INL/CON-21-61671-Revision-1



# Cyber-Informed Engineering Case Study of an Integrated Hydrogen Generation Plant

June 2021

Shannon Leigh Eggers, Katya L Le Blanc, Robert W Youngblood III, Timothy R McJunkin, Konor L Frick, Daniel S Wendt, Robert S Anderson

*Changing the World's Energy Future*


*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/CON-21-61671-Revision-1

# Cyber-Informed Engineering Case Study of an Integrated Hydrogen Generation Plant

**Shannon Leigh Eggers, Katya L Le Blanc, Robert W Youngblood III, Timothy R McJunkin, Konor L Frick, Daniel S Wendt, Robert S Anderson**

**June 2021**

**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**

# CYBER-INFORMED ENGINEERING CASE STUDY OF AN INTEGRATED HYDROGEN GENERATION PLANT

**Shannon Eggers, Katya Le Blanc, Robert Youngblood, Tim McJunkin, Konor Frick, Daniel Wendt, Robert Anderson**
Idaho National Laboratory
1955 N. Fremont Ave, Idaho Falls, ID 83415
shannon.eggers@inl.gov; katya.leblanc@inl.gov; robert.youngblood@inl.gov;
timothy.mcjunkin@inl.gov; konor.frick@inl.gov; daniel.wendt@inl.gov; robert.anderson@inl.gov

## ABSTRACT

Strategies for securing digital instrumentation and control (I&C) systems within the nuclear industry are provided by multiple standards and guidance documents. However, since selection and use of security controls outlined in these documents are frequently only considered during or after installation, there are often limitations on their use, such as technological constraints related to design or operation. Furthermore, alternative controls intended to provide the same or similar security countermeasure as the primary control may also be infeasible at these stages, leaving the I&C system vulnerable to cyber-attacks. The limitations associated with 'bolting on' security controls late in the systems engineering lifecycle can be reduced by integrating Cyber-Informed Engineering (CIE) into the process. This paper evaluates the use of CIE during the high-level design stage of a hydrogen generation project where heat and electricity are provided by a nuclear power plant. Applying CIE to this project highlighted potential cyber vulnerabilities of the initial design, leading to recommendations for process flow and I&C system design modifications to reduce, and at times eliminate, the risk from both deliberate and unintentional cyber incidents.

*Key Words*: Cyber-Informed Engineering, Cybersecurity, Integrated Energy Systems

## 1 INTRODUCTION

As a potential solution for increasing a light-water reactor's (LWR) economic viability, researchers have investigated new design concepts to integrate hydrogen generation plants (H2) with the thermal cycle of an LWR (Figure 1) [1]. The new digital instrumentation and control (I&C) systems required for integration will expand the digital footprint of the LWR. Since this expansion introduces new possibilities of digital failures and cyber hazards to the LWR, it is important to incorporate cybersecurity into the systems engineering lifecycle to proactively identify, eliminate, and/or mitigate these hazards. Strategies for securing digital I&C systems within the nuclear industry are provided by multiple standards and guidance documents [2-11], but these practices are often only considered during or after installation. This paper provides an overview of Cyber-Informed Engineering (CIE), how it was used during the high-level design stage of an integrated H2/LWR project, and how continued use throughout the project can enhance overall cyber-resilience of the final product.

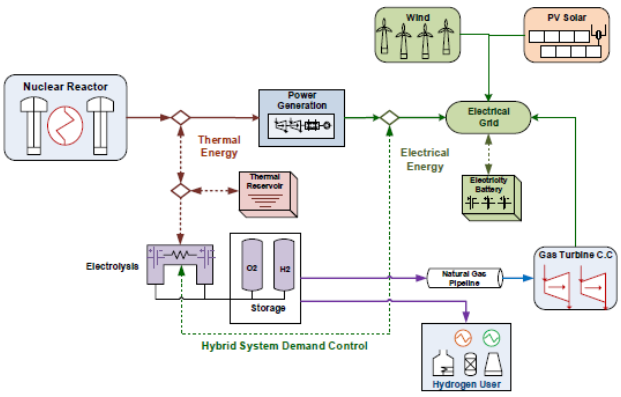


**Figure 1. LWR hybrid plant for H2 production [1].**

# 2 BACKGROUND

## 2.1 Cyber-Informed Engineering Throughout the Systems Engineering Lifecycle

CIE is a multidisciplinary approach to integrating cybersecurity concepts into all phases of the systems engineering lifecycle. Using CIE provides stakeholders unfamiliar with cybersecurity practices the knowledge to incorporate risk management techniques to understand, eliminate, and/or mitigate cyber risks from the conceptual design phase through operation, maintenance, and disposal phases [12]. Considering and designing for cyber risks early in the lifecycle provides a simplified, more secure solution at lower cost. Influencing the design early in the process also reduces the potential for using ineffective bolted-on cybersecurity solutions during later lifecycle phases.

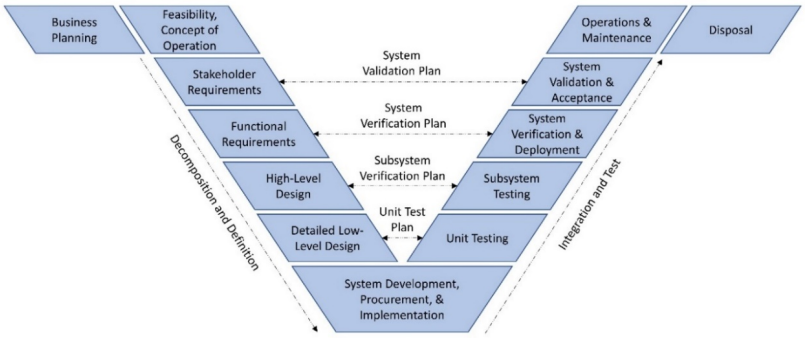


**Figure 2. Systems engineering lifecycle V-model adapted from [13].**

The stages in the systems engineering lifecycle are often graphically represented as a V-model, as shown in Figure 2 (adapted from [13]). The left branch of the model depicts top-down development moving from system level to subsystem level to component level. The right branch depicts bottom-up implementation and integration combined with relevant testing to validate and verify the requirements and design are adequately developed and integrated. Using the V-model leads to a repetitive process as testing and modifications occur.

CIE provides fundamental tools for incorporating solutions that combine engineering, information and communications technology (ICT), and operations technology (OT) to minimize cyber risk throughout each of the lifecycle stages. It is important to note that these stages are not necessarily linear—the stages may be performed out-of-order and/or iteratively as requirements and design details are modified throughout the lifecycle.

## 2.2 CIE Elements

Figure 3 illustrates CIE elements adapted from the framework provided by Anderson *et al.* [12]. The CIE secure-by-design elements are those fundamental cybersecurity engineering design practices and techniques that build cybersecurity and cyber-resilience into the system early in the lifecycle. These elements are also considered as the system progresses through each lifecycle stage to ensure the security posture is maintained as changes occur in both the system and threat environment. Designing and building cybersecurity into the system upon project initiation and then maintaining this cyber-aware approach through system maturity is more effective and less expensive than bolting on security controls during the system verification, deployment, or later stages. Also, the design may be influenced by factors that would improve the ease, simplicity, and effectiveness of cybersecurity for the system throughout the lifecycle without impacting the performance of the intended system objectives.

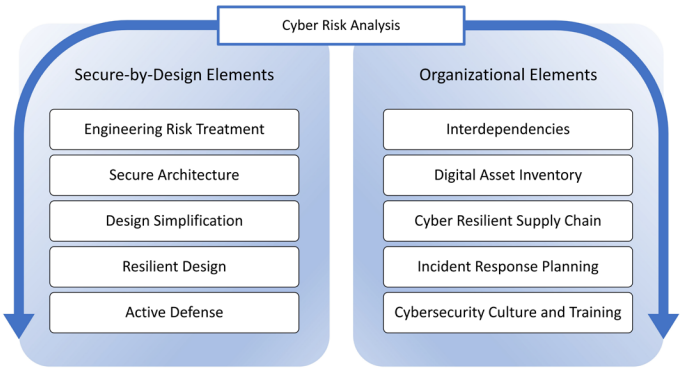


**Figure 3. CIE elements adapted from [12].**

# 3 CASE STUDY: CIE APPLIED TO AN INTEGRATED H2/LWR PROJECT

## 3.1 Integrated H2/LWR Project Overview

A CIE case study based on the elements in Figure 3 was performed as an H2/LWR project iterated through the feasibility, stakeholder requirements, functional requirements, and high-level design stages of the system engineering lifecycle shown in Figure 2. The initial H2/LWR project considerations were focused on establishing technical objectives and economic feasibility of the design to determine if and how the integrated energy system would provide additional revenue streams for an LWR [14]. After economic analysis determined operational characteristics required for both the LWR and H2 plant, high-level process flow diagrams were developed to describe the interconnection between an LWR steam cycle and a high-temperature solid-oxide electrolysis (HTSE) system used to split water into hydrogen and oxygen. As shown in Figure 4, the conceptual flow diagram included an intermediate processing facility (IPF) as a tertiary loop using heat exchangers (HX) to transfer heat from the LWR to the HTSE system. One pump circulates water through the IPF loop while a second pump returns condensate to the LWR.

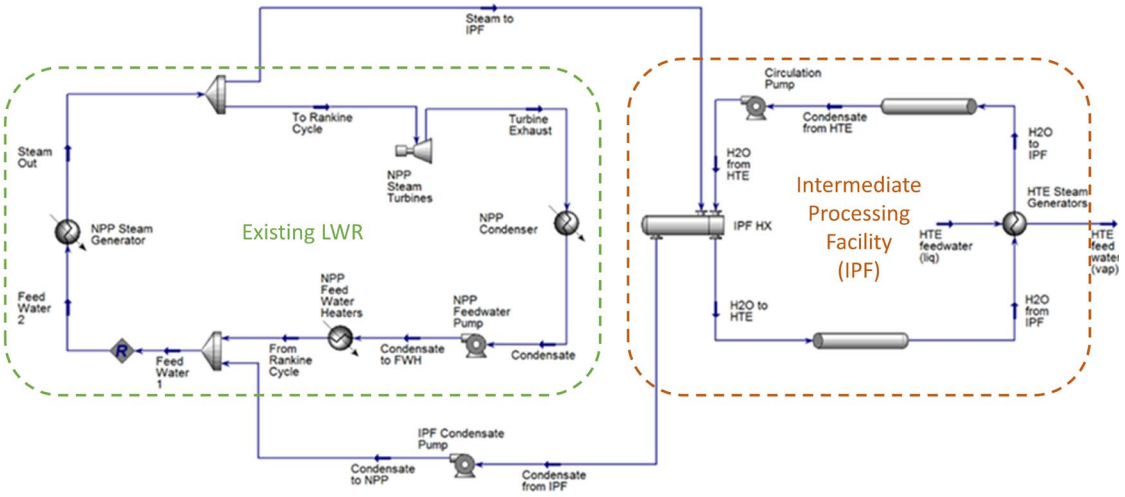


**Figure 4. Initial conceptual process flow diagram for the LWR and H2 plant interconnection.**

## 3.2 CIE Activities Performed During the High-Level Design Stage

Prior to reaching the high-level design stage, operational objectives, including a concept of control and communication, may be identified but not yet clearly defined. Therefore, the high-level design stage in the systems engineering lifecycle is characterized by developing these system and subsystem level technical engineering details. The high-level design may include systems architecture, component, and process flow requirements as well as actuators, sensors, data pathways, and control systems. It is also common to develop systems of systems interactions and dependencies in this stage. The following sections define the CIE elements considered in this case study on the project's high-level design, describe how they were used, and identify the benefits achieved.

### 3.2.1 Cyber risk analysis

Cyber risk is a function of threats, vulnerabilities, and consequences, including likelihood of scenario success given these threats and vulnerabilities:

$$Cyber\ Risk = f(threat, vulnerability, consequence) \quad (1)$$

Cyber risk analysis, therefore, includes a combination of threat analysis, vulnerability analysis, and consequence analysis to evaluate potential exposure from deliberate or unintentional cyber incidents. Consequence analysis identifies impacts to a system from a cyber incident. Potential consequences from

cyber incidents against LWRs include adverse impacts to the health and safety of the public from radiological release, financial impacts from lost generation or equipment damage, and reputation impacts from public perception and loss of public confidence.

During the design stages, it is important to evaluate the consequences or impacts that either a deliberate or inadvertent cyber incident has on the functions in a system and/or system of systems. The impacts of cyber incidents occurring on a digital I&C system range from loss of confidential information and stored secrets to loss of system integrity or availability, leading to mal-operation and/or failure of system functions. Consequence analysis also includes identification of critical functions to ensure they are adequately protected against a cyber incident. Evaluating cyber risk during the design phase enables the engineering team to identify engineering risk treatments, including alternative designs or approaches to eliminate, minimize, or mitigate hazards. Table I provides a sampling of potential high-consequence events associated with digital I&C cyber incidents at an LWR.

**Table I. Potential high-impact consequences from a cyber incident on an LWR digital system.**

| Potential Consequence | Functional Impact | Cyber Incident Examples |
|---|---|---|
| Radiation release | Failure of a safety function to actuate when needed | Digital reactor protection system does not trip the reactor on low feedwater flow |
| Extended plant shutdown | Inadvertent actuation of a safety system | Digital high-pressure coolant injection system initiation with no loss of coolant |
| Equipment damage | Failure of equipment protection to actuate when needed | Digital turbine control system does not trip on overspeed when mechanical overspeed is disabled |
| Reactor trip | Inappropriate operator action | Failure of operator to recognize incorrect process parameters displayed on the main control board |

Hazard and operability (HAZOP) studies have been used as risk management techniques in process industries since the 1960s to systematically identify potential hazards. In a HAZOP study, a multidisciplinary team carries out a structured analysis of a system, process, or operation by using a set of guidewords in combination with process parameters (e.g., pressure, flow, temperature) to identify deviations from the intended design that could lead to potential hazards [15]. A standard set of guidewords and their generic meanings are listed in Table II. As part of a HAZOP study, a team identifies a parameter and guideword combination (e.g., more flow), brainstorms potential causes for the deviation (e.g., valve opens), and then evaluates the potential consequence of the deviation.

**Table II. Standard set of HAZOP guidewords taken from [15].**

| Guideword | Meaning |
|---|---|
| No (not, none) | None of the design intent is achieved |
| More (more of, higher) | Quantitative increase in a parameter |
| Less (less of, lower) | Quantitative decrease in a parameter |
| As well as (more than) | An additional activity occurs |
| Part of | Only part of the activity occurs |
| Reverse | Logical opposite of the design intention occurs |
| Other than (other) | Complete substitution—another activity takes place OR an unusual activity occurs or uncommon condition exists |

While HAZOP studies are typically performed on well-defined processes or operations [15], a HAZOP was performed on the conceptual process flow diagrams for the interconnected LWR and H2 plant as part of high-level design activities. A team of individuals representing engineering, risk, and cybersecurity disciplines spent one week systematically reviewing the design to identify unanticipated process deviations (e.g., more flow, less flow, higher temperature, lower temperature in any given segment), potential causes of these deviations from control system signals (e.g., valve open or closed more than expected), and potential consequences as a result of the process anomaly.

The focus for the HAZOP was to identify the consequences of cyber incidents on the new I&C components. Cyber incidents considered included deliberate and inadvertent actions that could disrupt data or information flow within a control system leading to degradation, mal-operation, or failure of a digital device and/or system functions. Also considered were incidents that could result in an 'unknown' state—a potentially dangerous state for an LWR.

Cyber incidents were not considered in the I&C system design prior to this study. As illustrated in Figure 4, the preliminary process flow diagram did not include instrumentation or valves. Thus, as the start of the HAZOP study, the conceptual design was expanded by the team to add these process control elements. Figure 5 illustrates the final process flow and I&C diagrams that were developed and evaluated during the study. VLV-104 is the existing LWR turbine control valve (TCV); VLV-103 is a new IPF bypass valve that controls diverted steam flow to the IPF; and VLV-105 is a new IPF loop valve that controls flow through the IPF. The dashed red lines on the diagram identify the sensors used for valve control. Further modifications were added to improve overall thermal efficiencies, including the addition of a heat exchanger on the IPF and a split of the condensate return to provide preheat to a feedwater heater.

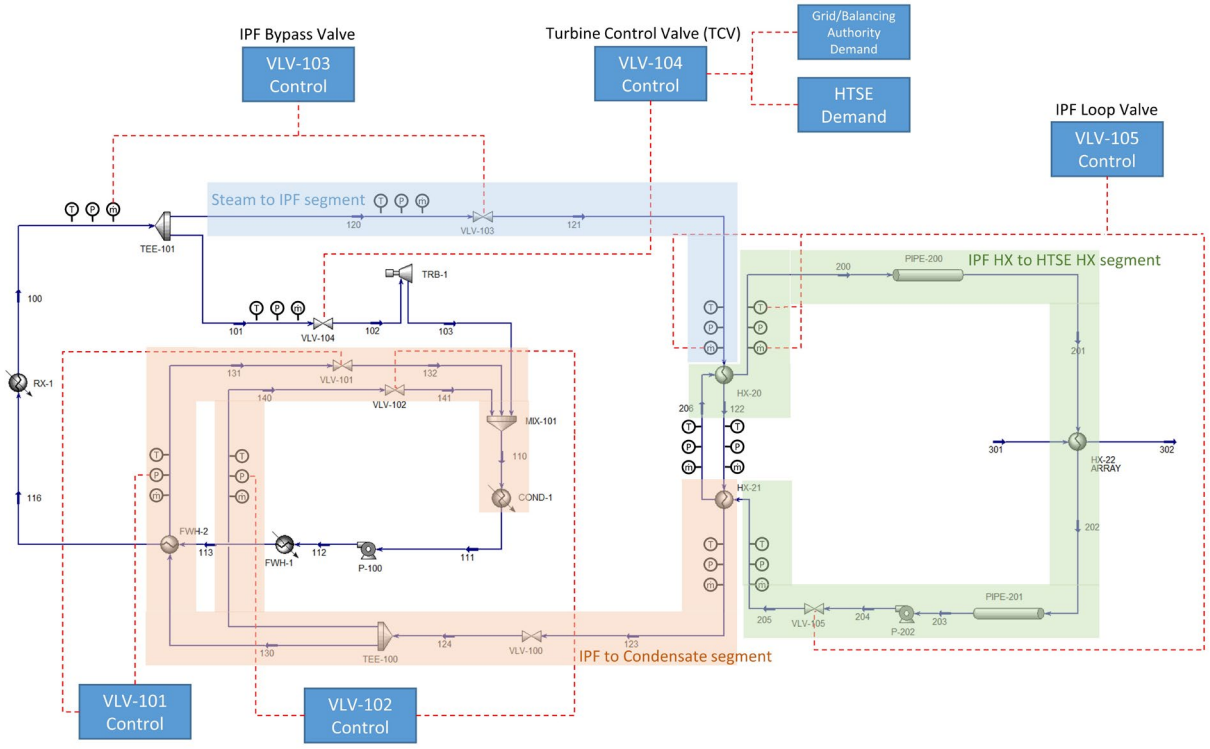


**Figure 5. Process flow diagram and I&C design of the integrated H2/LWR systems after the HAZOP study.**

The team evaluated three flow segments in the HAZOP: (1) steam to IPF (blue), (2) IPF to HTSE steam generator (green), and (3) IPF to condensate (orange). Assuming an LWR is controlled to maintain constant average reactor coolant temperature (Tave), several potential hazards to an LWR were identified that could result from a deliberate or inadvertent cyber incident. For instance, in segment 1, a deviation of 'more flow' on the steam line from the LWR to the IPF could be caused from (a) closure of the turbine control valve potentially resulting in an LWR trip due to steam generator overpressure or (b) by opening of the IPF bypass valve (VLV-103) potentially resulting in an unplanned reactivity change. The potential for the first postulated event exists in a current LWR while the second event is a new potential hazard resulting from the H2/LWR integration. Similarly, a deviation of 'more flow' on the condensate return line from the IPF in segment 3 could be caused by opening of the IPF valve, potentially resulting in decrease of the LWR steam generator pressure and unplanned reactivity change. Risk treatments were then considered for the complete listing of identified deviations and hazards from the HAZOP risk analysis study.

### 3.2.2 Engineering risk treatment

After completing a cyber risk analysis, risks are evaluated and prioritized based upon risk tolerance. Once prioritized, engineering risk treatments are determined. As shown in Figure 6, risk treatments include (a) elimination or avoidance—design out the risk; (b) transference—shift or move the risk, potentially to other organizations; (c) mitigation—reduce risk by use of security controls, such as administrative, physical, or technical controls identified by NIST SP 800-82 [3], Regulatory Guide (RG) 5.71 [4], or NEI 08-09 [5]; or (d) acceptance—a conscious decision to tolerate the risk without change.

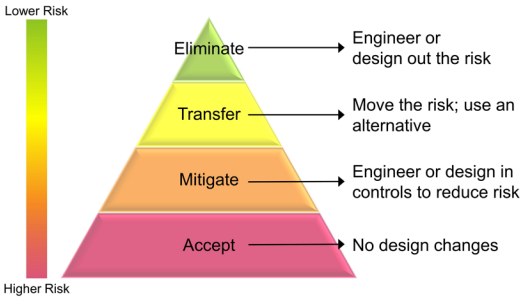


**Figure 6. Engineering risk treatment options.**

While it is unconventional to perform a HAZOP study on a preliminary design, the discussion between the multidisciplinary team members on potential cyber incidents and unsafe control actions, vulnerabilities, and consequences resulted in elimination of some of the identified risk through a redesign of the integrated system. The team also discussed designing and segmenting the system architecture to minimize the use of critical digital assets to reduce the cyber risk.

### 3.2.3 Design simplification

The goal of design simplification is to reduce the complexity of the system, component, and/or architecture while maintaining the intended function. Design simplification is considered in conjunction with the secure architecture, resilient design, and engineering risk treatment elements. Complex and/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. Simplifying the design, such as by using simpler digital devices and limiting or disabling unnecessary functions, 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.

As a result of this study, the process flow loops were modified and a simpler I&C design using pressure, temperature, and mass flow sensors to control valve positions was established as shown in Figure 5. This reduced digital footprint and smaller attack surface directly reduces the overall cyber risk.

### 3.2.4 Resilient design

Resilient design may be accomplished, in part, by the inclusion of diversity, redundancy, system hardening, and contingency planning into the design with the objective of ensuring continued operation of critical functions when possible, or graceful degradation when not possible, in the event of a 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.

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, then it is still a simplified design. Similar to the general design criteria for safety-related systems at an LWR, resiliency often involves separation, redundancy, and diversity. Separation is achieved by physical separation (e.g., distance, barriers) and electrical isolation; redundancy is achieved by using more than one component to perform the same function; and diversity is achieved by using different technology in the redundant components (e.g., different vendors, platforms, operating systems). Cyber resiliency also includes system hardening (i.e., elimination or prevention of unused functions or capabilities), contingency planning, and maintaining situational awareness via techniques such as network or system monitoring.

A resilience-based design recommendation from the study was to decouple and separate the LWR and H2 control functions to ensure heat demand from the H2 plant cannot change steam flow demand in the

'steam to IPF' segment. The team determined that decoupling and maintaining a hard separation of these control functions, including separation of data connectivity, lowers the risk of 'more flow/less flow' deviations in the segment, lowers the overall cyber risk of the H2/LWR integration, and reduces requirements associated with cybersecurity mitigations.

### 3.2.5 Interdependencies

The CIE organizational elements listed in Figure 3 are those fundamental cybersecurity practices that enable holistic integration of cybersecurity into other programs within the facility. The interdependencies element ensures that cybersecurity is considered within all the interconnections between systems and systems of systems. Interdependency also promotes a multidisciplinary approach to ensure that all stakeholders involved with digital systems, including disciplines such as engineering, safety, risk, design, maintenance, operations, human factors, and ICT, provide input and are knowledgeable about these system interdependencies and the potential consequences of a cyber incident on a digital asset, system, or system of systems.

Team members with engineering, risk, cybersecurity, and operations backgrounds participated in the week-long exercise. As a direct result of discussions surrounding the initial design and potential consequences from inadvertent or malicious cyber incidents, the design was modified to improve process flow and limit impacts. An important take-away from this study was to include cybersecurity regulatory considerations when designing new systems architecture to understand and/or minimize any potential compliance constraints. Upon conclusion of the exercise, participants indicated that the interaction among the diverse team resulted in enhanced cybersecurity knowledge and an improved, more secure design. Comments included:

> *"By including expertise from different fields, all "stakeholders" joined the development process to ensure the final results met all the needs (e.g., cyber security, efficiency) and are usable. This roundtable discussion accelerates the development process by efficiently eliminating misunderstanding from different backgrounds and raising up all needs from the beginning."*

> *"I came away from the experience with a great deal of new perspective. It was valuable for me to think through the potential vulnerabilities of nuclear hybrid energy systems, and the potential failure modes of these types of systems (both due to external attack as well as due to internal failure modes). …my increased awareness of these and other topics covered during the HAZOP exercise will undoubtedly help me to consider such factors in the future, and to the extent possible/practical for whatever related project(s) I may happen to be working on in the future, to try and incorporate design features that will help to address these issues. Interfacing with the multidisciplinary team was certainly a key part of being able to gain this additional perspective."*

## 4 CIE RECOMMENDATIONS FOR FUTURE H2/LWR PROJECT STAGES

**Cyber Risk Analysis and Engineering Risk Treatment.** As with any effective risk management program, cyber risk analysis should be continually repeated throughout the system engineering lifecycle. Threats, vulnerabilities, and consequences may change, resulting in changes to the cyber risk profile. Similarly, as the design matures, the team should continue to evaluate and prioritize engineering risk treatments based upon the cyber risk, including the use of security controls for cyber-attack prevention, detection, and response in accordance with best practices and regulatory guidance. A U.S. nuclear power plant will likely have a security control implementation strategy based on RG 5.71 [4] and/or NEI 08-09 rev 6 [5]. The team should perform a cyber assessment on the design early and often to identify critical digital assets. Regardless of the assessment outcome, however, security controls should be implemented as best practice to mitigate any identified cyber risks.

**Secure Architecture.** Secure architecture is the establishment of network and system architectures that segregate and limit data flows to trusted devices and connections within and between subsystems, systems, and systems of systems. The goal of secure architecture is to prevent unauthorized access or compromise of critical systems and digital assets. While not specifically addressed as part of this study, the

I&C system network and systems architecture is an important consideration during early system engineering stages to minimize the attack surface and reduce cyber risk. In addition to designing the new architecture for the H2 facility, the design team must also evaluate the existing nuclear power plant architecture and Cyber Security Plan (CSP) requirements when designing the integrated system. The communication and data flows must be segregated and limited to reduce impacts on either plant from a cyber incident. To ensure defense in depth, the design should consider use of isolated or segregated network levels and zones; boundary devices, data flow rules, and/or unidirectional, deterministic communication; and redundant sensors and/or instrumentation loops separate from the existing LWR or H2 facility instrumentation. Use of wireless networks or remote connections will require review to determine if they are allowed under the CSP, regulations, and guidance.

**Design Simplification.** As the H2 plant and the I&C design move further down the system engineering lifecycle, future cyber risk analyses may require additional design simplification. For instance, depending on the risk analysis and criticality designation of system function, the design team may consider reducing the attack surface by using analog instead of digital devices or using field-programmable gate arrays (FPGAs) instead of programmable logic controllers (PLCs). Unnecessary components, sub-components, functions, services, and software should be removed or disabled. Use of system interfaces, such as engineering workstations, human-machine interfaces, and maintenance connections should be limited to the lowest number required to achieve system functionality. Similarly, network architecture should be designed to use as few devices and shortest runs as possible.

**Resilient Design.** Currently, the proposed I&C system does not utilize redundant instrumentation or components. However, as the project progresses to the detailed low-level design phase, the design team should evaluate resiliency requirements to determine if any changes are required to assure continued operation of the LWR and integrated H2 plant. For instance, the team may determine that new process instrumentation and/or new or separated, redundant instrumentation loops will establish higher resiliency and less impact to the LWR than using the established LWR instrumentation. Any tradeoffs between safety, security, and resiliency should be evaluated and documented.

**Active Defense.** Instead of reliance on passive capabilities, active defense is the use of preemptive processes and techniques to prevent, detect, and respond to cyber incidents. While this study did not specifically evaluate active defenses for the integrated plants, active defenses, including security information event monitoring (SIEM) and other real-time tools, should be incorporated into the system and organization to quickly adapt and respond to emerging threats. In addition to maintaining a proactive security posture, active defenses enhance resilience capabilities by improving operational situational awareness.

**Interdependencies.** Further multidisciplinary engagements should continue throughout the systems engineering lifecycle to enhance overall knowledge and communication regarding how cybersecurity impacts each system function, discipline, and overall design. The nature of the engagements will differ with each lifecycle phase; similar to safety, the intent is to ensure cybersecurity remains a core domain throughout the process.

**Digital Asset Inventory.** The digital asset inventory element is intended to ensure an accurate as-built digital asset inventory is maintained throughout the engineering lifecycle, including initial design, maintenance, configuration changes, and upgrades or modifications. It is impossible to provide adequate protection against cyber incidents for unknown digital assets. Typically, the inventory cannot be established until the low-level design stage. Upon development of the low-level design, the team should establish a detailed list of the digital bill-of-materials (DBOM), including hardware, firmware, and software. In addition to the DBOM, configuration information, backup requirements, and restoration information should be maintained for each digital asset or system. Since cyber compromises do occur during the supply chain and system engineering activities, 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 element, this detailed information can be used to restore or rebuild a system after a cyber incident.

**Cyber Resilient Supply Chain.** The cyber resilient supply chain element includes the incorporation of techniques into the procurement and acquisition process to prevent malicious or inadvertent compromise of hardware, firmware, software, and system information. Primary objectives of cyber supply chain risk management include the ability to maintain authenticity, integrity, confidentiality, and exclusivity throughout the system engineering lifecycle. 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 [16]. Although the cyber supply chain was not considered during this activity, it is important to recognize that supply chain cybersecurity is necessary even during the early lifecycle stages. Theft of confidential or proprietary system information may result in loss of intellectual property, counterfeiting, and/or enable development of future sophisticated cyber-attacks. In addition, compromise of system information could lead to developers inadvertently including malicious codes, falsified data, latent vulnerabilities, or backdoors into the system or component. In addition, the parallel use of the design simplification element reduces the supply chain cyber-attack surface by reducing the number of stakeholders and touchpoints involved in the supply chain [17]. Logically, ensuring cyber supply chain provenance and trustworthiness is easier with a smaller supply chain cyber-attack surface.

**Incident Response Planning.** Incident response planning, in conjunction with contingency planning in the resilient design element and digital asset inventory organizational element, ensures that procedures, current backups, and accurate configurations are available to respond to and recover from deliberate or inadvertent cyber incidents. While incident response planning was not considered as part of this activity, it should occur early and often within a project to safeguard the organization, design, and product against a cyber incident. Cyber incidents can occur at any stage in the system engineering lifecycle, ranging from theft of system information or IP in the design stages, to introduction of malware by a subcontractor during the test stages, to download of corrupted firmware in the maintenance stage. Developing and adapting an incident response plan at each stage of the lifecycle is key to responding to and recovering from an incident.

**Cybersecurity Culture and Training.** Nuclear plants are guided by a nuclear safety and security culture which emphasizes the protection of the health and safety of the public over other competing goals, such as electricity generation. 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, similar to the nuclear safety culture, will equip all personnel with the knowledge, skills, and abilities to recognize, prevent, and/or respond to cyber incidents. The human-in-the-loop is essential for maintaining a robust security posture. While this activity did not directly address cybersecurity culture or cybersecurity training, it brought together individuals from different backgrounds and disciplines. Discussions regarding system design, plant interactions, and cyber-related concerns provided new awareness to team members regarding potential cyber-consequences and how changes in the design can heighten or lessen them. Developing cross-functional cyber-capabilities indirectly enhances the cybersecurity culture of both the project team and the greater organization by improving general awareness and appreciation of the problem space.

## 5 CONCLUSIONS

Integrating cybersecurity in the systems engineering lifecycle is necessary to ensure a digital system is developed, tested, installed, and operated with cybersecurity built into the process instead of bolting it on at the end. Considering cybersecurity early in the design lifecycle results in more effective and less expensive cyber security measures. This study used CIE during an early stage in a project lifecycle. Cyber risk analysis of the initial process flow diagram using a HAZOP study identified potential consequences of a cyber incident; this analysis directly led to design modifications and simplification. The multidisciplinary approach provided an opportunity for each participant to learn and understand more about the

interconnections between engineering, safety, risk, and cybersecurity. This provided awareness about the importance of incorporating cybersecurity into a design and indirectly enhanced the organization's cybersecurity culture. As the H2 generation project continues, continued use of CIE elements will directly enhance the cyber security posture of the final integrated system.

## 6 ACKNOWLEDGMENTS

This research was supported by the U.S. Department of Energy Office of Nuclear Energy LWRS and Cybersecurity programs under the DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

## 7 REFERENCES

1. S. Bragg-Sitton, "Hybrid energy systems (HESs) using small modular reactors (SMRs)," Idaho National Laboratory (2014).
2. "SP 800-53 Revision 5. Security and privacy controls for information systems and organizations," National Institute of Standards and Technology (2017).
3. K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "SP 800-82. Revision 2. Guide to industrial control systems (ICS) security," National Institute of Standards and Technology (2015).
4. "Regulatory Guide 5.71, Cyber security programs for nuclear facilities," U.S. Nuclear Regulatory Commission.
5. "NEI 08-09, Cyber security plan for nuclear power reactors, Revision 6," Nuclear Energy Institute.
6. "NEI 13-10 Cyber security control assessments, Revision 5," Nuclear Energy Institute.
7. "NST045, Computer security for nuclear security, Draft implementing guide, Step 12," International Atomic Energy Agency, Vienna (2018).
8. "Nuclear Security Series No. 17, Computer Security at Nuclear Facilities," International Atomic Energy Agency, Vienna (2011).
9. "NST047, Computer security techniques, Draft implementing guide, Step 12," International Atomic Energy Agency, Vienna (2018).
10. "IEC 63096:2020, Nuclear power plants - Instrumentation, control and electric power systems - Cybersecurity requirements," International Electrotechnical Commission.
11. "IEC 62645:2019, Nuclear power plants - Instrumentation, control and electric power systems - Cybersecurity requirements," International Electrotechnical Commission.
12. R.S. Anderson, J. Benjamin, V.L. Wright, L. Quinones, and J. Paz, "Cyber-Informed Engineering," Idaho National Laboratory (2017).
13. "Systems engineering for Intelligent Transportation Systems: An introduction for transportation professionals," U.S. Department of Transportation (2007).
14. K. Frick *et al.*, "Evaluation of hydrogen production feasibility for a light water reactor in the midwest," Idaho National Laboratory.
15. F. Crawley and B. Tyler, *HAZOP: Guide to Best Practice (Third Edition)*. Elsevier (2015).
16. M. Windelberg, "Objectives for managing cyber supply chain risk," *International Journal of Critical Infrastructure Protection,* **12,** pp. 4-11 (2016).
17. S. Eggers, "A novel approach for analyzing the nuclear supply chain cyber-attack surface," *Nuclear Engineering and Technology,* **53,** no. 3, pp. 879-887.