Advanced Reactor Safeguards & Security

Cybersecurity Scenarios

‘

Prepared for
US Department of Energy

Dr. William Hutton, CISSP
Fleur De Peralta, PE

Pacific Northwest National Laboratory

October 2025
PNNL-38627

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

Abstract

The use of digital control systems and automation in advanced nuclear power systems introduces different types of vulnerabilities compared to legacy (i.e. analog) control systems that cyber adversaries can exploit. These vulnerabilities pose a challenge to reactor operators and cyber operations staff due to the dynamic nature of the event in which a human response or a lack of response can potentially evolve into a worsening plant condition. Using the Department of Homeland Security Cyber and Infrastructure Security Agency's (CISA) critical infrastructure exercise framework, this document presents several cyber security scenarios typical of digital control systems that could be used in advanced reactor designs. These scenarios can be used in tabletop exercises to evaluate cyber security posture or conduct training on different aspects of cyber security, including detection, threat hunting using indicators of compromise, evaluating incident response, risk mitigation, incident reporting, information sharing and recovery.

Acknowledgements

The authors would like to extend gratitude and thanks to the Advanced Reactor Safeguards and Security (ARSS) Program and Department of Energy, Office of Nuclear Energy for funding this research. We especially would like to thank Ben Cipiti (National Technical Director) and Dan Warner (DOE Program Manager), for technical support and guidance throughout the project.

PNNL would also like to acknowledge Charles Bowler (Retired Nuclear Operator at Diablo Canyon Power Plant) for providing insights on digital control system design and nuclear power plant operations,

We would also like to extend our gratitude to PNNL colleagues Garill Coles (Nuclear Safety and Probabilistic Risk Assessment Analyst), Guy Landine (Cyber Security Researcher), and Grace McNally (Cyber Security Engineer) for performing the peer reviews of this report.

Finally, we would like to thank Paragon for their excellent training course on digital licensing of advanced reactors, including Ted Quinn (Vice President), Tighe Smith (Chief Nuclear Officer), Clark Artaud (Nuclear I&C Consultant), Chad Michaelis, Brian Haynes, Chris Harrington, Trevor Taylor, Richard Knott and Hope Levanites. The Paragon training provided an excellent opportunity for our cyber security SMEs to cross-train in nuclear issues.

Acronyms and Abbreviations

ACE	Arbitrary Code Execution
AOP	Abnormal Operating Procedure
ASIC	Application Specific Integrated Circuit
C^2	Command & Control
CCF	Common Cause Failure
CIM	Component Interface Module
CISA	Cybersecurity & Infrastructure Security Agency
CPG	Cybersecurity Performance Goals
CPU	Central Processing Unit
CTEP	CISA Tabletop Exercise Package
D^3	Diversity and Defense-in-Depth
DAS	Diverse Actuation Scheme
DDS	Data Display and Processing System
EOP	Emergency Operating Procedure
FPGA	Field-Programmable Gate Array
HBOM	Hardware Bill of Materials
I&C	Instrumentation & Control
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
LCO	Limited Condition of Operation
LDAP	Lightweight Directory Access Protocol
MitM	Man-in-the-Middle (cyber-attack)
NCEP	National Cyber Exercise Program
NIST	National Institute of Standards & Technology
OCC	Operation and Control Center
OSINT	Open-Source Intelligence
PCS	Plant Control System
PLC	Programmable Logic Controller
PMS	Plant Monitoring System
RCE	Remote Code Execution
SBOM	Software Bill of Materials
SMS	Special Monitoring System
TCP	Transmission Control Protocol
TOS	Main Turbine Control and Diagnostic System
TTP	Tactics, Techniques, and Procedures
V&V	Verification & Validation

Table of Contents

Summary

The use of digital control systems and automation in advanced nuclear power systems introduces different types of vulnerabilities compared to legacy (i.e. analog) control systems typically used in the current fleet of nuclear power plants in the United States. Vulnerabilities inherent in people, processes and advanced technology are constantly exploited by cyber adversaries. These vulnerabilities pose a challenge to reactor operators and cyber operations staff due to the dynamic nature of the event in which a human response or a lack of response can potentially evolve into a worsening plant condition.

Three cybersecurity scenarios were developed using Lockheed Martin Kill Chain methodology and the Department of Homeland Security Cyber and Infrastructure Security Agency's (CISA) critical infrastructure exercise framework. The Cyber Kill Chain framework is abstract enough to avoid specific safeguards and security information while remaining specific enough to be actionable in helping exercise participants to understand how a cyber security incident could impact their policies, procedures, and controls in an advanced reactor setting.

This document presents three cyber security scenarios typical of digital control systems that could be used in advanced reactor designs. The scenarios are designed to be used individually to highlight a specific step in the Cyber Kill Chain or used together to demonstrate the entire Cyber Kill Chain.

1. Open-Source Intelligence (OSINT) Awareness
2. Vulnerability Introduced by Diversity and Defense-In-Depth (D^3)
3. Loss of View for Plant Monitoring System (PMS)

Additionally, four other scenario seeds are introduced in this report to call attention to other cybersecurity risks to advanced reactors. These partial scenarios could be building blocks for tabletop exercises, implemented as a hands-on red-team / blue-team activity, or included in training discussion.

4. Lagging Regulations, Guidance, and Standards
5. Deep Dive into Vulnerabilities Introduced by Diversity and Defense-In-Depth (D^3)
6. Loss of Control for Diverse Action Scheme (DAS)
7. Supply Chain Risks to Field-Programmable Gate Arrays (FPGAs)

Each scenario can be used to evaluate cybersecurity posture, conduct training (e.g., detection, threat hunting using indicators of compromise, evaluating incident response, risk mitigation, incident reporting, information sharing, response and recovery, etc.).

Introduction

Advanced reactor designs incorporate the use of highly integrated digital instrumentation and control (I&C) systems to enhance plant safety, increase reliability, and improve overall plant efficiency. Adversaries may be able to exploit vulnerabilities in digital I&C systems, which could potentially result in common cause failures affecting nuclear systems. It is important to recognize that nuclear systems are categorized as safety and non-safety related systems. Nuclear safety related systems are traditionally deployed "air gapped" (i.e. disconnected from the Internet) and heavily protected by physical security controls. We may not make these same assumptions for advanced modular reactors.

Using a commonly known cyber scenario framework, scenarios were developed targeting such systems. These cyber scenarios could be used in red-teaming events to proactively identify and mitigate potential weaknesses in cyber security defenses, such as preparedness and incident response strategies. The cyber scenarios developed in this report are intended to simulate real-world cyberattacks. However, responses from cyber operations staff and plant operations staff may be different than those postulated in the scenario. This document is intended to be used by the ARSS Program for red-teaming purposes and training activities to assess a licensee's cyber security posture. Scenarios are developed based on insights obtained through review of typical digital I&C control systems used in nuclear power plants, interviews with nuclear plant operators, and current regulatory guidance for cyber security of advanced reactors. The cyber scenarios developed are not a reflection on a specific advanced reactor design.

Background on Digital I&C (Instrumentation & Control) Systems

Commercial nuclear power plants and advanced reactors have begun to integrate programmable digital devices into plant systems to improve performance and reliability. Networking digital systems can implement automation and improve human-machine interaction. Logic functions of programmable digital devices may be implemented in hardware, firmware, or software. Programmable digital devices range in flexibility from general-purpose central processing units (CPUs), followed by programmable logic controllers (PLCs), application-specific integrated circuits (ASICs), and field-programmable gate arrays (FPGAs). In general, the more flexible a programmable digital device is, the harder it is to secure. For this reason, FPGAs are the standard for safety and safety-related systems. Changes to how FPGAs are programmed may require license modification with the NRC. Some vendors that use FPGAs stipulate that only they can modify FPGA programming.

Unfortunately, the inherent interconnectivity of digital devices can also result in a single failure that could affect multiple control functions and result in a common cause failure. For example, a single failure within the software or hardware of a controller may result in erroneous processing that impacts upon multiple control functions integrated within the same controller. Another example could be single failure of a digital data communications interface that can impact communication between multiple control functions.

Nuclear regulatory guidance has been issued for plant operators to assess the implications on the safety system architecture, failure modes and effects analysis and the application of defense-in-depth principles. [3]

Advanced reactors, such as the Westinghouse AP1000TM, integrate data communications between the functional I&C systems and system components, such as pumps, valves, breakers, electrical contacts.

The I&C systems interface with safety system components using a Component Interface Module (CIM). From a high-level perspective, the architecture of the AP1000 can be divided into the following functional systems: [4]

- Safety Systems, such as the Protection and Safety Monitoring System (PMS)
- Non-Safety Systems, such as Plant Control Systems (PCS), Data Display and Processing System (DDS), Main Turbine Control and Diagnostic System (TOS) and Special Monitoring Systems (S)
- Other systems, such as the Diverse Actuation Systems (DAS), In-core Instrumentation System (IIS) and Operation and Control Centers (OCC) Systems.

The major non-safety systems (e.g., DDS, PLS, TOS, SMS) and the non-safety portions of both the IIS and OCS are integrated using a plant-wide real-time data distribution network. That network is implemented using the Emerson Ovation® network. Data transferred from both safety and non-safety portions of the I&C systems are transferred using unidirectional gateways, one for each of the PMS divisions. [4]

The NRC mandates single-failure analysis in the design phase. It is unlikely that any single failures would be a random, unknown and previously unanalyzed incident—but the probability of such a failure is not zero. Failures may also be caused by an adversary, especially via a supply chain attack. The consequence of impacting multiple control functions could result in placing the plant in an unanalyzed condition. Cyber security measures are implemented to monitor the network of systems, identify anomalies in these control systems, and respond to the anomalies. The scenarios developed in this report are generally based on digital I&C systems of advanced reactors, such as Westinghouse AP1000 design.

Attack Methods

The **Cyber Kill Chain™** framework developed by Lockheed Martin [1] identifies the stages of an attack and gives defenders insight into an adversary's typical tactics and techniques during each stage. The Cyber Kill Chain offers the appropriate level of detail in developing a cyber scenario for advanced reactors. The framework is abstract enough to avoid specific safeguards and security information while remaining specific enough to be actionable in helping exercise participants to understand how a cyber security incident could impact their policies, procedures, and controls in an advanced reactor setting. As illustrated in Figure 1, there are seven stages of the Cyber Kill Chain, which are discussed below:

1. Reconnaissance: Intruder selects a target, researches it, and attempts to identify vulnerabilities in the target network
2. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3. Delivery: Intruder transmits the weapon to the target
4. Exploitation: Malware weapon's program code triggers, which acts on target network to exploit vulnerability
5. Installation: Malware weapon installs an access point (e.g., "backdoor") usable by the intruder

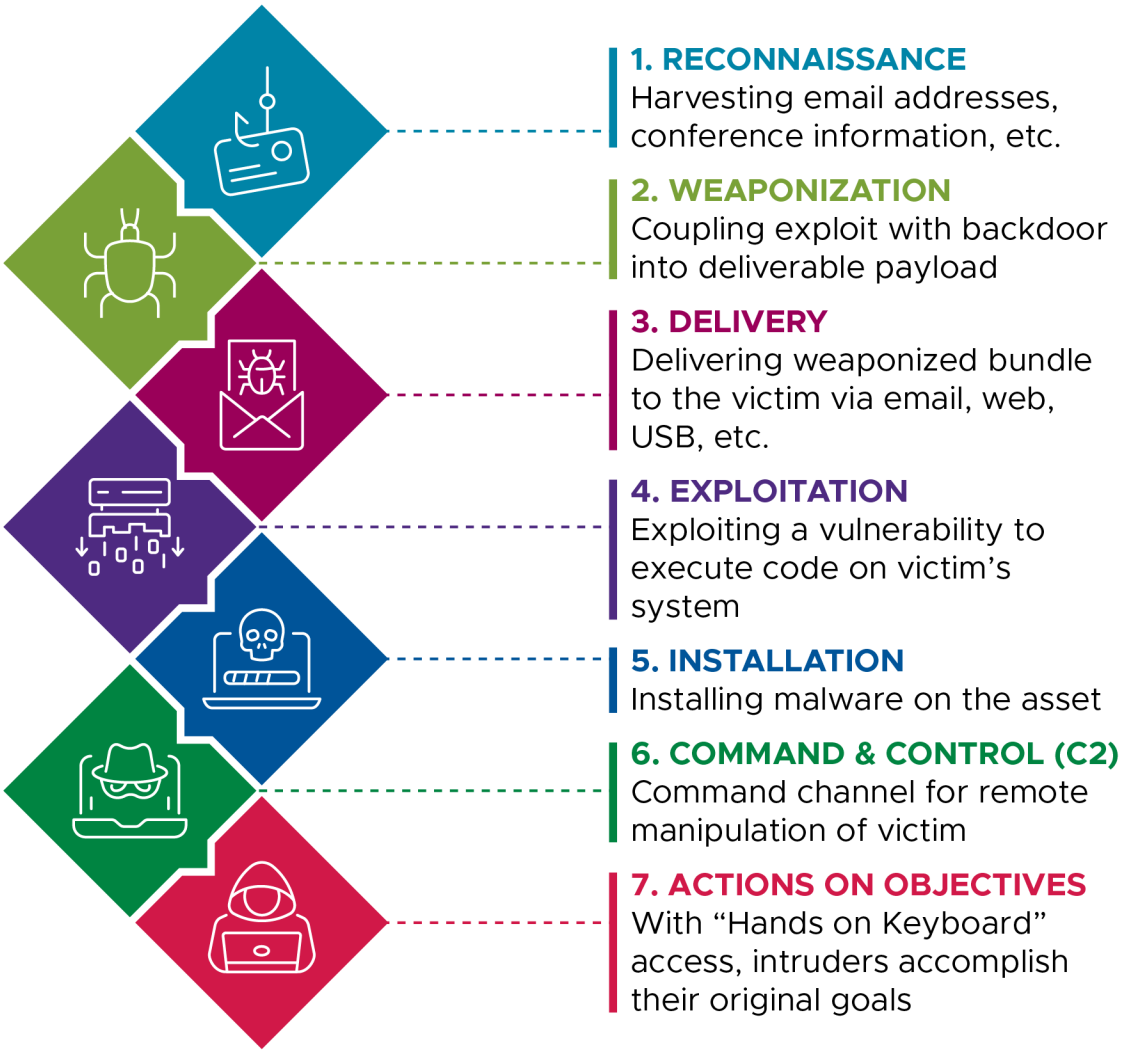

Figure 1. The Cyber Kill Chain

6. Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to the target network.

7. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction or encryption for ransom.

Target Selection

There are a variety of targets to focus on in an advanced reactor setting. For example, digital I&C systems can be non-safety or safety related systems and consequences vary on impact to nuclear safety. Additional factors that played a role in target selection include the exercise participant audience, the learning objective for that audience, technical feasibility, and demonstrated impact, both of which impact realism. It is important that exercise participants see their own systems in the cyber security scenario and that specific steps in the Cyber Kill Chain are believable.

Safety and Safety Related Systems

For the current fleet of nuclear power plants, safety and safety related systems are not typically connected to the Internet. However, for advanced reactor designs it is expected that digital systems would be used due to its ability to automate system operation by quickly responding to plant operational perturbations (inadvertent or advertent).

Most digital systems applied in nuclear power plants would involve reactor protection systems (RPS), engineered safeguards actuation systems (ESFAS), or plant protection systems (PPS). The NRC has approved the use of digital systems that have been used in other process industries, such as Invensys Triconex Tricon, Framatome ANP Teleperm XS, Westinghouse Common Qualified Platform, or Siemens TXS, for use in RPS and ESFAS systems [8]. The network architecture for these platforms may include software and modules from commercially available process logic controllers to perform various safety functions for the RPS, ESFAS and PPS or load shed/sequencing actions. These systems involve field sensors and actuators connected to data acquisition and management, monitoring and service interfaces. Safety and safety related systems typically use field-programmable gate arrays (FPGA) instead of microcontrollers and tend to be focused on hardware instead of software.

In some cases, new digital upgrades may be installed in existing cabinets, using existing terminal blocks and field wiring to centrally located systems. Actuators circuits could be maintained and Local I/O actuator circuits. Potential interfaces include the use of ESFAS slave relays (in many US plants) or standard digital interface, such as those found in European designs. [8]. In typical Westinghouse NSSS designs, the use of two redundant trains of coincident logic processing and four redundant sets of signal processing systems safeguard these systems from inadvertent actuations and operations in the event of a single failure. Priority modules or relay-based interlocks are also used to ensure safety-system commands override non-safety commands.

Protection of safety-related systems and systems important-to-safety from cyber incidents most likely will follow Regulatory Guide 5.71, “Cybersecurity Programs for Nuclear Power Reactors” [5] or Nuclear Energy Institute (NEI) guidance NEI 08-09, “Cyber Security Plan for Nuclear Power Plants” [6]. Specific cyber security regulations for advanced reactors is not yet been issued. Safety and safety related systems are protected by data diodes (e.g. cross-domain solutions) that limit the flow of information to prevent “writing up” from a system with less integrity, but do allow “writing down”, for example, to transfer telemetry to a historian. The probability of a cyber-attack on a safety or safety related system is low, but the impact of a successful cyber-attack would be very high. Insider threats and supply chain risks are the largest threats to safety and safety related systems.

Non-Safety Related Systems

Nuclear non-safety related (NSR) systems are generally functions that support balance of plant systems (i.e., Main Feedwater Systems, Turbine generation, condenser, etc.) and diagnostic instruments for monitoring and control that do not directly prevent accidents. In Westinghouse AP1000 designs, support systems, such as the chemical and volume control systems, the Plant Control system (PLS) and the Diverse Actuation System (DAS), are considered a non-safety system that supports a safety function. Digital technology would be implemented into these types of non-safety systems. Thus, this could involve widespread use of microcontrollers for programmable digital devices, which are easier to target but would have less of an impact. Multiple layers of defense-in-depth are integrated into the safety

design of advanced reactors, which include digital systems as the “first line of defense” (NSR systems) and passive systems, which rely on no air, no power and/or gravity to fail the equipment in the safe shutdown position (safety-related systems).

Adversary Model

Design basis threat (DBT) is a common adversarial model used in the nuclear industry. The details of site-specific DBTs are protected as Safeguards & Security information, but we can discuss the basic concept of DBT here and how DBT informs our adversary model for cybersecurity scenarios to be used in advanced reactors.

In a nutshell, DBT defines the specific threats a site is designed to repel. Any threat less than or equal to the DBT is mitigated by the site. Any threat larger than the DBT is the responsibility of the government. The adversary model used in developing the cybersecurity scenarios in this report focus on a remote adversaries and supply chain threats. The probability of adversary success is 1.0, meaning the adversary can execute an effective cyberattack at the time and place of their choice.

The likelihood of a remote attack is higher, but with a lower expected impact. The lower impact is attributed to a rigorous design licensing process and reduced attack surface of safety and safety-related systems. Typically, we expect the “worst case” scenario to be the safe shutdown of the nuclear reaction, resulting in a loss of availability of power. A local attack (e.g., insider threat, blended physical-cyber-attack, etc.) has a very low probability of occurring. Depending on the attacker goal and the site’s DBT, the impact could range from very low to very high.

Threats to the supply-chain of more deterministic hardware-based computational devices like FPGAs should also be considered. The resource sophistication required to execute a supply-chain cyberattack on advanced reactors would likely require nation-state sponsorship.

Full Cybersecurity Scenarios

This section presents three cyber security scenarios which may be used alone to focus on a specific portion of the Cyber Kill Chain, including adversary activities and defender responses. Scenarios are also designed to be combined to exercise the entire Kill Chain. In developing the full scenarios, certain considerations are described, such as policies and actions that may be exercised at the tabletop level. Each module also includes a timeline of adversary activities as well as test evaluation packages (TEPs), which may be “white carded” (i.e. simply explained) or implemented in a lab environment to provide hands-on experience for exercise players.

Module 1—OSINT Awareness

Virtually all cyber-attacks begin with reconnaissance (see Figure 1 above). Open-Source Intelligence (OSINT) activities use publicly available information to build knowledge about a target utility or licensee that can be useful in a successful cyber-attack. For example, a company web site may list members of a board of directors. Using this information, an adversary may scour social media web sites like LinkedIn for relationships that can be used for additional reconnaissance activities. Mentioning personal relationships can make spear phishing campaigns more effective, which are often used in step three (i.e.

delivery of malware) of the Cyber Kill Chain. Combining awareness of an OSINT profile with the tools, tactics, and procedures (TTPs) of most likely threat actors can be a powerful mitigation tool.

Day 1

An unknown adversary at an unknown location makes a single HTTP Request to a utility's web server, requesting the 'board.html' file. The 'board.html' file contains the names and photographs of all seven members of a utility 's Board of Directors.

For Consideration

- Availability of forensic evidence (e.g., HTTP requests) will only be available to cyber defenders when the activity occurs within your electronic perimeter and is logged. Retention policies should be sufficient to ensure availability if some time passes between malicious activity and detection.

- Cyber defenders may brainstorm information that may be of use to an adversary in the reconnaissance phase of the Cyber Kill Chain and implement logging and alerting following industry regulation and industry best practice. Publicly available information that may be misused may include, but is not limited to:

    - Employee names

    - Employee contact information:

        - Telephone numbers

        - Email addresses

        - Senior management

- Files shared on web sites may contain metadata that may leak additional information, such as:

    - Do you have an asset inventory for published information?

    - Do you have a policy or procedure to remove metadata from published files?

- Cyber defenders may also brainstorm indicators of reconnaissance activity and develop alerts to decrease detection and improve response time to interrupt the Cyber Kill Chain as early as possible. Analysis techniques to determine if activity is normal, abnormal, or malicious should be documented and evaluated during exercises. Policies and procedures may be updated based on what works.

TEPs

TEPS may be high fidelity digital artifacts that may be replayed on a cyber range, distributed as forensic files for analyst review, or "white carded" examples for familiarity and education purposes. Below is a list of potential TEPs that may be implemented to reduce the risk with OSINT:

- Approximately 10 network packets from initial TCP 3-way handshake to HTTP Request, HTTP Response, and session tear down.
- Web server log entries for HTTP Request and HTTP Response
- Firewall log entries
- Intrusion detection / prevention system logs

Day 3

An unknown adversary uses the list of names learned on Day 1 to scour social media sites like Facebook and LinkedIn to build profiles of each board member.

For Consideration

- "Acceptable Use Policy" for social media use. Social media web sites should be reviewed frequently for information that may be used by an adversary in the reconnaissance phase of the Cyber Kill Chain.
- Perform annual OSINT reporting exercises to see what information about your organization, facility, or systems are available to adversaries.
- Cybersecurity awareness training that includes how to recognize and respond to adversary efforts to collect personal information on your employees, phishing awareness and social engineering awareness.

TEPs

Not all adversarial activity against an individual or utility will be visible if it occurs on external networks.

Day 11

An unknown adversary browses the Careers section of your public web site looking for vendor names, specific hardware and software and other information they can use to enumerate potential weaknesses that can be weaponized for a spear phishing campaign.

For Consideration

- Implementing a policy for categorizing and controlling information. Focus on information that may reveal specific details about the technology use within their organization.

- Regularly reviewing public information for content that may leak information about sensitive technology.
    - Remember, "The Internet is forever.". If you find and remove sensitive information, it may be archived elsewhere. Sites like http://archive.org maintain previous versions of public web sites.

TEPs

Remember, not all adversarial activity against an individual or utility will be visible to you if it occurs on networks outside your organization.

Day 45

All seven members of a utility's Board of Directors receive well-crafted spear phishing emails with an urgent call to action to click the URL in the email. In each case, the email appears to have been sent from someone known to the individual. There are no obvious spelling or grammar mistakes because the adversary used artificial intelligence (AI) to help write the email.

Some members of the board have clicked the URL. One board member reached out to their IT Help Desk *after* clicking the link.

For Consideration

- Implement forensic capabilities to assess the impact of a cyber event, including:
    - Identify who clicked the URL and when.
    - Where the URL is hosted.
    - What data may have been brought inside your electronic perimeter by clicking on the URL.
        - Identify if the retrieved data is malicious (i.e. malware).
        - Identify if the retrieved data has spread within your organization (i.e. a worm).
        - If a spear-phishing email was forwarded to anyone else within the organization (i.e. Which employees or digital assets were impacted).
    - Implement incident response guides to respond to spear phishing (and other) incidents.
- Implement policies or procedures to contain malware delivered via email (or other media).
- Implement policies or procedures to respond to and recover from malware delivery (or other) incidents.

- Implement policies or procedures for sharing information about a malware delivery (or other) incident to help protect similar organizations.

TEPs

The following are examples to perform if an individual inadvertently opens a phishing email or link:

- Sample spear-phishing emails, with different sender and malicious URLs.
- Review and monitor Network and email server logs
- Review and monitor Firewall logs
- Review and monitor Intrusion detection or prevention system logs detailing email activity and HTTP Requests and HTTP Responses

Module 2—Vulnerability Introduced by Diversity and Defense-in-Depth (D^3)

In theory, diversity and defense-in-depth (D^3) is a good thing. If a security policy, technical control, or programmable digital device performing a critical function should fail, a backup device that is different in kind, should not fail in the same way at the same time.

Defense-in-depth has been described many ways, but one of the most visual analogies is layers of Swiss cheese, in which the holes in the cheese are analogous to vulnerabilities or gaps in security measures. Any threat that passes through a hole in the first layer of cheese is stopped by a second or third layer of cheese below, if the holes do not line up perfectly and allow a threat to pass through all the layers of cheese (see Figure 2). In nuclear power plants, defense-in-depth could also be used to describe the different layers of protection for nuclear safety systems: protect against an event, detect occurrence of an event, mitigate the event and implement safety systems to minimize consequences of the event. The scenario in Module 2 focuses on the diversity and defense-in-depth of a licensee's cyber security measures.

There are two important ways D^3 could introduce vulnerabilities that should be considered; true diversity and false diversity. If two components are truly diverse, they are different in kind. Therefore, the two components can be compared to each other, with one being objectively better than the other in various features such as dependability, reliability, security, etc. The inferior component will become the default attack path in a cyber-attack scenario. In this scenario, diversity leads to compromise. If the only mitigation is to remove the inferior component, the mitigation leads to a loss of diversity.

It is much more likely that at some level, two diverse components have something in common. This could be at the hardware, firmware, or software level. Each of these three levels consist of multiple sublevels. For example, software could refer to kernels, operating systems, static or dynamic libraries, drivers, applications, etc.

The growing field of hardware- and software-bill-of materials (HBOM and SBOM, respectively) endeavors to document the base components that make up a component or system. For example, two

different network switch vendors (e.g., Cisco and Linksys) may use the same Broadcom chip, which could suffer from a zero-day remote code execution (RCE) vulnerability. When the RCE is eventually discovered and exploited by an adversary in a cyber-attack, both network switches are vulnerable to the same problem.

NEI-20-07, "Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems," describes common cause failure (CCF) in a risk-informed, performance-based manner, which should be a familiar concept in the nuclear industry. [7]

In this case, diversity was assumed by purchasing network switches from different vendors. Without accurate HBOM and SBOM, it was unknown that they both shared a common component, providing a false sense of diversity.

This module may be used separately as steps 3-4 of the Cyber Kill Chain (e.g., Weaponization and Delivery) or in conjunction with Module 1 (i.e. Reconnaissance). N.b. Step 2 of the Cyber Kill Chain is rarely observable—taking place outside the electronic perimeter of the victim, unless "living off the land" methods are used. Even in these cases, skilled adversaries will conduct research and practice in a test environment to avoid detection and improve the probability of achieving their goal (i.e. step 7 or Actions on Objective).

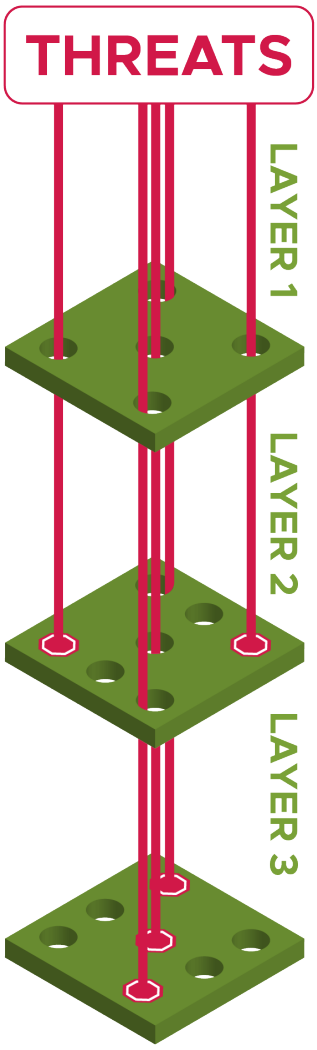

Figure 2. Defense-in-Depth

Day 1 - 11

Module 1 (see above) describes step 1 of the Cyber Kill Chain and how an adversary may begin to learn technical details about your organization. In this module, we assume that the adversary has discovered through online job postings or information or open-source news events that specific technology such as Main Feedwater Digital Controls Systems or Reactor Protection Systems, such as Eagle 21 Microprocessor, is used in a plant system.

Using this information, the adversary proceeds to step 2 of the Cyber Kill Chain—Weaponization. These activities are rarely visible to an organization. Over a period of three to six months, the adversary builds their own HBOM and SBOM. Using this information, the adversary looks for known vulnerabilities (e.g., CVEs, CWEs, etc.) which may be weaponized with little to no effort using tools such as Metasploit or Cobalt Strike.

Finding none, the adversary begins to research ways to crash a component both devices have in common. Another well-known cyber-attack recipe is:

1. Learn how to crash the device
2. Learn how to execute arbitrary code on recovery
3. Learn how to turn arbitrary code execute (ACE) into remote code execution (RCE)

TEPs

Please see Module 1.

Day 180

Having spent the last six months developing their own RCE, the adversary is now ready to move on to step 3 of the Cyber Kill Chain (i.e. Delivery). Assume the spear phishing campaign in Module 1 Day 45 (see above) is successful and delivers malware into the utility's network. This malware includes privilege escalation such as a reverse TCP shell executed in kernel-land that allows the adversary to progress through steps 4-5 of the Cyber Kill Chain (i.e. Exploitation and Installation) in a matter of minutes.

TEPs

Please see Module 1.

Day 181

After a member of the board falls victim to the adversary's spear phishing campaign, malware installing a reverse TCP shell has been placed on a system that is connected to the Internet.

The adversary uses this initial installation of malware (steps 3-4 of the Cyber Kill Chain) to gain initial access to one of the organization's systems. From this foothold, the adversary conducts additional reconnaissance (step 1) and further weaponization, delivery and installation (steps 2, 3, and 4 respectively) to look for additional targets (i.e. pivoting) until they find a system of interest that furthers their actions on the objective (step 7 of the Cyber Kill Chain).

For Consideration

- Many OT networks are fully connected logically, or worse—physically. This is also known as a "flat network", where there is no physical or logical segmentation (i.e. separation). Ensure the best practice of network segmentation is followed.
- Many OT networks take too much credit for being "air gapped" (i.e. not connected to the Internet). But there are many ways malware can be pushed to an "air gapped" network.

Brainstorm different ways malware could infiltrate your network. Also brainstorm how sensitive data may be exfiltrated from your network.

  - Many programmable digital devices provide an HTTP (i.e. web) user interface that can allow for arbitrary interactions or malicious activity.

  - If you need inspiration, investigate cyber security research that demonstrates malware can be transmitted and received via a computer speaker[1] or private keys can be determined by analyzing a server's power LED[2]. Other options may include rogue commodity Wi-Fi switches, forgotten third-party vendor access, managed security service provider updates[3], I&C laptops that bridge multiple networks, USB thumb drives, violation of established policy, etc.)

- Implement best practices to log, detect, alert, and prevent reconnaissance activity.

- Establish a normal baseline and automate anomalous alerts for privileged activity that violates the normal baseline (e.g., long connection times, unusual number of connections, etc.).

- Implement policies and procedures to grant, review, and revoke third-party network access.

- Firewalls, zero-trust architecture, software-defined networking, and other technologies should be used to implement a deny-by-default approach to network communications between programmable digital devices on the same subnet, at gateways, and at electronic perimeter boundaries.

- Review as-designed, as-built, and as-found network documentation for legacy or insecure protocols like TELNET (TCP 23) and FTP (TCP 21) that could leak information. For example, both protocols use clear text to transmit user credentials. If an adversary can observe a trivial system password that reveals the algorithm used to generate the password (e.g., system abbreviation + system name + month + year -> "DEVWWW092025"), the system password of a more impactful system could be guessed with little to no effort by the adversary.

  - If you use certificates for user or system account authentication, follow best practices to monitor and protect certificates to prevent theft and reuse.

[1] https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

[2] https://arstechnica.com/information-technology/2023/06/hackers-can-steal-cryptographic-keys-by-video-recording-connected-power-leds-60-feet-away/

[3] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

TEPs

- Active network scanning techniques like ping sweeps and port scans. Port scans may range in TTP from novice brute-force to well-known ports, or even previously compromised ports like TCP 1337 to take advantage of a previous adversary's work to establish persistent access.

Day 188

After enumerating active host IP addresses and the open service ports and what services are behind those ports, the adversary can use existing exploit code from the open-source Metasploit framework to pivot to and escalate privilege on the target database server using a remote buffer overflow attack. Well-resourced adversaries may use commercial penetration testing software like Cobalt Strike or develop their own exploits from scratch, which can be extremely difficult to detect due to a lack of previously known signatures. This is why establishing a normal baseline and investigating anomalous activity is especially valuable.

For Consideration

- Review log sources to support anomaly detection such as a flood of data that may indicate a remote buffer overflow or other type of attack.

TEPs

- TEPs will vary but should focus on previously discovered vulnerabilities of prior versions of production software used by your organization. This mimics the "low hanging fruit" an adversary will look for first.

- Other TEPs could include application specific tools such as "dib", "nikto", ZAP etc., for scanning and enumerating web sites and web applications, which are often used as configuration and management interfaces for digital programmable devices.

Day 189

Many people misconstrue the exploit used to gain initial access to a system as the actual cyber-attack. At this point, the adversary has only accomplished steps 1-4 of the Cyber Kill Chain. Now they establish persistent access and attempt to cover the evidence of their reconnaissance, deliver, and exploitation activities that got them this far.

If an organization already has an established method of providing remote access, blending in with that method, such as adding their own SSH key, modifying firewall rules, creating a user in Microsoft's Active Directory (or another centralized credential store like LDAP), or adding themselves to Microsoft Remote Desktop User Group.

For Consideration

- A technique called "living off the land" uses existing tools found on target systems to gain additional access. Microsoft Power Shell or Linux Bash Shell are very commonly abused tools. Additional command line tools for querying and modifying Active Directory (e.g., `dsquery`, `dsadd`, `dsmod`, etc.) may be used to create or modify accounts. Scripting interpreters and package management libraries are also very commonly used in Linux systems. Implement security policies and security controls to remove or monitor execution of these types of tools.

- Implement logging and alerting to detect the creation or modification of local and/or centralized user accounts.

- Implement specification-based rules to track remote connectivity anomalies such as the same administrator being logged in more than one time, logging in from an unusually distant geo-IP, executing commands that are not normal for that user or roll, or other insider threat or abuse-like activity.

- Implement multi-factor authentication (MFA) or two-factor authentication (2FA) for sensitive user access.

TEPs

- TEPs will vary depending on remote connectivity, security policies and security controls related to that remote connectivity, and method of authenticating users.

    - TEPs should include white card activities or actual network activities including privilege escalation, account creation, account modification, configuration management changes to host and/or network-based security controls such as logging, intrusion detection/prevention, etc. and establishment of initial access and remote connectivity.

Module 3—Loss of View for Plant Monitoring System (PMS)

Day 279

Command and control (C^2) activity between the adversary and malware on a compromised system occurs.

In this scenario, the installed malware is in support of a "man-in-the-middle" (MitM) attack, which can alter set points, measurement points, or both. MitM attacks are relatively easy to pull off in traditional IT or OT networks. Because of their robust design (e.g. four sensors and two channels), a MitM attack is still feasible, but requires compromising more systems or targeting the environment below or above system redundancies.

Existing penetration testing frameworks like Metasploit and Cobalt Strike are often used by adversaries to perform C^2 activities on compromised digital devices. An APT may make use of a covert channel to reduce the probability of detection.

For Consideration

- Implement a baseline of normal network communications.
- Implement security controls to detect and alert on anomalous network communications.
- Practice triaging alerts.
- Regularly review new threats and new adversary TTP. Keep logging and alerting up to date.
- Perform threat hunting in your network. Look for indicators of compromise and C^2 activity within your networks.
- Brainstorm ways to maintain mission assurance despite network compromise.
- If mitigation plans include network isolation, analyzed the impact of loss of availability on other systems.

TEPs

- Anomalous network traffic is observed on the network:
    - Anomalous network traffic may be from the same source (easy to detect).
    - Anomalous network traffic may be from different sources, but with similar payloads (less easy to detect).
    - Anomalous network traffic may be from a trusted source, but communicate in an unexpected way [e.g., different protocol (i.e. destination port), or different payload] (harder to detect). This is a common method of pivoting from one compromised internal system to another.
    - Anomalous network traffic may be from a trusted source but vary in timing [i.e. a covert timing channel] (difficult to detect).
- For high fidelity, a penetration testing toolkit like Metasploit or Cobalt Strike could be used to generate C^2-like network traffic.
    - If a digital twin is available, consider downgrading to make use of actual CVEs based on availability of existing exploits in Metasploit or Cobalt Strike. N.b. This approach should only be used in air-gapped networks for training purposes!

Day 280

The actions on the objective by the cyber adversary will vary depending upon the type of system compromised. The goal of the action is to violate the integrity of a measurement system leading to a limited operating condition (LCO) with the hope of tricking an operator into performing a remedial action that leads to a loss of availability due to safe shutdown or perhaps even damage to a system if there is enough disagreement between reported and actual measurements depending on the impacted system.

After the events of Three Mile Island (1979), reactor operators do not act based on a single indicator due to the possibility of a single failed instrument.

For Consideration

Review the following impacts based on an effective man-in-the-middle attack by a cyber adversary. (N.b. this attack does not change the actual readings of any sensor or the underlying environment—merely the reporting of value or values to the operator. For example, abnormal operations procedures (AOPs) are provided for diagnostic instruments that indicating incorrect pressure, temperature, water level or water flow. The abnormal operations procedures provide steps to verify correct operations of sensors and channels through local field verification or monitoring redundant indicators. In some cases, verified and validated cyber security scenarios and/or operating anomalies would require entrance into emergency operating procedures (EOPs). For example, incidents that involve straying from crucial set points or established limits would trigger an EOP after completion of cross-checks or validation of set points or limits

TEPs

TEPs will vary based on systems targeted by the adversary and the fidelity of the training environment. Potential TEPs may include:

- High or low pressure
- Valve position
- Water Level
- Flow rate (i.e. gallons per minute)

Partial Cybersecurity Scenarios

The following scenarios were identified as having impact on advanced modular reactor cyber security but were not turned into full scenarios due to limited project resources. They are included here for completeness. These partial scenarios could be the building blocks for tabletop exercise, implemented as a hands-on red-team / blue-team activity, to be used to generate discussion as a training activity, or even just to initiate a conversation with subject matter experts across departments.

These partial scenarios could be expanded upon by owners, operators, vendors, academic institutions, or national laboratories, research laboratories to advance the science of cyber security for advanced modular reactors. The template in Section 5 can be used to plan exercise based on this partial scenario.

Module 4—Lagging Regulations, Guidance, and Standards

Cyber security has always been co-evolutionary. Adversaries weaponize newly found vulnerabilities to escalate privilege and violate confidentiality, integrity, and availability in previously unseen ways. Defenders observe new adversarial tactics, techniques, and procedures (TTP) and develop their own detection, mitigation, response, and recovery methods, which force adversaries to look for new methods as their old TTPs become less effective. The saying, “attacks only get better” (often attributed to Bruce Scheier), aptly sums up this never-ending contest between attackers and defenders.

Most industries resist regulations, but when it comes to the availability of critical infrastructure or public health, some regulations are necessary to ensure adequate safety. There are two prevailing approaches to regulating cyber security: compliance-based regulation and performance-based regulation. Compliance-based regulation is objectively easier to write, implement and enforce. Compliance-based regulation clearly states the requirements to secure assets. Unfortunately, compliance-based regulation is also objectively less effective compared to performance-based regulation.

Writing clear, precise, and effective regulations can take many years. Any compliance-based regulation would likely quickly become outdated given the nature of constantly evolving cyber-attacks. Therefore, a risk-based approach is more favorable. However, each organization may face different risks, that require different approaches to detection, mitigation, response, and recovery. This makes writing, implementing, and assessing risk-based compliance difficult.

The domain of NRC regulation can be difficult to understand for the uninitiated. Consider the verification and validation (V&V) standard (reference) which dates to 2004! The standard was “modernized” based on IEEE 74.3.2, which dates to 2016, but not yet adopted at the time this document was written (September 2025). In the meantime, IEEE has updated their 2016 guidance. This example illustrates how outdated regulation can lag behind industry, often by decades.

The following is a list of industry standards, guides, and rules that should be reviewed from an adversarial viewpoint to identify gaps that could indicate weakness or vulnerabilities that an adversary could leverage in a cyber-attack.

1. NUMARC/EPRI TR-102348, “Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-To-Digital Replacements Under 10 CFR 50.59 (Generic Letter 95-02)”

2. 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”
3. 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”
4. 10 CFR 73, “Physical Protection of Plants and Materials”
5. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (formerly NUREG 75/087) - (No chapter dedicated specifically to cyber—see Chapter 7).
6. Branch Technical Position (BTP) 7-8, “Guidance for Application of Regulatory Guide 1.22”
7. BTP 7-19, “Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Instrumentation and Control Systems”
8. ISG-06, “Interim Staff Guidance for Digital Instrumentation & Control Systems”
9. IEEE 7-4.3.2 (2016), “Criteria for Digital Computers”
10. Guidance for software life cycles in safety systems at nuclear plants:

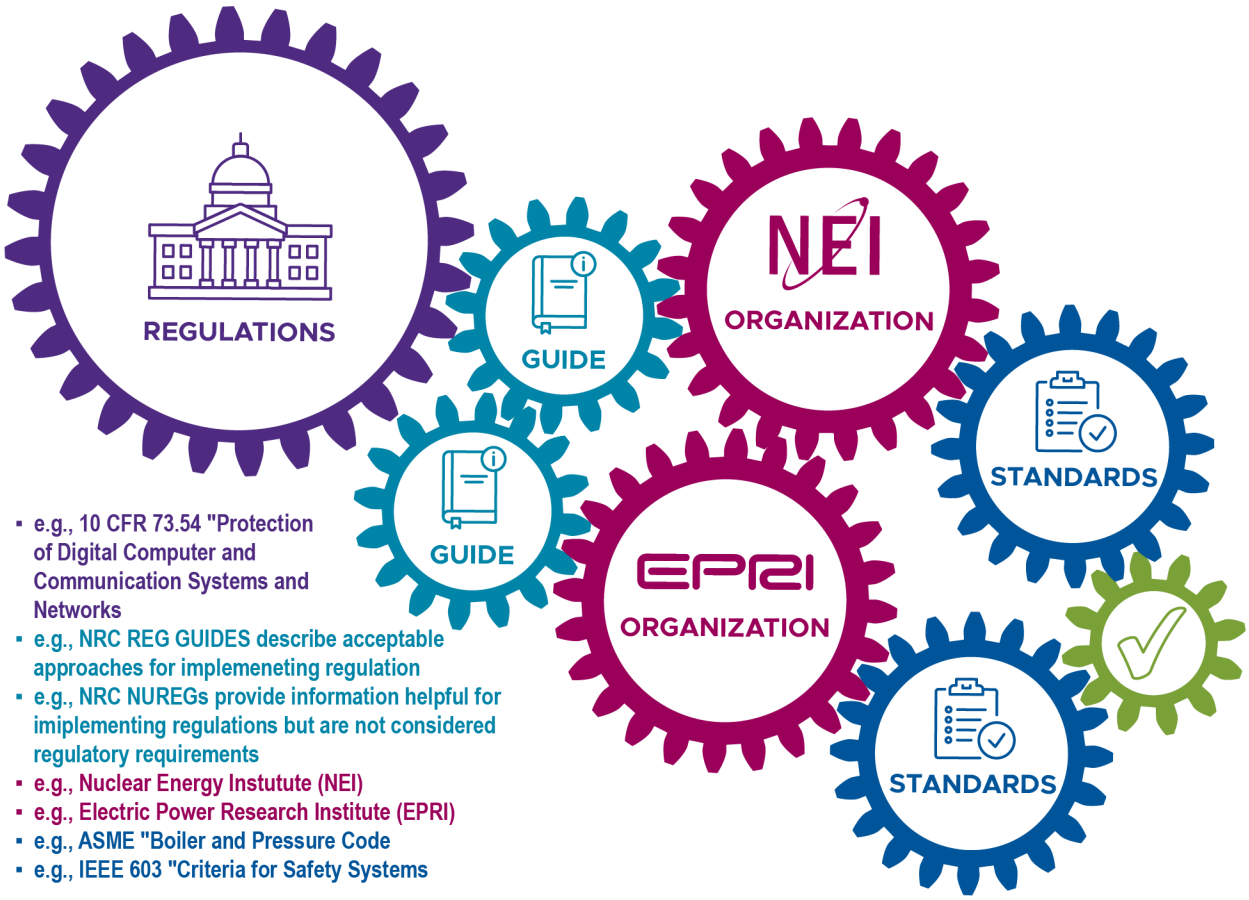

Figure 3. NRC Regulation Framework

a. BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”

b. Regulatory Guide 1.152, “Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants”

11. Guidance on verification and validation (V&V) in safety systems:

    a. EPRI 3002011816 Digital Engineering Guide Section 4.2

    b. IEEE Standard 1012 (2016), “System, Software and Hardware Verification and Validation”

12. For example, gaps may exist between using older software engineering methodologies or adopting out of date IEEE standards, or changes to human-interface design review guides, such as NUREG-0700. With the length of time between the design, construction and licensing stages of advanced reactors, design standards and regulations may be out of date by the time an operator receives an operating license. Broad topics to consider:

    a. Management

    b. Acquisition (Supply Chain)

    c. Supply

    d. Concept Development

    e. Requirements Analysis (Traceability)

    f. Detailed Design

    g. Construction, including Unit Test

    h. Integration (This is where many cyber problems can be found!)

    i. Interface points with other systems, human factors engineering, HMI, hardware, etc.

    j. Qualification

    k. Acceptance

    l. Operation

    m. Maintenance

    n. Disposal

NRC approval of plant system's design and operations comply with regulations and standards reviewed during the pre-licensing period. Licensees are legally bound to the document version referenced in their licensing basis documents. Plant owners generally would not upgrade system designs to current standards unless it is modifying an interconnected system or required by a regulator for safety reasons. Nonetheless, known security vulnerabilities on systems designed to older standards can be exploited by an adversary.

Module 5—Vulnerability Introduced by Diversity and Defense-in-Depth (D^3) [Deep Dive]

In theory, D^3 is a good thing, but there are two ways D^3 could introduce vulnerabilities:

1. False diversity:
    a. An unknown common component may be hidden at the hardware, firmware, software, or information level. For example, two different router manufacturers (e.g., Cisco and Linksys) may use the same Broadcom chip with a remote code execution (RCE) vulnerability.
    b. Common Cause Failure is a familiar concept in the nuclear industry—see NEI-20-07. Opaque similarity in D^3 could represent a shared vulnerability and lead to a common cause failure.
2. True diversity:
    a. Two truly different components can be objectively compared, and one could be less secure, leading to a specific attack path and loss of D^3 if the only mitigation is removal.
    b. Deploying two of everything results in double the attack surface.

For an introductory module based on D^3, please see Section 3.2 above. This partial scenario would expand upon the technical feasibility of obtaining privilege escalation to perform actions on object (the final step of the Cyber Kill Chain).

Module 6—Loss of Control for Diverse Action Scheme (DAS)

When used together, the three full scenarios (Modules 1-3 above) correspond to all seven steps of the Cyber Kill Chain. However, the action on objective in Module 3 is only a loss of view (i.e. integrity) of remote monitoring points. While changing these readings could lead a reactor operator to make an incorrect decision or take an unintended action that benefits the adversary, all things being equal, the adversary has not caused any real harm unless they can trick an operator into taking an action outside of established policies and procedures.

In Module 6, we propose a loss of control, which is a much more severe attack on the integrity of a system. In this module, the adversary also changes control points, not just readings. If readings are also changed (e.g., a "man-in-the-middle" attack), operators may not be aware that set points have been changed. This gives the perception of "situation normal" while levels, temperatures, and/or pressures

are driven high or low at the direction of an adversary that can command a system to dangerous consequences.

Below is an outline of events that could be white carded or developed with different degrees of fidelity for use in a cyber range or training exercise to assist with practicing policies and procedures in response to all seven steps of the cyber kill chain.

- Recon (See Module 1 above.)
- Weaponization (See Module 1 above.)
- Delivery
- Remote (e.g., IP-based) (See Module 2 above.)
    - Remote (e.g., Supply-chain—see Module 7 below.)
- Exploitation (See Module 2 above.)
- Installation (See Module 2 above.)
- C^2 (See Module 3 above.)
- Actions on Objectives Use the template in Section 5 to plan your own exercise based on this partial scenario.

Module 7—Supply Chain Risks to FPGAs

Supply chain risk management (SCRM) is an emerging branch of cyber security. Field programmable gate arrays (FPGAs) bridge the gap between general-purpose software and purpose-built hardware. Once programmed, FPGAs are far more deterministic programmable digital devices that add provable system safety when implemented correctly.

This forces a motivated adversary (e.g. advanced persistent threat like a nation state) to target supply chains to embed vulnerabilities and malicious logic that can be triggered at the time and place of their choosing to facilitate an effective cyber-attack.

The plant's Engineering group and FPGA subject matter experts (SMEs), evaluate how FPGAs are procured, implemented, and maintained in plant's hardware/software lifecycle.

.

References

[1] Lockheed Martin. “The Cyber Kill Chain”. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[2] Nuclear Regulatory Commission. SRM-SECY-22-0076: Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems. May 25, 2023. Accession Number ML223145A176

[3] Nuclear Regulatory Commission. Regulatory Guide 1.250, “Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants.” Revision 0. October 2022. Accession Number ML22153A408

[4] Westinghouse. WCAP-16674-NP/APP-GW-GLR-065, AP1000 I&C Data Communication and Manual Control of Safety Systems and Components, Revision 4, February 2011. <https://www.nrc.gov/docs/ML1105/ML110590487.pdf> Accessed 9 September 2025

[5] Nuclear Regulatory Commission. Regulatory Guide 5.71, “Cybersecurity Programs for Nuclear Power Reactors,” Revision 1, February 13, 2023, ADAMS Accession No. ML22258A204

[6] NEI 08-09, “Cyber Security Plan for Nuclear Power Plants” Revision 6 https://www.nrc.gov/docs/ML2406/ML24061A055.pdf accessed on 27 October 2025

[7] NEI-20-07, “Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems,” Revision E, July 2023 https://www.nrc.gov/docs/ML2407/ML24074A463.pdf accessed 27 October 2025

[8] Paragon Energy Solutions Technical Course in Licensing Digital and Nuclear Instrumentation Systems, Feb 17-21, 2025; Module 1.4 Digital Systems Applications