnel. Numerous vulnerability tracking databases and notification services exist for maintaining awareness of known or discovered vulnerabilities for installed digital assets [20–23].

Vulnerabilities also exist throughout the supply chain. DOE-NE Cybersecurity program researchers extended the work of Miller [24] to develop a novel digital I&C supply chain cyber-attack surface, as shown in Fig. 9. Hardware, firmware, software, and system information are vulnerable throughout the supply chain to attacks, such as theft of IP, malicious substitution, design alteration, malicious insertion, development tool alteration, and tampering [25]. The supply chain becomes more complicated with increasing complexity of the digital asset. For instance, the "simple" intelligent transmitter in Fig. 2 may have over a dozen globally dispersed stakeholders involved in the end-to-end supply chain, including those involved in design, fabrication, manufacturing, programming, integration, and/or testing activities.

5.3.5 Cyber risk evaluation

Once cyber risks are identified, traditional risk management processes are followed to evaluate and prioritize the risk based upon an organization's risk

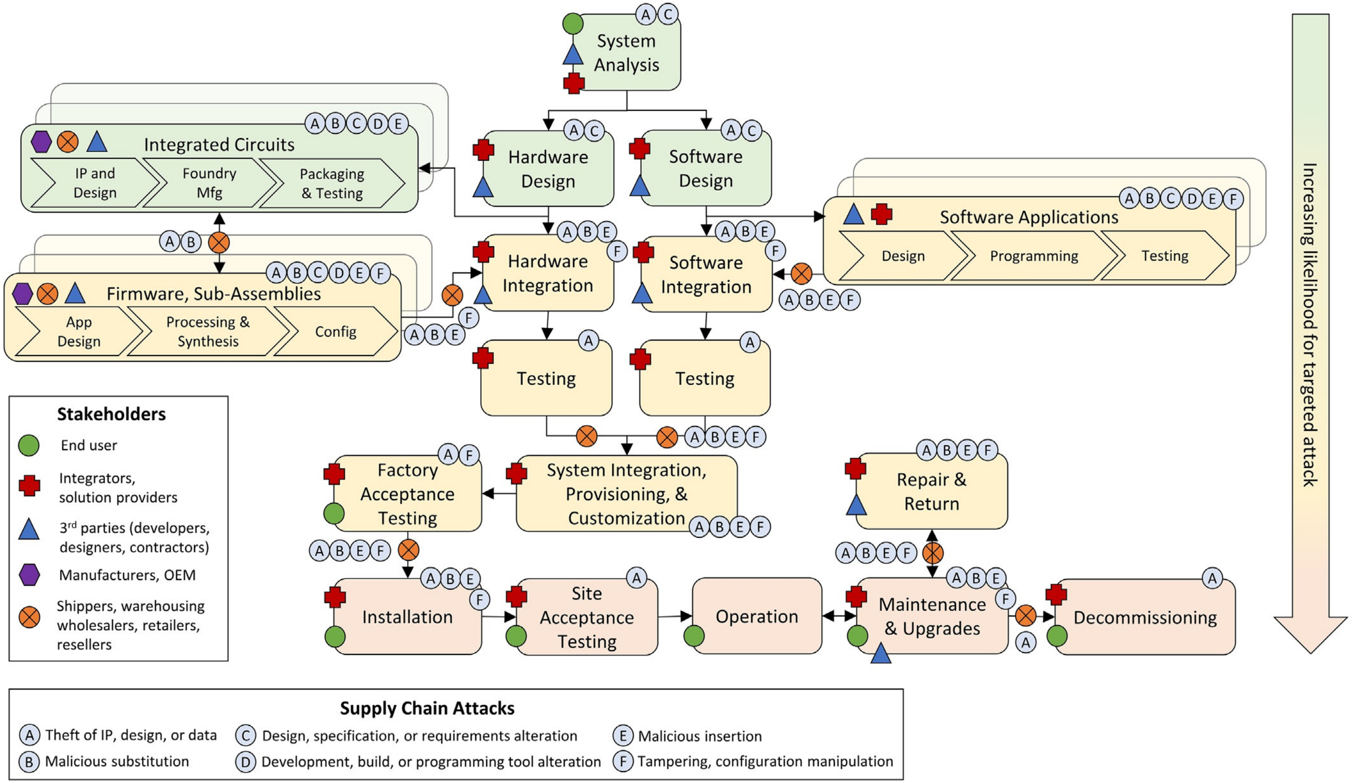

Fig. 9 The digital I&C system supply chain cyber-attack surface [3,25].

tolerance, considering regulatory, legal, and business (e.g., operational and financial) requirements. While operational and financial factors often drive the decision-making process for risk reduction in some industries, regulatory requirements in the nuclear industry often supersede other factors in the prioritization process. For example, since a nuclear power reactor in the U.S. is required to provide high assurance that CDAs are adequately protected against cyber-attacks, up to and including the plant's design basis threat as defined by 10 CFR 73.54 [4], regulatory guidance provided by the Nuclear Regulatory Commission (NRC) and Nuclear Energy Institute (NEI) may drive the risk evaluation process for a CDA [2,5,26,27].

5.3.6 Cyber risk treatment

After cyber risk is identified and evaluated, the next step is to select and implement appropriate risk treatments for protecting the C-I-A of critical nuclear systems, assets, and functions—the primary objective of nuclear I&C cybersecurity. As illustrated in Fig. 10 [28], risk treatments include:

1. Elimination or avoidance. Modification of the design to remove an identified risk, such as removal of wireless connectivity, USB ports, or unused device functions.
2. Transference. Transfer of the risk, such as by use of alternative products or solutions. While potentially not acceptable in the nuclear regulatory environment, it may also be possible to transfer risk to a vendor or an insurance policy.
3. Mitigation. Risk reduction by use of security controls or countermeasures.

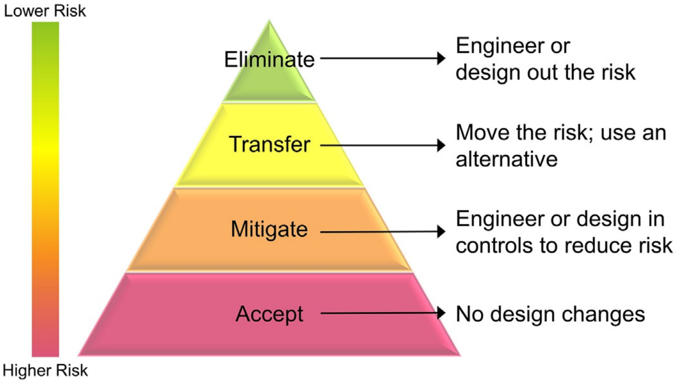
Lower Risk
Higher Risk
Eliminate
Engineer or design out the risk
Transfer
Move the risk; use an alternative
Mitigate
Engineer or design in controls to reduce risk
Accept
No design changes

Fig. 10 Cyber risk treatment options [28].

4. Acceptance. Consciously deciding to tolerate the risk without any changes, design modifications, or use of security controls.

If cyber risks in nuclear reactors cannot be eliminated or transferred, it is likely they will be mitigated by use of security controls. Catalogs of security controls (e.g., administrative, physical, and technical controls) are provided in industry guidance, such as NIST SP 800-82 [29], Regulatory Guide (RG) 5.71 [27], NEI 08-09 [26], and IAEA Nuclear Security Series No. 17-T [30]. While some cyber incidents may be unintentional, the cyber practitioner must think like an attacker to protect their facility. In cyber warfare, as an adversary continuously develops and enhances their capabilities (i.e., tactics, techniques, and procedures to distort, disrupt, destruct, disclose, and discover) the defender must continually adapt their defenses to prevent, detect, and respond to cyber-attacks.

The security control implemented by the U.S. nuclear fleet that arguably resulted in the largest reduction in cyber risk was secure defensive architectures (Fig. 11). These secure architectures typically use deterministic data diodes to segregate and control data flow between the control system, plant networks, security networks, and business networks to limit bi-directional traffic and maintain proper separation of critical functions. It is important to note, however, that although a properly architected and implemented secure architecture eliminates the "wired" threat pathway from impacting plant networks and control systems, segregated networks are still vulnerable to the other four threat pathways—wireless, direct physical access, portable media, and the supply chain.

5.4 Cyber-informed engineering (CIE)

There is a tendency in traditional engineering to delay consideration of cyber risks until after digital I&C systems and their related architecture have been designed. Failure to consider cyber risk early in the design process often results in a more expensive and less effective overall security posture. In Cyber-Informed Engineering (CIE), cyber risk management and other techniques are used throughout the systems engineering life cycle to identify, eliminate, and/or mitigate risks throughout product maturation and implementation [28,31]. The typical systems engineering V-model is shown in Fig. 12. Considering cybersecurity early and often throughout each stage of this life cycle results in a more secure solution at lower costs. For example, a CIE case study performed by DOE-NE Cybersecurity program researchers on the design of a hydrogen generation plant integrated with a nuclear power reactor led to

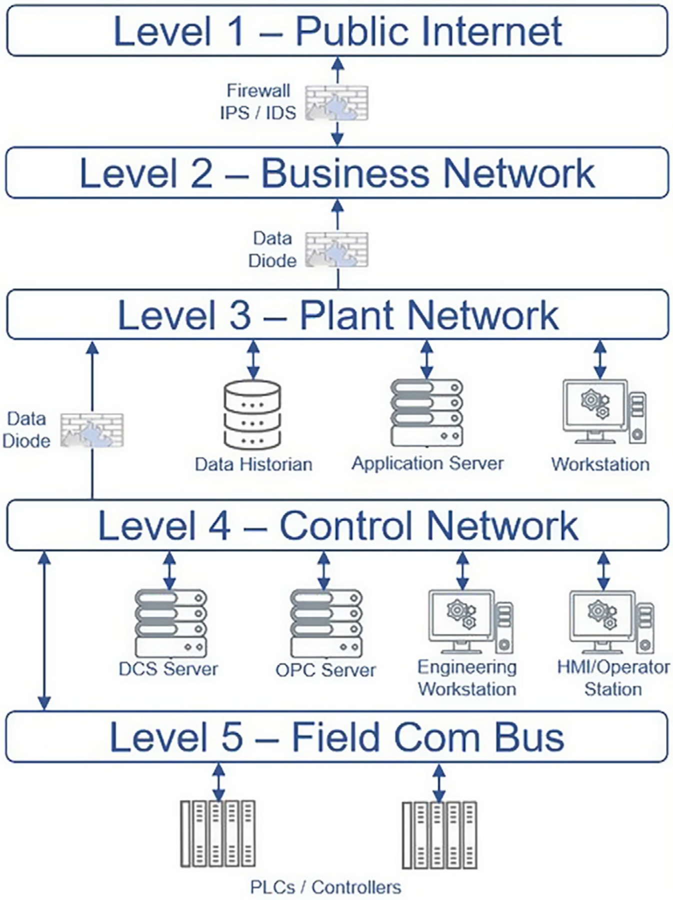

Fig. 11 Simple, notional secure defensive architecture.

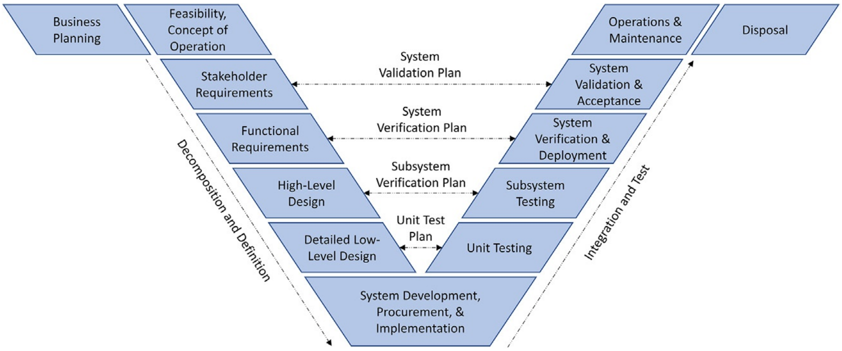

Fig. 12 Systems engineering lifecycle V-model [28].

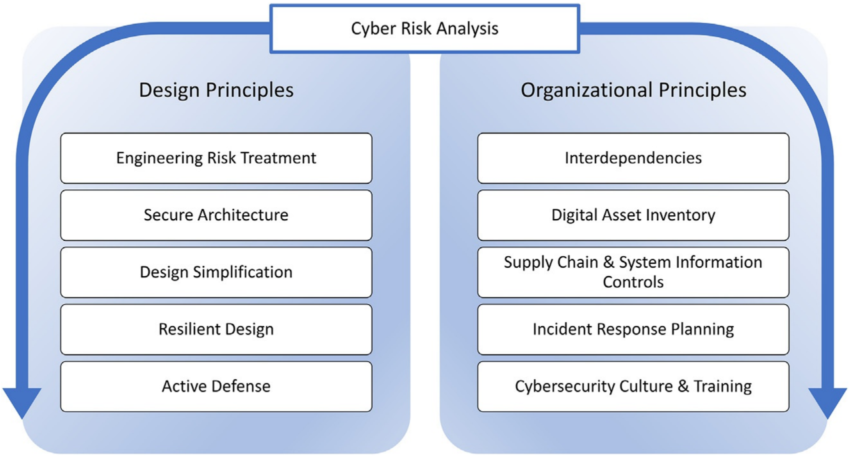
Cyber Risk Analysis
Design Principles
Engineering Risk Treatment
Secure Architecture
Design Simplification
Resilient Design
Active Defense
Organizational Principles
Interdependencies
Digital Asset Inventory
Supply Chain & System Information Controls
Incident Response Planning
Cybersecurity Culture & Training

Fig. 13 Elements of CIE [28].

recommendations for process flow and I&C system design changes to reduce cyber risks [28].

CIE elements are shown in Fig. 13. Aspects of each element should be used in each stage of the systems engineering life cycle. Cyber risk analysis is performed early and often throughout the life cycle to identify the set of potential cyber risks before applying appropriate engineering risk treatments as previously defined. It is easier to eliminate or design out cyber risks identified earlier in the life cycle. Other secure-by-design risk treatments in CIE include the use of secure architecture, design simplification, resilient design, and active defense practices. As described, secure architecture is the use of network and system architectures to reduce vulnerabilities by segregating and limiting data flows and connections within and between subsystems, systems, and systems of systems. Design simplification is the reduction of complexity in a system, such as using fewer digital assets and limiting or disabling unnecessary functions (i.e., risk elimination), to reduce vulnerabilities by minimizing the overall cyber-attack surface. Resilient design is the inclusion of diversity, redundancy, system hardening, and contingency planning into the design to ensure continued operation of critical functions when possible, or graceful degradation when not possible, during or after a cyber incident [28]. Active defense is the use of preemptive processes and techniques to prevent, detect, and respond to cyber incidents.

From an organizational perspective, CIE promotes understanding regarding the interdependencies between subsystems, systems, and systems of systems such that overall vulnerabilities are identified, including cascading effects from functional failures or compromises. Additionally, the interdependency element aims to promote a multi-disciplinary approach between stakeholders, including engineering, safety, risk, design, maintenance, operations, human factors, and information technology personnel. CIE also recommends additional organizational practices, such as an accurate, as-built digital asset inventory, incident response planning, and cyber resilient supply chains throughout the life cycle. As mentioned, failure to maintain an as-built inventory (including configuration and restoration information) during initial design, maintenance, and upgrades increases cyber risk since it is impossible to protect assets if their existence or true configuration is unknown.

Incident response planning, in conjunction with an accurate inventory, ensures that procedures, current backups, and accurate configurations are available to respond to and recover from deliberate or inadvertent cyber incidents. Additionally, as discussed, it is important to maintain authenticity, integrity, confidentiality, and exclusivity throughout the supply chain to protect hardware, firmware, software, and system information from malicious or inadvertent compromise. Lastly, CIE promotes the development of a cyber security culture and training program within all organizations involved throughout the life cycle. Similar to instilling a nuclear safety culture across all levels of an organization, equipping all personnel with the knowledge, skills, and abilities to recognize, prevent, and/or respond to cyber incidents is essential for maintaining a robust security posture.

5.5 Conclusions

The prevalence of digital I&C components and systems used within the nuclear industry will continue to increase. This growth, combined with constant advancements in technology and adversarial sophistication, translates into continuously evolving cyber risk. Failure to recognize and mitigate the risks associated with deliberate or inadvertent cyber incidents at a nuclear reactor can potentially lead to unanticipated, high-impact consequences. In cyber risk management, cyber risks are identified by considering vulnerabilities, threats, and consequences. These risks are then evaluated and prioritized such that risk treatments can be applied to mitigate, eliminate, or transfer the risk.

This chapter provides an overview of digital assets and I&C systems used in nuclear reactors as well as the vulnerabilities, threats, and consequences associated with their incorporated elements—hardware, firmware, software, and system information. Researchers are continuing to develop risk analysis techniques for nuclear reactors and their supply chains to better enumerate cyber risks of digital I&C. Considering cyber risks and using processes such as CIE throughout the systems engineering life cycle for both existing reactors and new advanced reactor designs will reduce overall cyber risk, thereby directly improving a facility's security posture.

Acknowledgment

This work was supported by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity Crosscutting Technology Development program under the DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

References

[1] IAEA, Power Reactor Information System (PRIS), International Atomic Energy Agency (IAEA), Vienna, 2020. Available: https://www.iaea.org/resources/databases/power-reactor-information-system-pris.

[2] NEI 10-04 Identifying Systems and Assets Subject to the Cyber Security Rule, Revision 3, Nuclear Energy Institute, October 2021.

[3] S. Eggers, A novel approach for analyzing the nuclear supply chain cyber-attack surface, Nucl. Eng. Technol. 53 (2021) 879–887, https://doi.org/10.1016/j.net.2020.08.021.

[4] 10 C.F.R. § 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. Nuclear Regulatory Commission, 2009.

[5] NEI 13-10 Cyber Security Control Assessments, Revision 7, Nuclear Energy Institute, October 2021.

[6] Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, 2019.

[7] T. Quinn, J. Mauck, K. Thomas, Digital Technology Qualification Task 2-Suitability of Digital Alternatives to Analog Sensors and Actuators, Idaho National Laboratory, 2012.

[8] S. Eggers, K. Le Blanc, Survey of cyber risk analysis techniques for use in the nuclear industry, Prog. Nucl. Energy 140 (2021), https://doi.org/10.1016/j.pnucene.2021.103908.

[9] S. Kaplan, B.J. Garrick, On the quantitative definition of risk, Risk Anal. 1 (1) (1981) 11–27, https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.

[10] C. Anderson, K. Sadjadpour, Iran's Cyber Threat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International Peace, 2018.

[11] D.R. Coats, Statement for the Record: worldwide Threat Assessment of the US Intelligence Community, Office of the Director of National Intelligence, January 29 2019.

[12] Dragos, Global Oil and Gas Cyber Threat Perspective: Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry, Dragos, August 2019. Available: https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf. (Accessed 8 August 2019).

[13] Annual report to Congress: Military and security developments involving the People's Republic of China, Office of the Secretary of Defense, 2019.

[14] US-CERT, TA17-117A: Intrusions Affecting Multiple Victims Across Multiple Sectors, Revised December 20, 2018, Available: https://www.us-cert.gov/ncas/alerts/TA17-117A.

[15] US-CERT, TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, Revised March 16, 2018, Available: https://www.us-cert.gov/ncas/alerts/TA18-074A.

[16] R. Langner, Stuxnet: dissecting a cyberwarfare weapon, IEEE Secur. Priv. 9 (3) (2011) 49–51, https://doi.org/10.1109/MSP.2011.67.
[17] ICS-CERT, Ongoing Sophisticated Malware Campaign Compromising ICS (Update E), 2016.
[18] ICS-CERT, Cyber-Attack Against the Ukranian Critical Infrastructure, 2016.
[19] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, C. Glyer, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FireEye Threat Research Blog, 2017. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html. (Accessed 24 April 2019).
[20] Common Vulnerabilities and Exposures (CVE), The MITRE Corporation. Available. https://cve.mitre.org/.
[21] Common Weakness Enumeration (CWE), The MITRE Corporation. Available. https://cwe.mitre.org/.
[22] Common Vulnerability Scoring System (CVSS), FiRST Available. https://www.first.org/cvss/.
[23] ICS-CERT Alerts, Cybersecurity and Infrastructure Security Agency. Available. https://us-cert.cisa.gov/ics/alerts.
[24] J.F. Miller, Supply Chain Attack Framework and Attack Patterns, The MITRE Corporation, MacLean, VA, 2013.
[25] S. Eggers, M. Rowland, Deconstructing the nuclear supply chain cyber-attack surface, in: Proceedings of the INMM 61st Annual Meeting, Online Virtual Meeting: Institute of Nuclear Materials and Management, 2020.
[26] NEI 08-09, Cyber security plan for nuclear power reactors, Revision 6, Nuclear Energy Institute, April 2010.
[27] Regulatory Guide 5.71, Revision 1, Cyber Security Programs for Nuclear Power Reactors, U.S. Nuclear Regulatory Commission, February 2023.
[28] S. Eggers, et al., Cyber-Informed Engineering case study of an integrated hydrogen generation plant, in: ANS 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT), Online Virtual Meeting: American Nuclear Society, 2021.
[29] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, SP 800-82. Revision 2. Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, 2015.
[30] Nuclear Security Series No. 17-T, Computer security techniques for nuclear facilities, Revision 1, International Atomic Energy Agency, Vienna, 2021.
[31] R.S. Anderson, J. Benjamin, V.L. Wright, L. Quinones, J. Paz, Cyber-Informed Engineering, Idaho National Laboratory, 2017.