INL/JOU-21-65020-Revision-0

Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control

March 2022

Shannon Leigh Eggers, Robert S Anderson

Changing the World's Energy Future

Idaho National Laboratory

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

INL/JOU-21-65020-Revision-0

Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control

Shannon Leigh Eggers, Robert S Anderson

March 2022

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

Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control

Shannon Eggers and Robert Anderson

Abstract

As nuclear reactors transition from analog to digital technology, the benefits of enhanced operational capabilities and improved efficiencies are potentially offset by cyber risks. Cyber-Informed Engineering (CIE) is an approach that can be used by engineers and staff to characterize and reduce new cyber risks in digital instrumentation and control systems. CIE provides guidance that can be applied throughout the entire systems engineering lifecycle, from conceptual design to decommissioning. In addition to outlining the use of CIE in nuclear reactor applications, this chapter provides a brief primer on nuclear reactor instrumentation and control and the associated cyber risks in existing light water reactors as well as the digital technology that will likely be used in future reactor designs and applications.

Keywords: cyber-informed engineering, nuclear digital instrumentation and control, digital instrumentation and control, cyber risk, nuclear cybersecurity

1. Introduction

Nuclear reactors rely on instrumentation and control (I&C) systems to maintain critical primary and secondary processes within desired parameters to ensure safe and efficient operation. Safety-related I&C systems are specifically designed to protect against critical failures that can lead to high consequence events. Designers rely on traditional safety-analyses, such as failure modes and effects analysis and probabilistic risk assessments (PRA), to inform them of specific protections needed in the design of these systems to maintain safe operation and the health and safety of the public.

I&C systems maintain real-time response, high availability, predictability, reliability, and distributed intelligence via a set of interconnected assets and subsystems that perform three main operations: acquisition, control, and supervision. Reactors have historically used analog I&C systems. As modernization occurs in the existing reactor fleet and as new advanced reactors are designed and commissioned, analog systems are replaced with digital I&C (DI&C) systems due to their many advantages, including reliability, efficiency, additional functionality, and data analytics. While DI&C provides enhanced operational capabilities, new risks associated with adverse impacts from cyber incidents are introduced. Whereas nuclear safety is the primary focus of reactor design, cyber risk must now also be considered in any digital-based reactor design. Cyber risk not only includes digital

failures and unintentional cyber incidents, but the possibility that an adversary may try to purposefully disrupt, deter, deny, degrade, or compromise digital systems in such a manner as to place a reactor outside its intended design.

Since the complete set of failure modes for DI&C may never be fully known, and since DI&C can never be completely secured, a robust process is required to address and reduce cyber risk throughout the entire systems engineering lifecycle. Specifically, engineering and design personnel must be fully cognizant of the cyber risks and understand how to protect against intentional and unintentional cyber incidents. Cyber-Informed Engineering (CIE) is an approach in which cyber risks are considered at the earliest design stages and are continually reanalyzed throughout the entire lifecycle. Regardless of reactor design, cyber risk must be eliminated or reduced as much as possible to sustain a safe and secure nuclear industry.

The remainder of this chapter is organized as follows: Section 2 provides a background on nuclear reactor I&C systems, both analog and digital, as well as considerations for use of DI&C in new advanced reactor designs and applications. Section 3 steps through aspects of cyber risk analysis and cyber risk management for nuclear reactors. Section 4 provides an overview of CIE along with detailed descriptions of each CIE principle prior to concluding the chapter in Section 5.

2. Background

Chemical, manufacturing, and nuclear processes rely on instrumentation, such as pressure, temperature, and flow sensors, to measure and monitor process parameters. These industrial processes are then maintained by control systems that operate physical equipment, such as valves, pumps, and heaters, to keep the process parameters within predefined limits. Nuclear reactors vary by type (e.g., pressurized water reactor, pool-type reactor, liquid metal cooled reactor, molten salt reactor, gas cooled reactor) and purpose (e.g., power reactor, research reactor, nuclear propulsion). The remainder of this section first describes the fundamentals of generic nuclear reactor I&C prior to discussing the transition to digital technology, including its benefits and challenges. The section concludes with an overview of future DI&C applications, including those in new and advanced reactors, as well as integrated systems and decision support systems.

2.1 Fundamentals of reactor instrumentation and control

Nuclear reactors initiate and control nuclear fission or fusion reactions. These processes must be monitored and closely controlled to ensure reliable and efficient operation while maintaining the health and safety of the public. The number and type of parameters monitored in a reactor will vary depending on the reactor type and purpose, but both nuclear and non-nuclear instrumentation will likely be used. Nuclear instrumentation includes detectors to monitor neutron and gamma flux for routine reactor monitoring and control as well as reactor safety. Neutron detectors, such as proportional counters and ion chambers, are commonly used to provide source range, intermediate range, and power range monitoring, while gamma detectors are used for post-accident monitoring. These detectors may be out-of-core or in-core, or a combination thereof, depending on the reactor type. Other compact in-core detectors, such as small fission chambers or self-powered neutron detectors, are also commonly used for continuous real-time monitoring of reactor core conditions, including reactor power distributions.

Non-nuclear instrumentation includes sensors used to monitor process parameters, such as temperature, pressure, differential pressure, level, and flow.

Additionally, non-nuclear instrumentation may be used to monitor other parameters, including control rod position, area radiation, fuel-pin fission gas pressure, vibrations, acoustics, fuel or vessel strain, process fluid chemistry, moisture and gas analysis, and leaks.

Local instrumentation data is transmitted from the sensors to control board indicators, data recorders, applications, and control systems via analog or digital circuits, often through multiplexers or combinatorial logic circuits. Applications are commonly used to auctioneer (e.g., signal selection), aggregate, and/or perform calculations on the data to provide real-time reactor and plant status indications to operators.

While operators will also perform manual actions on a reactor, such as starting and stopping pumps or opening and closing valves, I&C systems are commonly used to automatically control reactor operations and maintain reactor safety. Control systems can be simple, like a single programmable logic controller, or complex, like a reactor control system. Control systems can combine numerous sensors, transmitters, controllers, and actuators to change the physical state of process equipment, such as a valves, pumps, or motors, by using signal feedback loops to monitor and maintain desired conditions. In a nuclear power plant (NPP), non-safety control systems may include feedwater control (or fluid control), turbine control, and reactor control.

Most nuclear reactors will have at least two types of control systems—reactor control systems and reactor safety systems. Depending on a reactor's purpose, there may also be other control systems, such as plant control systems in an NPP or experiment/sample control systems in a research and test reactor. Reactor control systems are used to control the nuclear fission or fusion reaction within specified acceptable fuel design limits by adjusting physical components according to the reactor design. For example, a reactor control system may raise or lower control rods in a light water reactor (LWR), turn control drums in a heat pipe reactor, or start or stop feedwater flow in a research reactor.

In an LWR, reactor control systems are used to maintain desired thermal megawatts by balancing primary and secondary systems. For example, as shown in **Figure 1**, an integrated control system may automatically maneuver reactor, feedwater, and turbine systems to match megawatts generated to megawatts demanded by adjusting control rod positions, valve positions, and pump speeds.

In comparison to reactor control systems, reactor safety systems are used to shut down and maintain safe shutdown of a reactor in the event a reactor safety limit

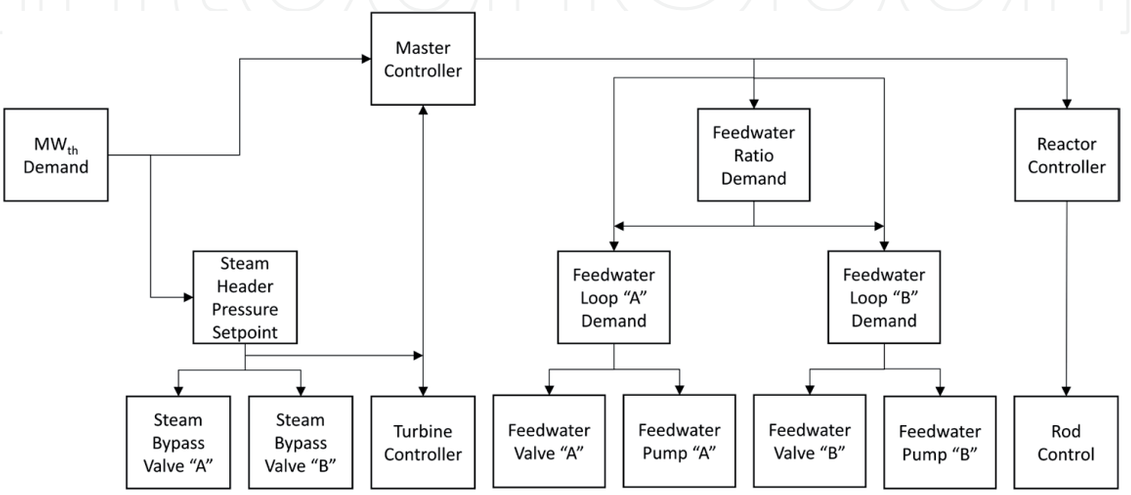

Figure 1.
A notional automatic integrated reactor control system for an LWR.

is met or exceeded to assure reasonable protection against uncontrolled release of radioactivity. For example, reactor safety systems in an LWR include Reactor Protection Systems (RPS), Engineered Safety Feature Actuation Systems (ESFAS), and diverse actuation or diverse trip systems. Reactor safety systems often use either two-out-of-four or two-out-of-three logic. For instance, an RPS may have four redundant instrumentation channels that monitor key parameters, such as reactor power, reactor coolant temperature, reactor coolant pressure, reactor coolant flow, reactor building pressure, reactor pump status, and steam generator level. If any design limits are exceeded on two separate channels, an automatic trip signal is sent to the control rod system to shut down the reactor. A notional representation of an RPS is shown in **Figure 2**.

In an LWR, an ESFAS is designed to provide emergency core cooling for the reactor and to reduce the potential for offsite release of radiation. Comparable to an RPS, ESFAS uses multiple channels of equipment in two-out-of-three logic (or similar) to monitor signals such as reactor coolant pressure and containment pressure. Based upon the specific coincident actuation signals received, ESFAS will start the required safety system, such as emergency core cooling systems, emergency feedwater, containment isolation and ventilation, containment spray, or emergency diesel generators.

2.2 Digital instrumentation and control

Although the first closed-loop industrial computer control system was installed by Texaco Company at its Port Arthur refinery in 1959 [1], I&C in nuclear reactors

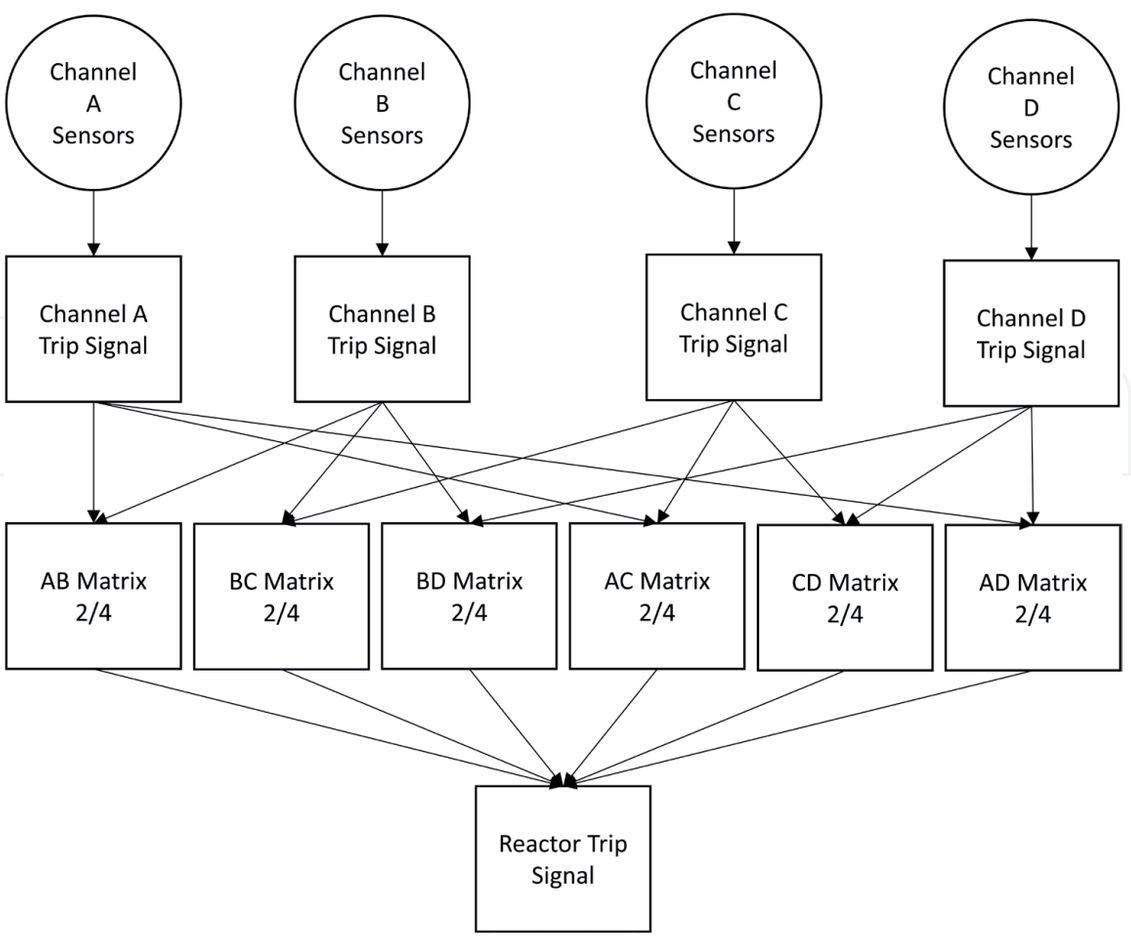

Figure 2.
Signals for a notional RPS.

largely remained analog until about 30 years ago when digital transmitters, indicators, controllers and data recorders began replacing analog sensors, indicators, actuators, and pen-based chart recorders. And, while non-safety digital control systems (e.g., feedwater control systems, turbine control systems and reactor control systems) are now commonly installed in nuclear reactors, safety-related digital control systems (e.g., RPS, ESFAS) are much less common, especially in the United States. The United States has been slow to adopt digital technology because of previously unanalyzed risks associated with new and unknown attributes, including common cause failures and cyber risks. International adoption of digital technology in nuclear reactors, including safety-related control systems, has been more aggressive than in the United States. Of course, new advanced reactors are being primarily designed with DI&C.

As described by the Nuclear Energy Institute (NEI), an I&C device in the U.S. power reactor industry is typically considered 'digital' if it contains any combination of hardware, firmware, and/or software that can execute internally stored programs and algorithms without operator action [2]. Hardware includes microelectronics, such as digital or mixed signal integrated circuits, as well as larger assemblies, such as microprocessors, memory chips, and logic chips. Hardware may also include other peripherals, such as expansion drives or communication controllers. Software includes operating systems, platforms, and applications used for process control, human machine interfaces, and other specific programs used for device or system operation. Firmware is software stored in non-volatile memory devices that provides low-level control specific to the hardware. Firmware executes higher-level operations and controls basic functionality of the device, including communication, program execution, and device initialization.

Field sensors and controllers may be standalone, small local systems, or larger distributed control systems. Devices may be connected by physical cables or wireless technology (e.g., WiFi, cellular, satellite, Bluetooth, radio frequency identification). There is also a range of communication protocols used in DI&C depending on the design and manufacturer.

The systems, structure, and components (SSCs) used in U.S. NPP safety-related protection systems are categorized as Institute of Electrical and Electronics Engineers (IEEE) class 1E technologies as defined by IEEE 308-1971 (and later) [3]. They must be designed to conform with General Design Criteria (GDC) in 10 CFR 50 Appendix A [4], IEEE 279-1971 [5], IEEE 308-1971 [3], and IEEE Std 603-1991 [6], as applicable based on construction permit dates. Guidance in Regulatory Guide 1.152 [7] and IEEE 7-4.3.2-2003 [8] may also be used to comply with Nuclear Regulatory Commission (NRC) regulations. Internationally, applications or components that perform IEC category A safety-related functions may fall under IEC 61513 [9], International Atomic Energy Agency (IAEA) SSR-2/1 [10], and IAEA SSG-39 [11] requirements.

These general design criteria include conformance requirements for independence and single-failure criterion such as defense-in-depth, diversity (i.e., different technology), redundancy (i.e., secondary equipment that duplicates the essential function), physical separation, and electrical isolation. The purpose of single-failure criterion is to ensure no single failure of a component interferes with the safety function and proper operation of the safety system [6]. Generally, it is impossible to prove that digital systems are error free. And, while common-cause failures can occur with analog equipment, it is more likely that software errors will result in common-cause failures, such as identical software-based logic errors that could cause simultaneous functional failure of all four RPS divisions. Thus, since unanticipated common-cause failures are more likely in digital systems than analog systems, there is increased burden to prove to the regulator that the design adequately meets the general design criteria outlined in the applicable requirements.

2.3 Benefits and challenges of digital instrumentation and control

The systems engineering lifecycle for analog modifications, such as changing mechanical relay logic, can take significant time to design, procure, reconfigure, and test hard-wired devices installed inside control cabinets. These changes can require many hours for maintenance personnel to rewire, physically rearrange components, and/or add new cabinets, terminal blocks, power supplies, and wiring. Labor resources are also required for post installation quality checks.

Contrary to analog I&C, a significant benefit of DI&C is the ability to quickly reprogram the functionality of a device or system with minimal physical hardware changes. These modifications are performed via microprocessors, expansive memory storage, and standardized communications that allow for remote connectivity. Moreover, the utilization of reusable software and common microprocessors lowers overall product costs. Moreover, the global supply chain has promoted further innovation, improved efficiencies, better product availability, and reduced costs.

An additional benefit of DI&C is the capability to incorporate numerous functions within one device. This capability reduces overall size of the I&C systems (e.g., fewer racks and cabinets) and relieves potential space constraints within facilities. Furthermore, the ability to choose from a wide array of functions in one device not only reduces the cost, but also allows for unique control algorithms not necessarily available in the past. Whereas analog I&C was limited to using a single proprietary signal conveying only one piece of information (e.g., the process value), adding a digital signal overtop an analog signal allowed for increased device diagnostics and calibration capabilities without any additional hardware changes and helped pave the way for logical extension of DI&C in nuclear facilities.

Other applications enabled by DI&C include enhanced online monitoring for condition-based maintenance systems. These systems improve visibility into equipment conditions to improve maintenance activities and potentially reduce or eliminate required preventive maintenance. Additionally, training departments are now able to simulate plant operations with fine detail that was difficult to achieve before.

On the other hand, digital technology introduces new challenges. As existing nuclear reactors are modernized, plant personnel throughout the organization must be trained on their design, installation, operation, and maintenance. This skillset is often very different than what is required for analog I&C and can take many years to acquire. Moreover, not only is there an increase in common-cause failures and potentially unknown failure modes with DI&C, but there is also additional risk associated with malicious and unintentional cyber threats not typically seen with analog I&C. These DI&C cyber risks are further described in Section 3.

2.4 Future technology considerations

2.4.1 New and advanced reactor designs

While existing reactors primarily designed and built with analog technology are transitioning to DI&C, new generation III+, small modular reactor (SMR), microreactor, and advanced reactor designs will likely apply digital technology from project inception to take advantage of increased flexibility, better performance, and improved reliability. It is anticipated that these designs will also include hybrid approaches, similar to existing reactors, incorporating both analog and DI&C components and systems for reactor control and reactor safety. However, since most of the new reactor designs will likely incorporate passive safety features, they may have fewer (or no) safety-related control systems compared to current LWRs.

Nuclear reactors are primarily designed with safety as the underlying principle. Ensuring safety of reactor personnel and maintaining the health and safety of the public is more important than secondary objectives, such as producing electricity or medical isotopes. Thus, any new reactor technology that challenges the nuclear safety paradigm is met with strong caution. However, as new advanced reactors are designed with DI&C, significant effort and analysis will be undertaken to ensure cyber risks are fully understood such that the designs will fully withstand regulatory and public scrutiny and not interfere with reactor safety. Nevertheless, the inclusion of passive safety features that reduce the footprint of digital safety systems not only reduces the number of high-consequence design basis accidents (DBAs), it also reduces overall cyber risk.

Sites built with multiple reactor modules (e.g., SMRs) may have additional I&C systems to enable integrated and coordinated operation across multiple units. Furthermore, proposed advantages of SMRs and microreactors include the capability for remote and autonomous (or nearly autonomous) operation, including anticipatory control strategies to maintain operational limits for both planned and unplanned internal or external disturbances which increase overall operational flexibility. The passive safety systems in advanced reactors may enable fewer operators and more automation, however, these new modes of operation and previously unanalyzed consequences require careful evaluation by designers and regulators to ensure minimization of cyber risks. Mobile reactor designs must also anticipate and address additional requirements for safe and secure transportation.

Similar concerns exist for remote operations, which is under consideration for advanced reactors in isolated environments or reactors connected to microgrids using autonomous distributed energy control schemes. Remote operations imply some finite distance between reactor and operator utilizing digital communications for both monitoring and control. Not only does the external pathway potentially enable an exploitable pathway for adversaries, it also potentially presents unanticipated cyber risks from communication failures.

2.4.2 Integrated energy systems

Whereas remote and autonomous reactor operation may have a long timescale for development, regulatory acceptance, and construction, integrated energy systems may be available on a shorter timescale. As shown in **Figure 3**, integrated energy systems use the thermal heat from reactors for other purposes, such as hydrogen generation, district heating, water purification, and chemical manufacturing. They may also have direct electrical connections to integrated systems. The interconnections between a reactor and these secondary processes will likely contain additional sensors, controllers, and actuators in order to balance the electrical and heat demands of the plant with the demands from the integrated energy systems.

2.4.3 New supporting applications

Digital twins are virtual replications of a physical system that can be used to provide various capabilities and decision-support at a nuclear facility. The degree of representation by a digital twin depends upon the computing power and the ability to accurately model both reactor physics and data-driven processes. Proposed applications include the use of digital twins for running artificial intelligence or machine learning (AI/ML) applications for hybrid control schemes, such as flexible operation for electric grid load-following, anticipatory control, or autonomous control; the use of AI/ML on digital twins for equipment condition monitoring, diagnostics,

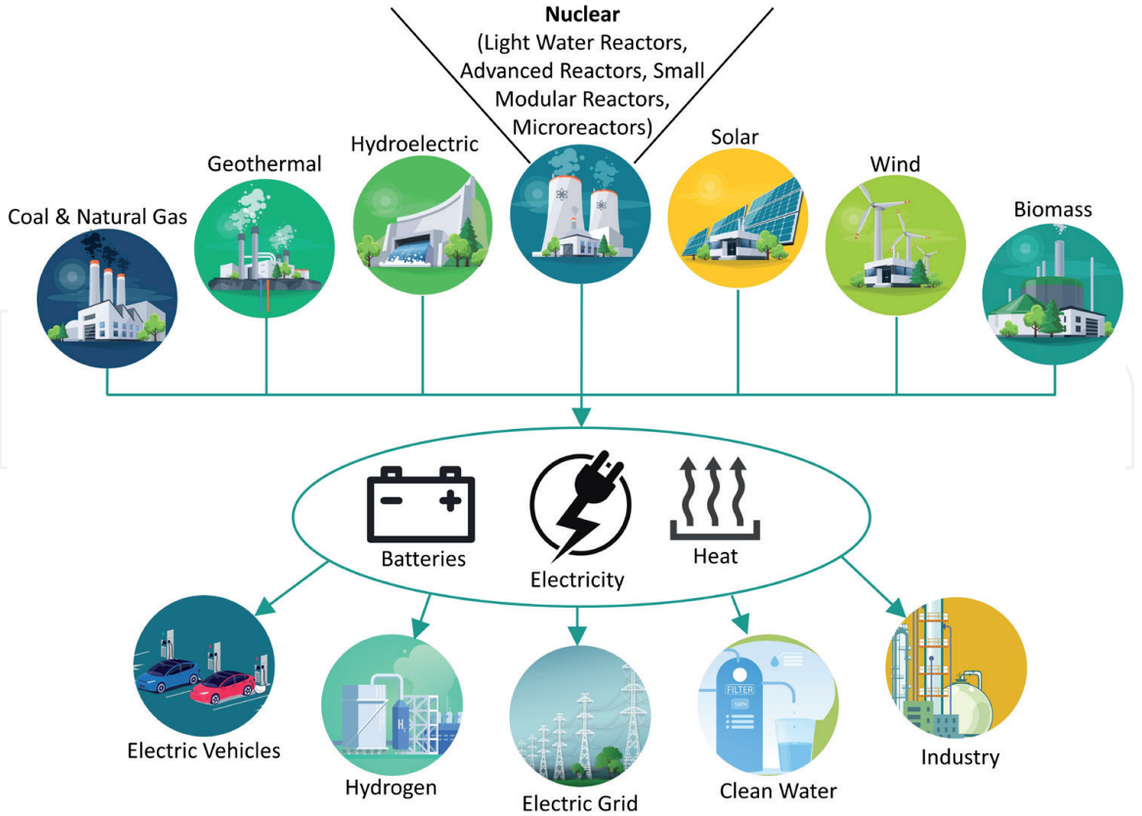

Figure 3.
Conceptual integrated energy system including generation sources and applications.

prediction, and prognostics; and the use of digital twins for designing engineering modification prior to building the actual physical system.

Using digital twins for reactor and/or system design may enable vulnerability discovery, such as potential for equipment failure, process anomalies, human error, or cyber compromise. Understanding system operation as well as potential vulnerabilities and consequences prior to construction is not only a benefit to designing better and safer reactors but also, if used with CIE principles as described in Section 4, a reactor with reduced cyber risk.

Applications of digital twins will likely continue to expand. The capabilities of digital twins, AI/ML, and other monitoring and control systems will be enabled with the increased use of wireless technologies (e.g., Wi-Fi, radio frequency identification, Bluetooth, Zigbee, cellular) in addition to traditional wired networks. Moreover, the use Internet of Things (IoT) or Industrial Internet of Things (IIoT) will continue to expand within nuclear facilities enabling improved efficiencies, reduced maintenance, and real-time insights for decision-making. Whereas the difference between operational technology (OT) and information communications technology (ICT) is that OT uses digital devices to control physical processes, such as nuclear reactors, IIoT uses a wide range of lower cost sensors that are traditionally connected via wireless networks to increase the number datapoints available for machine-to-machine communication and enhanced monitoring using data analytics, big data, and AI/ML.

3. Cyber risk

Risk is classically defined by Kaplan and Garrick as the possibility of loss or injury, including the degree of probability of such a loss [12]. Traditional safety PRA in the nuclear industry uses a logical framework combining fault tree analysis

and event tree analysis to identify the likelihood and consequence of severe accidents which could lead to radiation release impacting the health and safety of the public. Nuclear 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).

Unfortunately, the PRA approach is insufficient for cyber risk analysis as the complete set of failure modes for digital assets and systems may be unknown as they can fail in unexpected ways. Additionally, deliberate actions, such as intentional, intelligent, and adaptive actions by an adversary are challenging, if not impossible, to effectively model. Furthermore, threats and vulnerabilities are constantly evolving, a reality which does not lend itself to PRA. Therefore, rather than follow the Kaplan and Garrick risk triplet of 'scenario, likelihood, consequence' [12], cyber risk is better identified by evaluating threats, vulnerabilities, and consequences [13].

It is important to note that cyber risk includes all risk from both intentional and unintentional actions. Holistic cyber risk includes human performance errors and equipment failures as well as adversarial events. Adversarial events include malicious actions, including those by an unwitting insider, intended to cause damage or disruption to reactor and facility operations. Adding to the concern, intelligent threat actors can potentially adversely impact nuclear DI&C by remotely exploiting vulnerabilities, a threat that does not exist with analog I&C.

3.1 Consequence analysis

A nuclear reactor has a licensing basis that identifies high-consequence DBAs that can potentially lead to radiological release. This licensing basis includes those safety-related SSCs that must remain functional during a DBA to protect the health and safety of the public. While safety-related impacts are the primary concern, consequences from a cyber incident at a nuclear reactor could potentially range from intangible impacts (e.g., reputation damage, industry perception) to financial impacts (e.g., lost generation, equipment damage, repair costs) to adverse public health and safety impacts due to radiological release or theft of special nuclear material (SNM). Examples of low to high consequence impacts from a cyber incident are illustrated in **Figure 4**. **Table 1** expands on several of these consequences to provide causal examples of functional failures from hypothetical cyber incidents.

Cyber-induced consequences at a nuclear reactor can be minimized by maintaining availability, integrity, and confidentiality of DI&C components and systems. Nuclear reactors may be designed to run continuously (e.g., NPP) or intermittently (e.g., research and test reactor). In either case, data and communication flow must remain available to ensure safe and reliable operation of the reactor. Delay, disruption, or prevention of data or communication within an OT system can result in

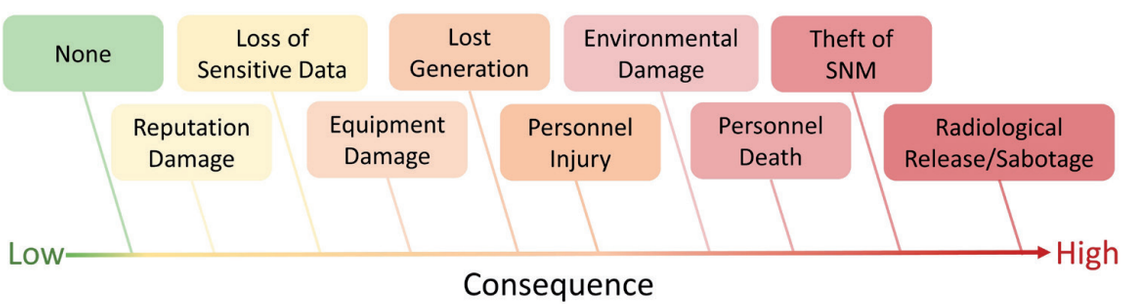

Figure 4.
Potential consequences from a cyber incident at a reactor.

Potential consequence	Functional failure	Initiating cyber incident
Radiological release	Failure of a safety system to actuate when needed	Digital RPS does not trip the reactor on low feedwater flow
Lost generation	Inadvertent actuation of a safety system leads to extended plant shutdown	Digital high-pressure coolant injection actuation with no loss of coolant
Lost generation	Inappropriate operator action	Operator does not recognize that a digital indicator on the main control board is incorrect
Equipment damage	Pump suction valve closed	Digital valve controller closed valve with pump running

Table 1.
Potential consequences from a cyber incident at a reactor along with hypothesized functional failure and initiating cyber incident.

unintended control actions, such as inadvertent component actuation or reactor trip. As listed in **Table 2**, cyber incidents that impact availability can be malicious and intentional, such as from a denial of service attack [14], or non-malicious and unintentional, such as excessive network traffic from failing equipment [15].

The integrity of DI&C information, data, and system parameters must also be maintained. Control systems require accurate, truthful, and complete information for safe and reliable operation. For instance, unintended modification of data, logic, or commands by man-in-the-middle attacks can cause equipment failure [16] or poorly executed software updates can reset plant data and cause actuation of a safety system [17]. Operators also rely on truthful and accurate data for decision making; inaccurate data on indicators or human-machine interfaces could cause operators to make improper decisions or perform incorrect actions. Operationally, it is often more dangerous to have a reactor in an unknown state instead of safely shut down. Consider an unexpected cyber incident that is visible to the operator—the operator can detect and respond to the incident, thereby minimizing further impacts. On the other hand, cyber incidents that are invisible to the operator can potentially result in persistent and higher consequence adverse impacts as operators are unaware of true reactor status.

While not as important in OT systems, confidentiality is also a cybersecurity objective. Loss of confidentiality, such as unauthorized exfiltration of sensitive information [18] or inadvertent posting of sensitive data in the public domain, can enable development of further attacks or cause other business-related concerns. Gaining sensitive nuclear information can provide adversaries roadmaps, schedules, vendors, plant layouts, and a host of other sensitive information shortening the attack timeline and delivering potential pathways to be considered towards ransomware, blackmail, or general political unrest.

3.2 Threat analysis

Cyber threat vectors into a nuclear reactor include wired and wireless networks or connections, portable media and maintenance devices (e.g., USB drives, maintenance laptops), insiders, and the supply chain. Furthermore, cyber threats can be classified as non-malicious or malicious. Non-malicious actions are often caused by employees or other facility personnel who perform actions not intending to cause harm. These actions are often human performance errors in which a worker mistakenly performs an adverse action, such as misconfiguring a device, selecting the wrong option, or disclosing sensitive information.

Security objective	Malicious incident	Non-malicious incident
Availability	Denial of service attack [14]	Failing equipment leading to excessive network traffic [15]
Integrity	Man-in-the middle attack [16]	Software update resetting plant data [17]
Confidentiality	Reconnaissance attack leads to data exfiltration [18]	Sensitive data posted on external site

Table 2.
Examples of malicious and non-malicious cyber incidents by security objective.

Malicious threats against nuclear reactors are initiated by adversaries with the intent to cause harm. Adversaries include recreational hackers, malicious and unwitting insiders, criminals, terrorist organizations, and nation states. Sophisticated attacks against nuclear reactors will likely be launched by organizations that have greater resources (e.g., skilled personnel, funding, time) and sufficient motivation (e.g., economic gain, military advantage, societal instability). Additionally, cyber-attacks may be one-dimensional or multi-dimensional, hybrid, coordinated attacks combining multiple threat vectors in both physical and cyber domains. For instance, adversaries may use cyber means to gain access to enable physical destruction or theft of SNM or use physical means to gain access to computer systems to enable unauthorized theft of sensitive information or sabotage.

In the United States, power reactors licensed by the NRC must provide high assurance that critical digital assets (CDAs) are protected against cyber-attacks, up to and including the design basis threat (DBT) [19]. CDAs are defined as digital assets associated with safety-related, important-to-safety, security, or emergency preparedness functions as well as support systems and equipment which, if compromised, would adversely impact these functions. A DBT describes adversarial attributes and characteristics, including level of training, weapons, and tactics, that must be defended against to safeguard the reactor against radiological sabotage and prevent theft or diversion of SNM. Generally, a beyond-DBT, a threat from an adversary who has capabilities beyond what is defined by the DBT, is considered nation-state activity which falls under responsibility of the state (e.g., federal government) for prevention, detection, and response.

3.3 Vulnerability analysis

Vulnerabilities are known or unknown weaknesses. Vulnerabilities in hardware, firmware, and/or software can leave digital assets susceptible to accidental failure or unintentional human error. Additionally, vulnerabilities may be exploitable, enabling adversaries to extract information or insert compromises allowing unauthorized access to perform malicious activities. Vulnerabilities can allow adversaries to penetrate and move throughout systems without the user's knowledge to compromise the availability, integrity, and confidentiality of complex control systems.

Most digital devices can be reprogrammed or modified to perform unintended or undesired functions. Any vulnerability that allows an unauthorized reprogramming or modification of a critical digital asset can result in adverse function of the DI&C systems. As most design approaches wait until system implementation to evaluate vulnerabilities, vulnerability response and mitigation often relies on bolted on security controls. However, if engineers who design and maintain complex control systems are trained to identify, understand, and mitigate these vulnerabilities throughout the lifecycle, including during design stages, vulnerabilities can be addressed early and often, thereby leading to lower overall cyber risk.

From a maintenance perspective, manufacturers often identify vulnerabilities and send information notices to asset owners along with mitigation measures, if applicable. Numerous vulnerability tracking databases and notification services also exist which serve to improve awareness and facilitate mitigation or protection [20–23]. Engineers and stakeholders should maintain awareness of these external vulnerability notifications or sites for their digital assets throughout the entire lifecycle so that they can be addressed immediately.

3.4 Cyber risk management

Of course, cyber risk cannot be calculated by simply multiplying numerically derived values of threats, vulnerabilities, and consequences together. For instance, low-threat, high-consequence cyber incidents will likely have a much different risk significance at a nuclear reactor than a high-threat, low-consequence incident. While many techniques have been proposed for incorporating the results of consequence, threat, and vulnerability analyses into a final cyber risk analysis [13], determining, evaluating, and prioritizing cyber risk is highly dependent on the reactor design, regulatory requirements, and organization's risk tolerance.

Cyber risk management is the continual process of analyzing cyber risk, evaluating and prioritizing the identified risk against organizational and regulatory requirements, and then applying risk treatments. In the United States, current nuclear power reactors typically follow guidance in NRC Regulatory Guide 5.71 [24] or the NEI cybersecurity series (NEI 10-04 [2], NEI 08-09 [25], and NEI 13-10 [26]) to identify CDAs and risk treatments. Corresponding cyber security guidelines for the international nuclear community are provided in IAEA Nuclear Security Series (NSS) No. 13 [27], NSS 17-T (Rev. 1) [28], NSS 42-G [29], NSS 33-T [30], and IEC 62645 [31]. For risk management activities, IAEA NSS 17-T (Rev. 1) refers readers to ISO/IEC 27005. Additionally, IEC 62443-3-2 provides an international security risk assessment standard for I&C systems [32]. Cybersecurity regulation and guidance for advanced reactors is still in development.

Regardless of the equation or formula used, cyber risk is managed by analyzing the potential worst-case consequences and then using risk treatments (e.g., avoidance or elimination, mitigation, transference, or acceptance) to lower the risk to a level acceptable to the organization. Unlike analog I&C, where failure analysis was the primary focus of PRA, the use of DI&C has resulted in the capability for hardware, firmware, and software to be altered in a manner not intended by the original design. Since both malicious and unintentional actions can potentially adversely impact operational functions, continually evaluating cyber threats, vulnerabilities, and consequences in a cyber risk management program is necessary to maintain awareness into the constantly evolving risk environment. The goal of this consequence-driven analysis is to prioritize risk treatments for those DI&C components needed to ensure critical reactor functions are maintained.

Consequence-driven, Cyber-Informed Engineering (CCE) is a formal cyber risk management approach that focuses on reducing the impact from high consequence events (HCE) for an overall business entity [33]. As shown in **Figure 5**, CCE is a four-step process. In phase 1, HCEs are identified and prioritized using a severity score calculated based upon consequence criteria weights and criteria severity. For the identified HCE(s), a system of systems analysis identifies the most critical functions in phase 2 and potential cyber-attack scenarios on those functions are then identified in phase 3. In phase 4, appropriate protection and mitigation strategies are developed.

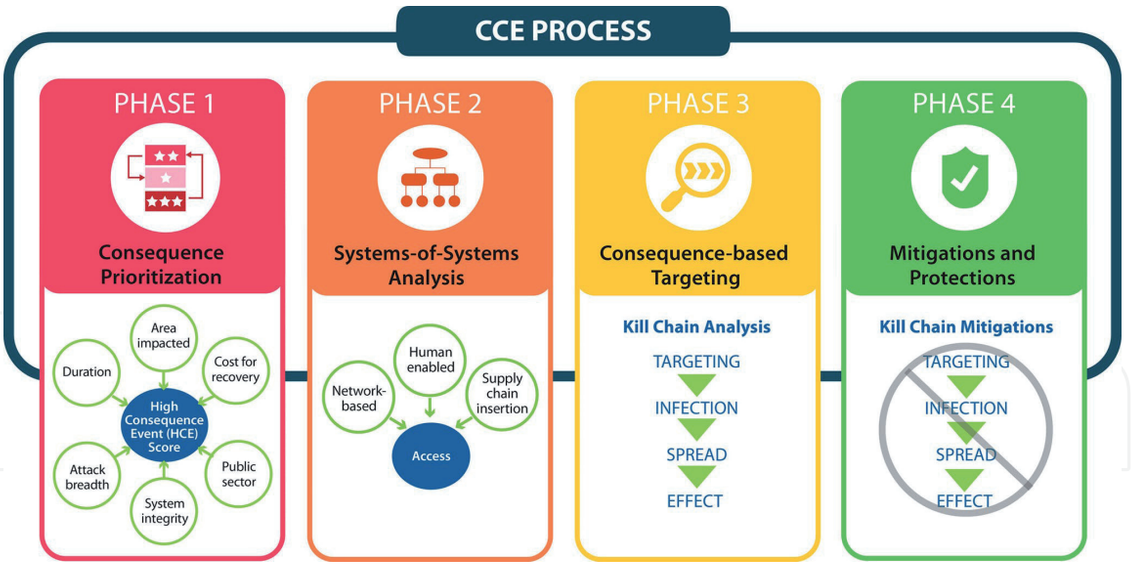

Figure 5.
The four-phase CCE process [34].

Additionally, cyber risk management must not only be considered for nuclear reactor SSCs, but also any digital technology used in their design, operation, and maintenance. For instance, AI/ML and digital twin applications are susceptible to both adversarial and unintentional cyber risk. These technologies are often considered 'black box' techniques in which the end-user is unaware of how the insights are determined. Even if more 'gray box' techniques are used, trust in AI/ML and digital twin models must be established to gain acceptance and approval by operators and regulators. Similarly, adversaries can gain access to these tools and cause data and/or model corruption to adversely affect model operation.

4. Cyber-informed engineering

Digital technology will be increasingly used in both existing and future nuclear reactors. While DI&C enables improved operations and new capabilities, the cyber risks must not only be understood, but risk treatments and protections must be put in place to lower this risk from malicious and unintentional actions. Whereas significant strides have occurred with securing ICT systems, these ICT-based solutions are not always effective for OT systems which are often designed to perform a limited set of functions and therefore have limited processing, memory, storage, retrieval, and proprietary communication protocols. Additionally, cyber risk mitigations have historically been applied after DI&C systems are installed, which limits the range of risk treatments available. On the other hand, applying the concepts of CIE throughout the entire systems engineering lifecycle can reduce overall cyber risk.

Engineers, operators, maintenance personnel, and other technical staff who support the systems engineering process are critical to the design, implementation, and secure operation of complex control systems. Nevertheless, this staff often lacks the necessary knowledge, skills, and abilities to effectively address and mitigate cyber risk. Given the critical functions of DI&C in nuclear reactors, this gap must be filled. For this reason, the Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response is developing a national strategy for CIE to fundamentally change the culture of the engineering discipline to consider cybersecurity as a fundamental design principle.

4.1 Systems Engineering Lifecycle

Figure 6 illustrates the typical stages in the systems engineering lifecycle. While this model is intended to be used iteratively and potentially out-of-order throughout the lifecycle as design modifications occur, the left side of the V-model indicates a top-down approach moving from system to subsystem to component levels and the right side indicates a bottom-up approach through implementation, integration, and testing. This model is useful for both new builds (e.g., new reactor designs) or existing builds (e.g., engineering modifications).

4.2 CIE overview

CIE is a multidisciplinary approach that advocates the use of CIE principles in each of the systems engineering lifecycle stages to ensure that cyber considerations are included in every aspect of design, testing, implementation, operation, maintenance, and disposal or decommissioning [36]. CIE is fundamentally a cyber risk management tool that complements existing OT cybersecurity risk standards and guidelines by incorporating engineering solutions along with ICT and OT cyber solutions to minimize risks from malicious and unintentional cyber incidents. Considering cyber risk and cyber risk treatments early and often throughout the lifecycle provides simpler, more secure solutions at lower cost, precluding the need to use ineffective, bolt-on solutions during later lifecycle stages.

As shown in **Figure 7**, the primary CIE principle that encompasses the entire CIE methodology is cyber risk analysis. The remaining CIE principles are divided into two categories: design principles and organizational principles. The CIE design principles are fundamental engineering design practices and techniques that build cybersecurity and cyber-resilience into DI&C early in the systems engineering lifecycle and then continue to ensure cyber-awareness is maintained throughout the remaining stages. This secure-by-design approach is more effective and less expensive than bolting on security controls after installation as the design can be influenced by factors that improve the ease, simplicity, and effectiveness of cyber considerations without impacting the performance of the intended system function.

Cyber risk is also reduced by instilling cyber-awareness at organizational- or facility-level functions. CIE organizational principles are fundamental cyber practices that enable holistic integration of cyber considerations into other programs within the facility, such as asset inventory, supply chain, response planning, and training.

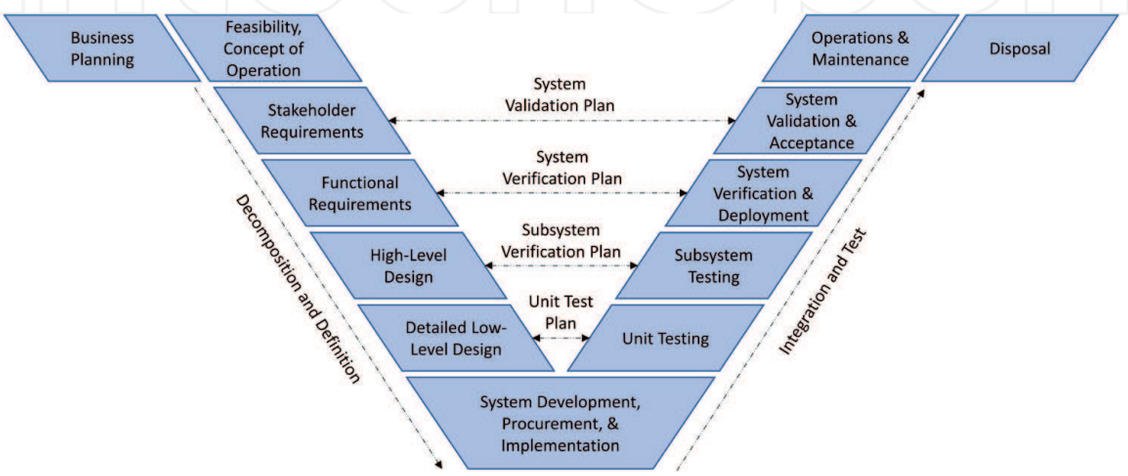

Figure 6.
Systems engineering V-model [35].

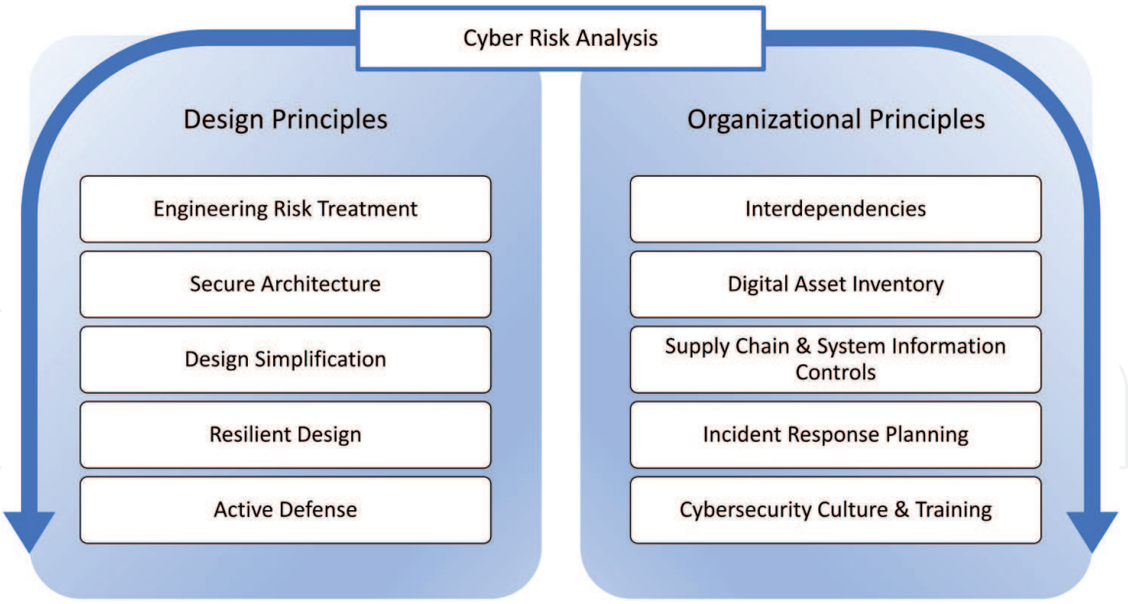

Figure 7.
CIE principles adapted from [36].

4.3 Cyber risk analysis

While cyber risk and cyber risk analysis were discussed in Section 3, it is important to remember that consequence-driven risk analysis is necessary to prioritize design requirements and risk treatments of those digital SSCs required for ensuring reactor safety and the health and safety of the public. Like the CCE methodology, since resources are often limited, organizations should first ensure that the most stringent protections are around those critical functions that, if compromised or lost, could lead to unacceptable radiological consequences, sabotage, or theft of SNM.

4.4 CIE design principles

4.4.1 Engineering risk treatment

Risk management is the process of identifying, evaluating, and responding to risk. Traditional risk treatments for responding to risk include risk avoidance or elimination, risk transference, risk mitigation, and risk acceptance. As shown in **Figure 8**, engineering risk treatments for cyber risk are similar, where risk can be designed out, shifted to another organization, mitigated with security controls or countermeasures, or accepted by making a conscious decision to tolerate the risk without implementing changes.

Security controls, as identified by National Institute of Standards and Technology (NIST) SP 800-82 [37], NRC Regulatory Guide (RG) 5.71 [24], or NEI 08-09 [25] are typically considered administrative, physical, or technical. As indicated in **Figure 8**, these controls mitigate cyber risk that cannot be eliminated. Unfortunately, engineering risk treatments, including security controls, are typically not considered until after installation. However, waiting until after installation is often too late to provide adequate protection. On the other hand, implementing engineering risk treatments during design stages can actually eliminate specifically identified risks by designing it out altogether or more efficiently and effectively reduce risk by incorporating security controls into the design.

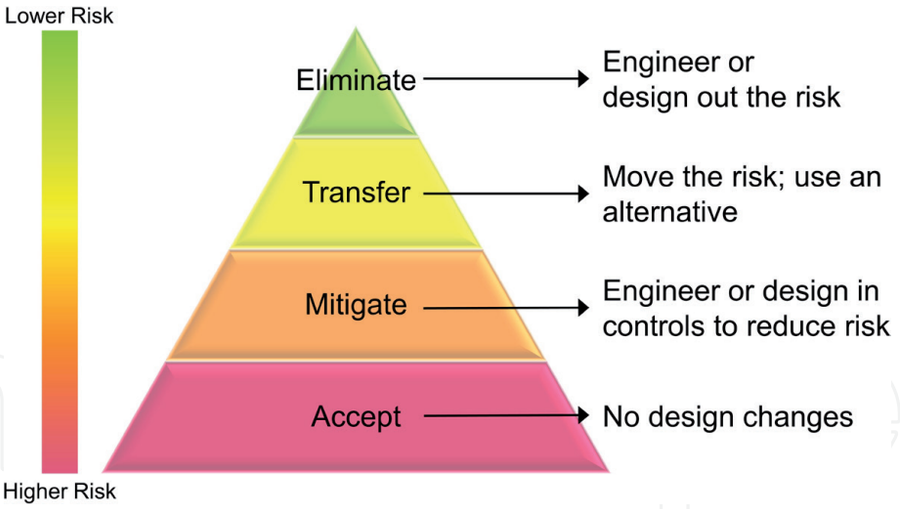

Figure 8.
Engineering cyber risk treatments [35].

4.4.2 Secure architecture

The goal of the secure architecture CIE principle is to establish network and system architectures that segregate and limit data flows to trusted devices and connections within and between subsystems, systems, and systems of systems. Properly designed architectures reduce cyber risk by isolating critical functions, minimizing the cyber-attack surface, and lowering the probability of unauthorized access or compromise of critical SSCs.

To ensure defense in depth, the design should consider use of isolated (e.g., air-gapped) or segregated network levels and zones, boundary devices, data flow rules, and unidirectional, deterministic communication, such as data diodes. In the United States, NRC Regulatory Guide 5.71 recommends power reactors to implement a defensive architecture with only one-way data flow from safety and security network levels outward to the plant network [24]. Internationally, as illustrated in **Figure 9**, the IAEA recommends implementing security levels with common requirements and zones separated by decoupling devices, such as data diodes and other boundary devices, such as gateways, routers, or firewalls, to minimize communications to untrusted devices [38]. Engineers should consider these secure architecture approaches during design stages to limit overall risks from compromised pathways or devices.

4.4.3 Design simplification

A cyber incident can only adversely impact DI&C functions if a vulnerability is exploited by a threat (intentional or unintentional). Vulnerabilities decrease as the complexity of DI&C decreases. Thus, the goal of the design simplification principle is to reduce the complexity of the system, component, and architecture while maintaining the intended function. Design simplification minimizes vulnerabilities and reduces overall cyber risk.

Design simplification is considered in conjunction with the secure architecture, resilient design, and engineering risk treatment principles. Complex or overbuilt designs result in a digital footprint larger than necessary. As the number of digital assets increases in a system, the number of digital failure possibilities and exploit locations also increases. Additionally, it is possible for adversaries to repurpose unused or latent functions and features on SSCs to behave in unanticipated ways.

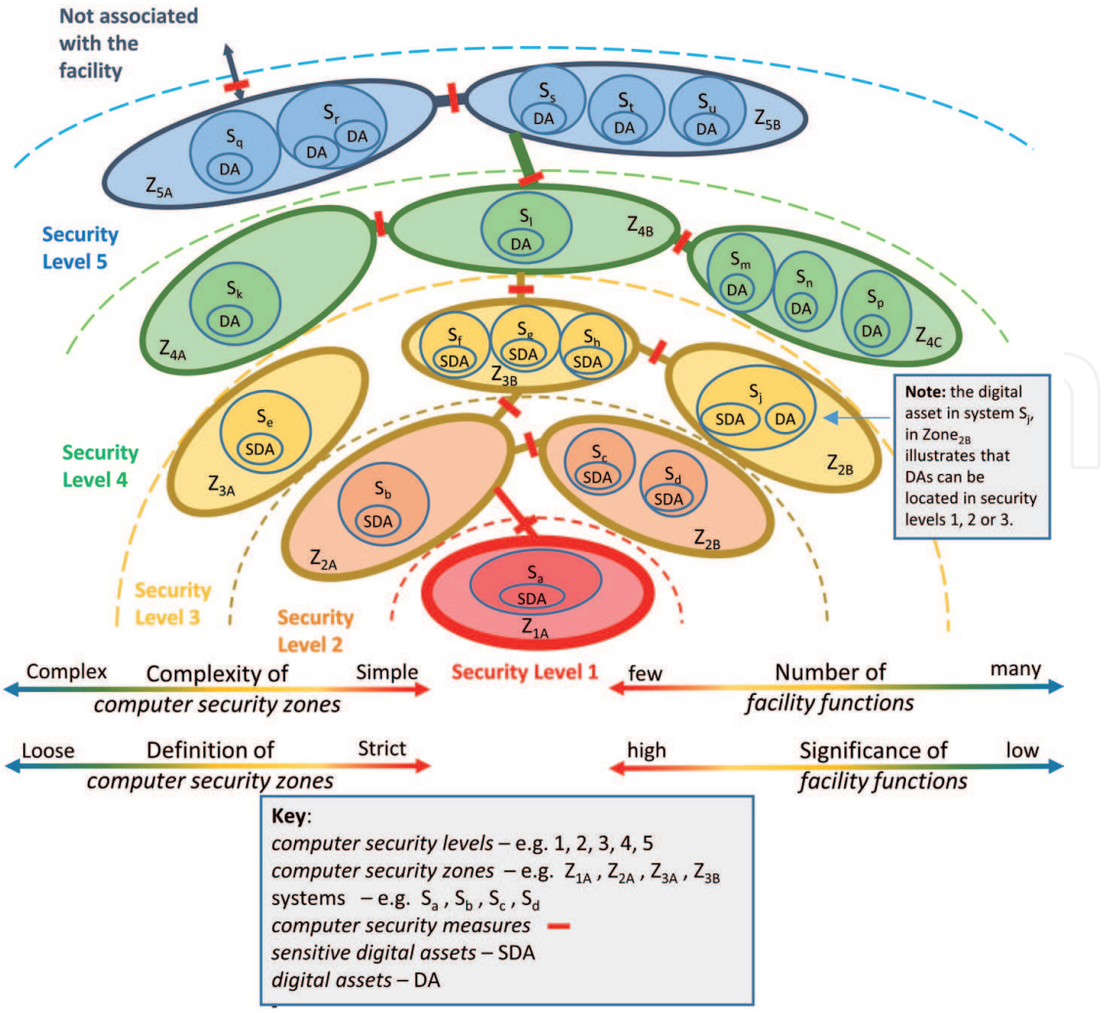

Figure 9.
Example implementation of a secure architecture [38].

On the other hand, simplifying the design, such as by using simpler digital devices or hardening the system by eliminating, limiting, or disabling unnecessary functions or capabilities, minimizes the overall cyber-attack surface and reduces vulnerabilities. The intent of design simplification is to simplify the engineering design itself, not sacrifice security requirements for the sake of simplicity. Nevertheless, in cases where extreme safeguards are required, analog I&C may be implemented instead of DI&C to protect against cyber incidents.

4.4.4 Resilient design

Resilience is a system's capability to withstand internal and external disruptions, including equipment failure, grid disturbances, or cyber incidents. A control system is resilient if it continues to carry out its mission by providing its required functionality despite disturbances that may cause disruptions or degradation. In nuclear reactors, general design criteria of separation, redundancy, diversity, and defense in depth are used for designing safety-related systems. Separation and independence are achieved by physical separation and electrical isolation. Redundancy is achieved by using more than one component to perform the same function. Diversity is achieved by using different technology within the system and with the redundant components.

Current DI&C systems operate in an untrusted environment, which presumes that users, devices, and systems cannot be trusted (e.g., users can be unauthorized,

devices can be infected with malware). Additionally, it is impossible to design DI&C systems to withstand every malicious or unintentional cyber incident. Thus, resilient design is required to ensure continued safe and secure operation of the reactor and facility not only during an incident, but afterward as well.

While safety-related DI&C systems in nuclear reactors should be designed using the general design criteria, consideration should be given to designing similar features into non-safety DI&C systems to address this zero-trust paradigm, depending on the cyber risk prioritization. The objective of resilient DI&C design is to ensure continued operation of critical functions when possible, or graceful degradation when not possible, in the event of an SSC failure or cyber incident. Failure of one function, device, or system should not result in failure of another function. System design and control logic should attempt to eliminate the possibility of such cascading failures.

Additionally, resilient design may also include contingency planning and situational awareness. Contingency planning provides alternative methods for continued operation of critical functions. Using techniques, such as network and system monitoring, to provide situational awareness enables rapid decision making that may be needed for continued operation during a cyber incident. Moreover, operators have been trained to trust their instruments and indicators. This training model may need to be revisited due to the new zero-trust environment.

Finally, it should be noted that while resilient design may seem contrary to design simplification, the intent is to ensure that critical functions remain operational during a cyber incident. If additional devices are required to adequately assure resilience, there may be a tradeoff between resiliency and simplicity.

4.4.5 Active defense

Security countermeasures and protections can be applied passively or actively. Passive defenses include those defensive architecture techniques described in Section 4.4.2. These passive defenses establish barriers using defense-in-depth techniques to deter and protect against a malicious adversary. This technique, however, is static and reactionary. It is also at a disadvantage for defending against dynamic and adaptive adversary capabilities.

Instead of reliance on passive capabilities, engineers need to build in active defenses to preemptively prevent, detect, and respond to cyber incidents. This paradigm shift is needed to proactively identify malicious and inadvertent cyber incidents to quickly stop the incident and remove the threat before degradation or unrecoverable damage occurs. Active defenses include security information event monitoring and other real-time anomaly detection and response tools that may not yet be developed or deployed. The objective is to enhance resilience capabilities by improving operational situational awareness via dynamic and testable strategies. Ideally, active defense tools can identify cyber anomalies in all five threat vectors (e.g., wired networks, wireless networks, portable media and maintenance devices, insiders, and supply chain).

4.5 CIE Organizational principles

4.5.1 Interdependencies

The CIE organizational principles listed in **Figure 7** are those fundamental cybersecurity practices that enable holistic integration of cybersecurity into other programs within the facility or organization. Technical and administrative interdependencies are necessary for safe and secure reactor operation. From a technical

perspective, this principle ensures that cybersecurity is considered within all the interconnections between systems and systems of systems, including extended data pathways. Additionally, 10CFR73.54 not only requires adequate protection of safety-related and important-to-safety SSCs but also those support systems relied upon to ensure safe operation of those functions. Support systems may include power, communications, water, or HVAC. Even though there is the potential for adverse safety or security consequences if a cyber incident impacts a support system, these interdependencies are often overlooked.

From an administrative perspective, the interdependency principle promotes a multidisciplinary approach to ensure all project personnel are involved. For instance, when designing or modifying a reactor safety system to perform specific functions, a design engineer relies on safety engineers to provide expertise on safety-related functions, quality engineers to verify correct design implementations, maintenance personnel to provide perspectives on accessibility and maintainability, operators to provide operational feedback under various conditions, and competent authorities to provide safety and security requirements.

With the shift towards DI&C, cyber engineers or specialists should also be included throughout the systems engineering lifecycle to provide valuable insight into cyber risk and risk (and cost) minimization strategies, such as cyber risk treatments, policies, and procedures. Additionally, it is paramount to ensure other disciplines, such as engineering, safety, risk, design, maintenance, operations, human factors, and ICT, are knowledgeable about these system interdependencies and the potential consequences of a cyber incident on a facility function, digital asset, system, or system of systems. While the nature of the multidisciplinary engagements may differ with each stage, similar to safety, the intent is to ensure cyber engineering remains a core domain throughout the entire lifecycle.

4.5.2 Digital asset inventory

Although new installations or modifications to existing facilities will include equipment database inventories of SSCs, this list often is out-of-date, incomplete, and without enough information to support cyber requirements and incident response decisions. Thus, the digital asset inventory CIE principle is intended to ensure that an accurate as-built digital asset inventory is maintained throughout the systems engineering lifecycle, including initial design, maintenance, configuration changes, and upgrades or modifications.

It is impossible to provide adequate protection against cyber incidents if there are unknown digital assets installed in a facility. Therefore, it is necessary to establish complete, accurate, and detailed asset inventories for the entire digital bill of materials (DBOM), including make, model, and version information for hardware, firmware, and software. For instance, if a vendor or intelligence agency provides vulnerability and threat information for a specific digital asset, a facility can easily use their inventory to determine if they have that asset installed. Accurate digital asset inventories improve the overall vulnerability management process. Without the inventory, it is very difficult to track whether newly identified cyber risks are applicable to the facility.

In addition to the DBOM, configuration information, backup requirements, and restoration information should be maintained for each digital SSC. Since cyber compromises do occur within the supply chain and early lifecycle stages, this complete design record should be maintained under secured configuration control such that all modifications or updates are captured. When used in conjunction with the incident response planning principle, this detailed information can be used to restore or rebuild a system after a cyber incident.

4.5.3 Supply chain and system information controls

The use of third-party digital hardware, firmware, and software has increased tremendously in the past several decades. The cost-benefit of purchasing general purpose multifunctional digital devices has become a mainstay for many custom in-house and engineered solutions. However, since vendors, integrators, and service providers are profit driven, they will likely not invest in additional cyber security designs and controls for their products and services unless required by procurement specifications.

Since the supply chain is one of five threat vectors into a nuclear facility, it is imperative to develop supply chain controls that incorporate techniques into the procurement and acquisition process to prevent malicious or inadvertent compromise of hardware, firmware, software, and system information, where system information is defined as the "complete record of information regarding a digital system or component, including system level and component level information and/or data such as requirements specifications, design documentation, fabrication, assembly or manufacturing details; validation and verification documentation; operation and maintenance manuals; credential, authentication, or cryptographic information; and product lifecycle plans" [39].

The primary objectives of cyber supply chain risk management include the ability to maintain authenticity, integrity, confidentiality, and exclusivity throughout the system engineering lifecycle [39]. Authenticity assures the components are genuine; integrity assures the components are trustworthy and uncompromised; confidentiality assures there is no unauthorized loss of data or secrets; and exclusivity assures there are limited touchpoints to reduce the number of attack points [40].

A simplified, notional DI&C supply chain cyber-attack surface is illustrated in **Figure 10**. It is important to understand this attack surface so appropriate risk treatments can be implemented to reduce cybersecurity risk throughout the lifecycle. Logically, the parallel use of the design simplification CIE principle reduces this supply chain cyber-attack surface by reducing the number of stakeholders and touchpoints. Ensuring cyber supply chain provenance and trustworthiness is easier with a smaller supply chain cyber-attack surface.

Procurement contracts should include cybersecurity requirements, such as those provided by the Department of Homeland Security [41], the Energy Sector Control Systems Working Group [42], or Electric Power Research Institute [43]. This procurement language should include all aspects of a product or service including the ability to review the supply chain stakeholder's cybersecurity program, including any assessments or cybersecurity testing. Without inclusion of cybersecurity requirements into procurement contracts, the likelihood of insecure or compromised products and services increases.

It is important to recognize that supply chain cybersecurity is necessary during early lifecycle stages even when only system information is available. Reconnaissance is a primary method used by an adversary to acquire preliminary information about an organization, operations, and system designs. Theft of confidential or proprietary system information may result in loss of intellectual property, counterfeiting, and enable development of future sophisticated cyber-attacks. In addition, compromise or falsification of system information could lead to developers inadvertently including malicious codes, falsified data, latent vulnerabilities, or backdoors into the system or component during supply chain activities.

Unfortunately, protection of sensitive information is historically inadequate—sensitive information can often be found on social media, corporate websites, conferences, business and employment-oriented online services, vendor advertising, and other third-party entities that store nuclear-related information, such as

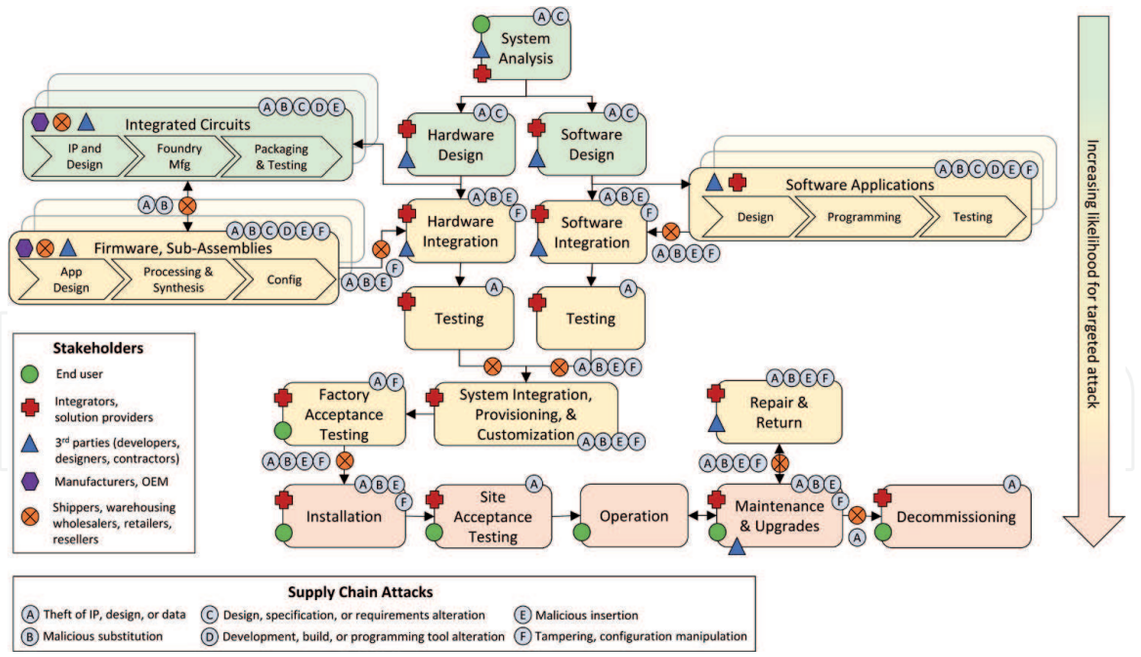

Figure 10.
A notional DI&C supply chain cyber-attack surface illustrating the complexity of the supply chain lifecycle overlaid with potential supply chain attacks at key stakeholder locations and touchpoints [39].

nuclear regulators. Of course, poor cybersecurity hygiene can occur at every stakeholder in the supply chain, including hardware manufacturers, programmers, and integrators, as well as the reactor designer and operator. Since engineering records, asset inventories, master drawings, procedures, specifications, analysis, and other sensitive system information is much more accessible today, responsibility for protecting system information lies not only with the entire nuclear organization but all supply chain stakeholders.

4.5.4 Incident response planning

Incident response planning, in conjunction with contingency planning in resilient design and an accurate and complete digital asset inventory, ensures that procedures, current backups, and accurate configurations are available to respond to and recover from deliberate or inadvertent cyber incidents. Cyber incidents can occur at any stage in the lifecycle. For example, theft of system information or IP can occur during design, introduction of malware by a subcontractor can occur during testing, and downloading of corrupted firmware can occur as part of maintenance. Incident response planning should occur in each stage of the systems engineering lifecycle to safeguard the stakeholder, system information, and DBOM against a cyber incident. IAEA TDL006 [44] and NIST 800-61 [45] provide incident response guidelines.

4.5.5 Cybersecurity culture and training

An organization's culture is demonstrated every day through the actions of its employees. Nuclear facilities are guided by a nuclear safety and security culture which emphasizes protection of public health and safety over other competing goals, such as electricity generation. Personnel are instilled with the understanding that they can and should speak up when there are safety or security concerns. Since cybersecurity is part of the overarching nuclear security policy to guard against theft and sabotage, developing and maintaining a cybersecurity culture and training program is just as important.

The human-in-the-loop is essential for maintaining a robust security posture. As digital technology is prevalent in both OT and ICT systems, every person is responsible for cybersecurity, not just ICT or engineering staff. Similar to the nuclear safety culture, an organization-wide cybersecurity culture and training program will equip all personnel with the knowledge, skills, and abilities to recognize, prevent, and respond to cyber incidents. The goal of CIE is to develop cyber-informed engineers and personnel as opposed to cybersecurity specialists. Development of cyber-awareness and cross-functional cyber capabilities will provide personnel with information on the importance of their role in an organization's overall security plan. Simply recognizing and reporting phishing emails or suspicious activity can prevent an adversary's entry into an organization. Without this knowledge of how cyber incidents can occur and what unauthorized interactions can look like, compromises can remain persistent and undetected, thereby leading to greater consequences for the organization or nuclear reactor.

5. Discussion

Applying the CIE approach throughout the entire systems engineering lifecycle, from design and testing to maintenance and decommissioning, provides enhanced capabilities for cyber protection, detection, and response. **Figure 11** is a notional diagram summarizing potential usage of CIE principles throughout the lifecycle. The primary objective of CIE is to ensure engineers and stakeholders consider CIE principles during each activity within every stage of the lifecycle. Continual cyber risk analysis ensures that new or updated consequences, threats, and vulnerabilities are quickly identified. CIE design principles ensure that approaches to address and reduce the identified cyber risk are considered to the greatest extent possible. And, finally, CIE organizational principles provide long-term cyber risk reduction benefits by holistically integrating cyber considerations throughout the facility and organization.

Since nuclear engineering projects differ in scope, it is impractical to define a standard level of effort for all CIE principles across each stage. For instance, the design and construction of an advanced reactor will likely have a very long timeline

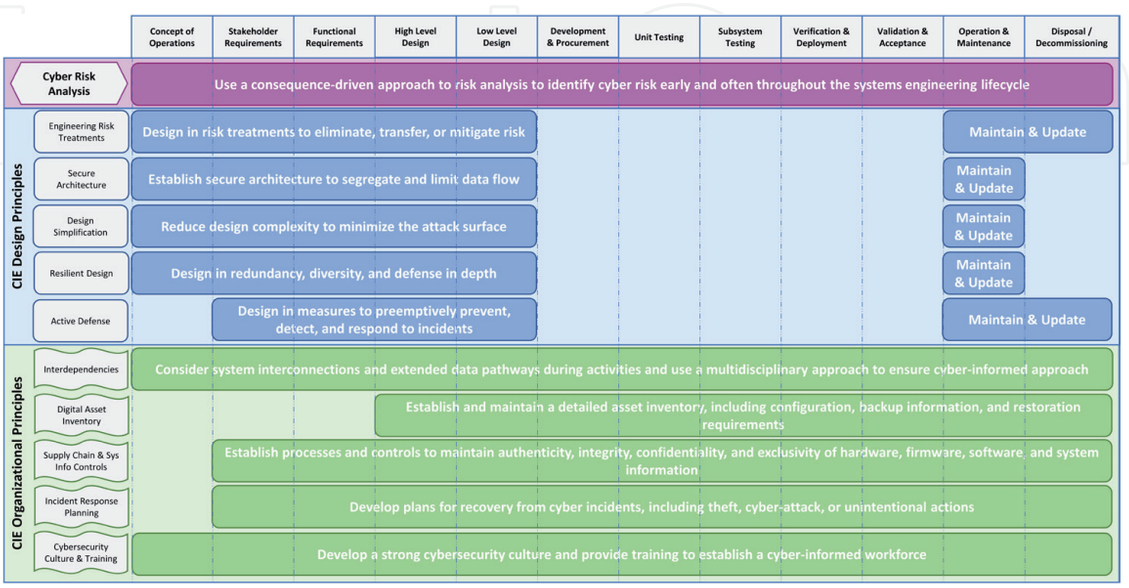

Figure 11.
Notional usage of CIE principles throughout the systems engineering lifecycle.

and involve multiple organizations, while a simple modification at a research reactor may occur relatively quickly and include only a small group of people. As an applied integrated energy system example, the CIE approach was used during the high-level design of a hydrogen generation project in which heat and electricity were provided by an interconnected NPP [35]. The use of a multi-disciplinary team to address system of system interdependencies through a structured risk analysis process resulted in new insights into the potential for both adversarial and unintentional cyber risks. As a result, the system was immediately redesigned to eliminate specific identified risk as well as to incorporate more simplified and resilient design features [35].

6. Conclusions

With the continued modernization of the existing nuclear fleet and future advanced reactor designs and applications, the use of DI&C in nuclear reactors will continue to grow. Additionally, once DI&C is installed or new reactors are commissioned, maintenance and updates will occur throughout a reactor's lifetime. The fundamental CIE objective to consider cyber requirements from the onset of conceptual design provides expanded opportunities for recognizing cyber risks, thereby enabling cyber risk reduction through redesign prior to initiation of any procurement or construction activities. While CIE can positively impact design modifications in existing reactors, it may have even greater potential in improving the security posture of new reactors. Convening multidisciplinary teams will enable novel cyber solutions that otherwise would not be possible, thus minimizing cybersecurity-related costs and expensive rework later in the lifecycle. Addressing cyber concerns after installation with bolt-on solutions is arguably less effective and less efficient, especially given the fact that some SSCs may not tolerate or allow the use of security controls.

CIE is a multidisciplinary approach incorporating design and organizational principles to protect digital technology from cyber risk. The continued adoption of CIE in nuclear organizations as well as the development of curriculum in academic engineering and industry education programs furthers the goal of globally reducing nuclear cyber risk.

Acknowledgements

The authors wish to acknowledge the contributions of Dr. Katya Le Blanc and Timothy R. McJunkin, who provided critical reviews and suggestions.

Funding

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

Conflict of interest

The authors declare no conflict of interest.

Acronyms

AI	artificial intelligence
CDA	critical digital asset
CCE	consequence-driven, cyber-informed engineering
CIE	cyber-informed engineering
DBA	design basis accident
DBOM	digital bill of material
DBT	design basis threat
DI&C	digital instrumentation and control
DOE	Department of Energy
ESFAS	engineered safety feature actuation system
GDC	general design criteria
HCE	high consequence event
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IIoT	industrial internet of things
IoT	internet of things
LWR	light water reactor
ML	machine learning
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSS	nuclear security series
OT	operational technology
PRA	probabilistic risk analysis
RPS	reactor protection system
SMR	small modular reactor
SNM	special nuclear material
SSC	systems, structures, and components
USB	universal serial bus

Author details

Shannon Eggers* and Robert Anderson
Idaho National Laboratory, Idaho Falls, ID, USA

*Address all correspondence to: shannon.eggers@inl.gov

References

[1] Stout TM, Williams TJ. Pioneering work in the field of computer process control. IEEE Annals of the History of Computing. 1995;**17**(1):6-18. DOI: 10.1109/85.366507

[2] NEI. NEI 10-04: Identifying systems and assets subject to the cyber security rule. Revision 2. Washington, DC: Nuclear Energy Institute; 2012. Available from: https://www.nrc.gov/docs/ML1218/ML12180A081.pdf

[3] IEEE. IEEE 308-1971—IEEE standard criteria for class 1E electric systems for nucler power generating stations. New York, NY: Institute of Electrical and Electronics Engineers; 1971. DOI: 10.1109/IEEESTD.1971.6714366

[4] 10 C.F.R. § 50 Appendix A. Domestic Licensing of Production and Utiliziation Facilities. 2007. Available from: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appa.html

[5] IEEE. IEEE 279-1971—Criteria for safety systems for nuclear power generating stations. New York, NY: Institute of Electrical and Electronics Engineers; 1971. DOI: 10.1109/IEEESTD.2012.6125207

[6] IEEE. IEEE 603-1991—IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. New York, NY: Institute of Electrical and Electronics Engineers; 1991. DOI: 10.1109/IEEESTD.1991.101077

[7] NRC. Regulatory Guide 1.152. Revision 3. Criteria for use of computers in safety systems of nuclear power plants. Washington, DC: U.S. Nuclear Regulatory Commission; 2011. Available from: https://www.nrc.gov/docs/ML1028/ML102870022.pdf

[8] IEEE. IEEE 7-4.3.2-2003—IEEE standard for digital computers in safety systems of nuclear power generating stations. New York, NY: Institute of Electrical and Electronics Engineers; 2003. DOI: 10.1109/IEEESTD.2003.94419

[9] IEC. IEC 61513:2011. Nuclear Power Plants—Instrumentation and Control Important to Safety—General Requirements for Systems. Geneva, Switzerland: Rev 2.0. International Electrotechnical Commission; 2011. Available from: https://webstore.iec.ch/publication/5532

[10] IAEA. Specific Safety Requirements No. SSR-2/1. Safety of Nuclear Power Plants: Design (Rev 1). Vienna: International Atomic Energy Agency; 2016. Report No. STI/PUB/1534. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1534_web.pdf

[11] IAEA. Specific Safety Guide No. SSG-39. Design of Instrumentation and Control Systems for Nuclear Power Plants. Vienna: International Atomic Energy Agency; 2016. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf

[12] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis. 1981;**1**(1):11-27, 1981. DOI: 10.1111/j.1539-6924.1981.tb01350.x

[13] Eggers S, Le Blanc K. Survey of cyber risk analysis techniques for use in the nuclear industry. Progress in Nuclear Energy. 2021;**140**:1. DOI: 10.1016/j.pnucene.2021.103908

[14] NRC. NRC Information Notice 2003-14: Potential vulnerability of plant computer network to worm infection. Washington, DC: U.S. Nuclear Regulatory Commission; 2003. Document No. IN200314. Available from: https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf

[15] NRC. NRC Information Notice 2007-15: Effects of ethernet-based, non-safety related controls on the safe and continued operation of nuclear power stations. Washington, DC: U.S. Nuclear Regulatory Commission; 2007. Available from: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf

[16] Langner R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy. 2011;**9**(3):49-51. DOI: 10.1109/MSP.2011.67

[17] Krebs B. Cyber incident blamed for nuclear power plant shutdown. Washington Post. June 5, 2008. Available from: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

[18] Graham M. Context threat intelligence—the Monju incident. New York, NY: Context Information Security; 2014. Available from: https://www.contextis.com/en/blog/context-threat-intelligence-the-monju-incident

[19] 10 C.F.R. § 73.54. Protection of Digital Computer and Communication Systems and Networks. 2009. Available from: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

[20] Common Vulnerabilities and Exposures (CVE). The MITRE Corporation. Available from: https://cve.mitre.org/ [Accessed: September 29, 2020]

[21] Common Weakness Enumeration (CWE). The MITRE Corporation. Available from: https://cwe.mitre.org/ [Accessed: September 29, 2020]

[22] Common Vulnerability Scoring System (CVSS). FiRST. Available from: https://www.first.org/cvss/ [Accessed: September 29, 2020]

[23] ICS-CERT Alerts. Cybersecurity and Infrastructure Security Agency. Available from: https://us-cert.cisa.gov/ics/alerts [Accessed: September 29, 2020]

[24] NRC. Regulatory Guide 5.71. Cyber security programs for nuclear facilities. Washington, DC: U.S. Nuclear Regulatory Commission; 2010. Available from: http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf

[25] NEI. NEI 08-09: Cyber security plan for nuclear power reactors. Revision 6. Washington, DC: Nuclear Energy Institute; 2010. Available from: https://www.nrc.gov/docs/ML1011/ML101180437.pdf

[26] NEI. NEI 13-10: Cyber security control assessments. Revision 6. Washington, DC: Nuclear Energy Institute; 2017. Available from: https://www.nrc.gov/docs/ML1723/ML17234A615.pdf

[27] IAEA. Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). Vienna: International Atomic Energy Agency; 2011. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

[28] IAEA. Nuclear Security Series No. 17. Computer Security at Nuclear Facilities. Vienna: International Atomic Energy Agency; 2011. Available from: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

[29] IAEA. NSS 42-G. Computer Security for Nuclear Security. Vienna: International Atomic Energy Agency; 2021. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf

[30] IAEA. NSS 33-T. Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Vienna: International Atomic Energy Agency;

2018. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf

[31] IEC. IEC 62645:2019. Nuclear power plants—Instrumentation, control and electric power systems—Cybersecurity requirements. Geneva, Switzerland: International Electrotechnical Commission; 2019. Available from: https://webstore.iec.ch/publication/32904

[32] IEC. IEC 62443-3-2. Security risk assessment and system design. Geneva, Switzerland: International Electrotechnical Commission; 2020. Available from: https://webstore.iec.ch/publication/30727

[33] Bochman AA, Freeman S. Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE). Boca Raton, FL: CRC Press; 2021. DOI: 10.4324/9780367491161

[34] Consequence-Driven Cyber-Informed Engineering. Idaho National Laboratory. Available from: https://inl.gov/cce/ [Accessed: November 8, 2021]

[35] Eggers S, Le Blanc K, Youngblood R, McJunkin T, Frick K, Wendt D, et al., editors. Cyber-Informed Engineering case study of an integrated hydrogen generation plant. ANS 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT); 2021 June 13-16, 2021; Online Virtual Meeting: American Nuclear Society.

[36] Anderson RS, Benjamin J, Wright VL, Quinones L, Paz J. Cyber-Informed Engineering. Idaho Falls, ID: Idaho National Laboratory; 2017. DOI: 10.2172/1369373

[37] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A. SP 800-82. Revision 2: Guide to industrial control systems (ICS) security. Gaithersburg, MD: National Institute of Standards and Technology; 2015. DOI: 10.6028/NIST.SP.800-82r2

[38] IAEA. NSS 17-T. Rev 1. Computer Security Tecniques for Nuclear Facilities. Vienna: International Atomic Energy Agency; 2021. Available from: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf

[39] Eggers S. A novel approach for analyzing the nuclear supply chain cyber-attack surface. Nuclear Engineering and Technology. 2021;**53**(3):879-887. DOI: 10.1016/j.net.2020.08.021

[40] Windelberg M. Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection. 2016;**12**:4-11. DOI: 10.1016/j.ijcip.2015.11.003

[41] DHS. Cyber Security Procurement Language for Control Systems. Washington, DC: Department of Homeland Security; 2009. Available from: https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

[42] ESCSWG. Cybersecurity procurement language for energy delivery systems. Washington DC: Energy Sector Control Systems Working Group; 2014. Available from: https://www.energy.gov/sites/default/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

[43] EPRI. Cyber Security in the supply chain: Cyber security procurement methodology. Revision 2. Palo Alto, CA: Electric Power Research Institute; 2018. Document No. TR 3002012753

[44] IAEA. TDL005. Computer security incident response planning at nuclear facilities. International Atomic Energy Agency; 2016. Available from: http://

www-pub.iaea.org/MTCD/
Publications/PDF/TDL005web.pdf

[45] NIST. SP 800-61. Rev 2. Computer security incident handling guide. Gaithersburg, MD: National Institute of Standards and Technology; 2012. DOI: 10.6028/NIST.SP.800-61r2