SAND2023-05188C

Proceedings of the 2023
30th International Conference on Nuclear Engineering
ICONE30
May 21-26, 2023, Kyoto, Japan

ICONE30-1709

AN EFFICIENT GRADED APPROACH FOR THE DESIGN OF SECURE INSTRUMENTATION AND CONTROL SYSTEMS

Lee T. Maccarone
Sandia National Laboratories
Albuquerque, NM

Jacob R. James
Sandia National Laboratories
Albuquerque, NM

Daniel R. Sandoval
Sandia National Laboratories
Albuquerque, NM

Alexandria W. Haddad
Sandia National Laboratories
Albuquerque, NM

Michael T. Rowland
Sandia National Laboratories
Albuquerque, NM

ABSTRACT

Prescriptive approaches for the cybersecurity of digital nuclear instrumentation and control (I&C) systems can be cumbersome and costly. These considerations are of particular concern for advanced reactors that implement digital technologies for monitoring, diagnostics, and control. A risk-informed performance-based approach is needed to enable the efficient design of secure digital I&C systems for nuclear power plants. This paper presents a tiered cybersecurity analysis (TCA) methodology as a graded approach for cybersecurity design. The TCA is a sequence of analyses that align with the plant, system, and component stages of design. Earlier application of the TCA in the design process provides greater opportunity for an efficient graded approach and defense-in-depth.

The TCA consists of three tiers. Tier 1 is design and impact analysis. In Tier 1 it is assumed that the adversary has control over all digital systems, components, and networks in the plant, and that the adversary is only constrained by the physical limitations of the plant design. The plant's safety design features are examined to determine whether the consequences of an attack by this cyber-enabled adversary are eliminated or mitigated. Accident sequences that are not eliminated or mitigated by security by design features are examined in Tier 2 analysis. In Tier 2, adversary access pathways are identified for the unmitigated accident sequences, and passive measures are implemented to deny system and network access to those pathways wherever feasible. Any systems with remaining susceptible access pathways are then examined in Tier 3. In Tier 3, active defensive cybersecurity architecture features and cybersecurity plan controls are applied to deny the adversary the ability to conduct the tasks needed to cause a severe consequence. Tier 3 is not performed in this analysis because of the design maturity required for this tier of analysis.

Keywords: Cybersecurity; Operational Technology; Instrumentation and Control; Industrial Control Systems; Risk

1. INTRODUCTION

Under the United States Nuclear Regulatory Commission (US NRC) Regulatory Guide 5.71 [1], licensees of light water reactors (LWRs) have been required to broadly apply a large set of technical and operational cybersecurity controls to all identified critical digital assets (CDAs). For advanced reactors (ARs), this prescriptive approach places a large time and resource burden on the licensee and does not allow the licensee the flexibility to prioritize the systems with the greatest potential for physical harm. The regulation that sets cybersecurity policy for ARs, Title 10 of Code of Federal Regulations (10 CFR) 73.110 specifies, "Technology neutral requirements for protection of digital computer and communication systems and networks," and is currently in draft review stages [2]. The draft rule proposes a graded approach to cyber security controls based on potential consequences of credible postulated attacks at each risk level.

To address the requirements outlined in 10 CFR 73.110, the US NRC has presented "U.S.A. Regulatory Efforts for Cyber Security of Small Modular Reactors/Advanced Reactors," at the International Atomic Energy Agency (IAEA) Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors [3]. The presentation included a three-tier cybersecurity analysis approach proposed in the draft regulatory guide. The methodology is pre-decisional,

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

but the concepts are used in this paper to analyze a hypothetical heat pipe reactor design and develop a risk-informed cybersecurity design.

The Tiered Cybersecurity Analysis (TCA) is demonstrated for a hypothetical high-temperature heat pipe microreactor in the system-level design phase. The TCA begins with a candidate digital control system design. In Tier 1 analysis, passive safety features of the reactor are examined. Accident sequences that are not mitigated by passive safety features are examined in Tier 2. In Tier 2, measures are implemented to deny the adversary access to pathways needed to cause the unmitigated accidents. Finally, Tier 3 analysis is used to identify active cybersecurity controls for any pathways that are not defended in Tier 2. The outcome of the TCA is a risk-informed instrumentation and control (I&C) system design that achieves defense-in-depth (DID) through a graded approach.

2. BACKGROUND

The need for a tiered (or iterative) approach for cyber risk management is captured in many standards such as NIST SP800-37 [4], IAEA NSS 17-T [5], and the draft 10 CFR 73.110 [2]. NIST SP800-37 affirms the need for an organization-wide risk management approach originally established in NIST SP800-39 [6]. This organization-wide approach has three levels: organization, mission/business process, and information system. NIST SP800-37 also provides a seven-step risk management framework to address risk at each of these levels [4].

The IAEA NSS 17-T emphasizes the protection of functions using a Defensive Cybersecurity Architecture (DCSA) (IAEA publications use the term "computer security" rather than "cybersecurity") [5]. Several key definitions are quoted below from NSS 17-T.

- Function: "a coordinated set of actions and processes that need to be performed at a nuclear facility" [5].
- Security Level: "a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function" [5].
- Security Zone: "a logical and/or physical grouping of digital assets that are assigned to the same computer security level and that share common computer security requirements owing to inherent properties of the systems or their connections to other systems" [5].

Figure 1 shows the relationship between functions, levels, and zones. The facility computer security risk management (CSRM) plan pertains to the relationship between facility functions and security levels, and the system CSRM plan pertains to the relationship between the systems and security zones.

A zone is a region bounded by logical and physical protections which contains at least one system. Communication between assets within a zone is trusted, while communication between different zones is restricted and controlled [5]. Zones are the arrangement in a DCSA that provide DID against cyber-attacks, by placing the most significant assets within the most protective boundaries.

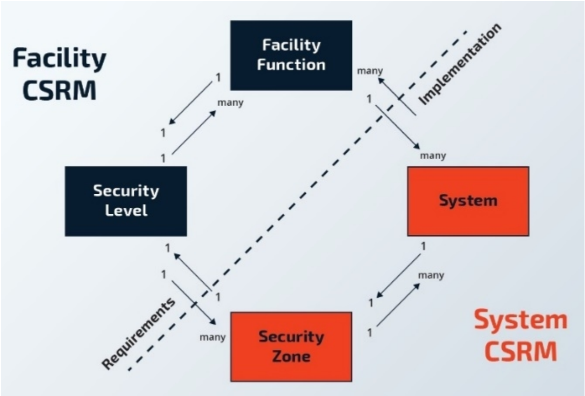

Figure 1: DCSA FEATURES AND THEIR RELATIONSHIPS [5]

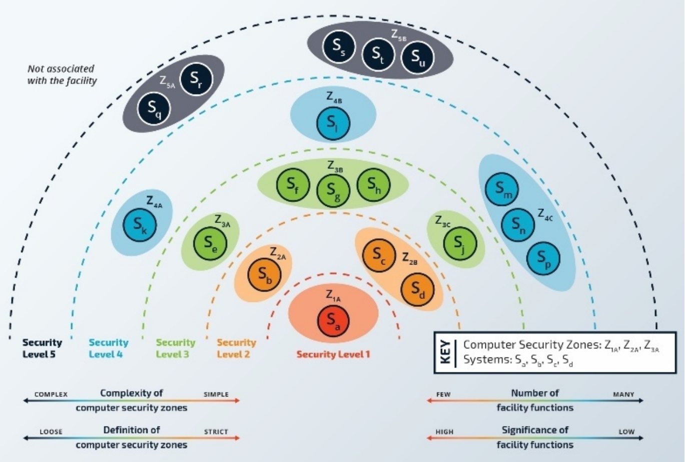

Figure 2: CONCEPTUAL DCSA MODEL [5]

DCSA levels provide a framework for implementing security measures corresponding to the criticality of each level. Each plant function is assigned a level based on its criticality. The stringency of measures put in place for a given level is directly related to the significance of the function protected by the level. Levels allow flexibility in security requirements across the facility which allows designers to prioritize the areas of greatest risk. Each level includes one or more zones. Figure 2 provides an example of how DCSA zones and levels would be implemented.

The TCA given in the draft DG-5075 (RG 5.96) that meets the proposed draft rule 10 CFR 73.110 is consistent with the risk management approaches presented in NIST SP800-37 and IAEA NSS 17-T. The tiered nature of the TCA is adapted from the organization-wide approach developed in NIST SP800-37, and the TCA leverages DCSA principles given in IAEA NSS 17-T.

3. TIERED CYBERSECURITY ANALYSIS

The TCA is a cybersecurity assessment methodology that aligns domestic standards, international standards, and technical guidance to select Secure-by-Design (SeBD) requirements to develop defensive network architectures and apply effective cybersecurity controls. This section provides an overview of the TCA methodology. The TCA process is shown in Figure 3.

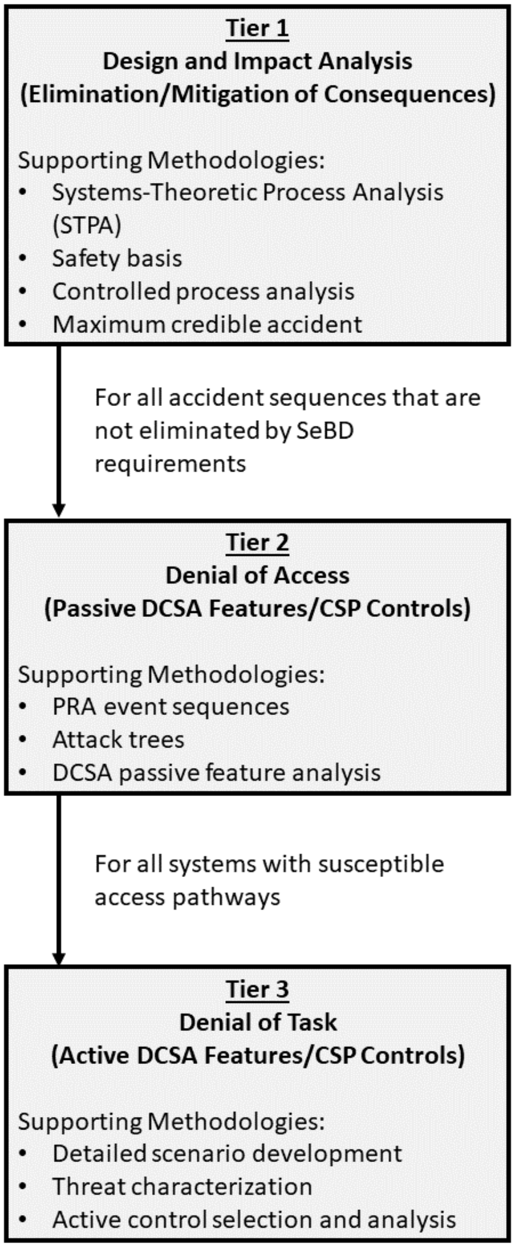
Tier 1
Design and Impact Analysis
(Elimination/Mitigation of Consequences)
Supporting Methodologies:
• Systems-Theoretic Process Analysis (STPA)
• Safety basis
• Controlled process analysis
• Maximum credible accident
For all accident sequences that are not eliminated by SeBD requirements
Tier 2
Denial of Access
(Passive DCSA Features/CSP Controls)
Supporting Methodologies:
• PRA event sequences
• Attack trees
• DCSA passive feature analysis
For all systems with susceptible access pathways
Tier 3
Denial of Task
(Active DCSA Features/CSP Controls)
Supporting Methodologies:
• Detailed scenario development
• Threat characterization
• Active control selection and analysis

Figure 3: TIERED CYBERSECURITY ANALYSIS

The TCA begins by considering unacceptable consequences (e.g., radiological release) and plant control actions that can lead to unsafe states. The process assumes that safety analyses pertinent to the consequences of concern have been performed prior. Tier 1 of the TCA is Design and Impact Analysis and is used to evaluate safe-by-design features. SeBD is an extension of safe-by-design. While safe-by-design considers how consequences of an accident or random failure can be mitigated or eliminated, SeBD considers the mitigation or elimination of consequences caused by an adversary. While these design features would have already been assessed in the safety analysis, security analysis asks two unique questions:

1. Can safe-by-design elements be credited for cybersecurity purposes such that the physical plant design or controlled process does not allow the most advanced adversary to achieve a consequence? That is, are protections at Tier 1 sufficient to prevent the adversary's desired outcome, regardless of the adversary's ability to compromise a system?

2. Can an adversary circumvent safety considerations in the design and achieve accident conditions considered to be unlikely from a safety perspective?

If it is determined that SeBD elements and passive safety features are not able to fully eliminate the consequence, then Tier 2 (Denial of Access) is required for the functions that are in place to mitigate the consequence. This generally takes the form of accident sequences, and analyzes each function credited by safety with preventing accident conditions following an initiating event. Key considerations in the Tier 2 analysis are access pathways. A function may have supporting systems, networks, and components that represent access points for the adversary. The goal is to inform secure network architecture and passive security features at this level, or otherwise identify areas that require further control measures, and therefore further analysis in Tier 3 (Denial of Task). Tier 3 analysis is performed for all systems analyzed in Tier 2 that require further control (i.e., systems for which passive safety features do not mitigate all access pathways). Tier 3 analysis is an assessment of more detailed scenarios and the active cybersecurity plan (CSP) elements that can be implemented to protect the system.

The remainder of this section discusses each of the tiers of the TCA. For more information readers are encouraged to refer to [7].

3.1 Tier 1 Analysis

The goal of Design and Impact Analysis is to evaluate the plant's safety design features and determine if they can be credited as SeBD features. Crediting the design features means that they would prevent an attack from leading to an unacceptable consequence, and therefore a more detailed analysis of the scenario is not required. To make this claim, the impact of an attack would need to be eliminated. Protective measures that would delay an attack are valuable to the security of the plant, but still require Tier 2 analysis of the function because the impact is not eliminated. Abstraction at the three tiers is best thought of as adversary capabilities. At Tier 1, the scenarios are developed considering an adversary that is limited only by the physical limitations of the plant design. This adversary is assumed to have access to any digital system, component, or network in the plant, and is assumed to be capable of implementing any control action within the capability of the system.

3.2 Tier 2 Analysis

The goal of Denial of Access Analysis is to evaluate adversary access vectors and implement passive measures to deny system and network access. At this tier of analysis, it is assumed that the adversary can achieve their objective if they gain access to the appropriate systems. Once again, safety analyses are taken as inputs and used to identify unsafe event sequences. One method to represent attack sequences and bound the scope of scenarios is to use traditional probabilistic risk assessment (PRA) event trees. Each plant function that must operate to mitigate an accident should be considered. This analysis should examine each system in the sequence of plant functions required for accident mitigation and identify available pathways for an adversary. The results of Tier 2 analysis are passive or deterministic DCSA or CSP elements.

For each function that supports plant safety, access pathways that need to be considered include, but are not limited to, the following:

- Physical access
- Wired network access
- Wireless network access
- Portable media/mobile device interface

Attack trees can be developed to capture the complexity of combined access vectors. A comprehensive analysis examines and improves security around each node of the attack tree. The attack trees can be used to identify critical points of common access or common points of failure across multiple attack scenarios. A DCSA can then be developed using insights from the attacks. When an access pathway is eliminated, no further analysis is required for that vector on the system. When an access pathway is mitigated, prescriptive controls should be implemented to ensure the mitigative measures are effective against all attacks. Unmitigated access pathways require Tier 3 analysis.

3.3 Tier 3 Analysis

The goal of Denial of Task Analysis is to provide risk-informed control measures to unmitigated systems identified in Tier 2. In Tier 3, it is assumed that the adversary has obtained the access required to achieve their objective and control measures must be implemented to prevent the adversary from completing their objective. Generally, a body of controls may consist of baseline controls and risk-informed controls. Baseline controls apply broadly and provide information security assurance while risk-informed controls treat a specific identified risk. There are several methods that can be leveraged to identify applicable risk-informed controls (e.g., combining control action modeling using STPA and adversary sequence modeling using attack tree modeling).

4. TCA DESIGN MATURITY REQUIREMENTS

Each tier of the TCA requires a different level of plant design as input to the analysis. These requirements can be viewed in terms of the phases of plant design maturity defined by the World Nuclear Association (WNA) [8]. The design maturity phases are shown in Figure 4. The first phase of design maturity is the conceptual phase where the reactor concept is developed. In Phase 1 critical questions are asked and major risks are identified. The second phase of design maturity is plant-level design. In Phase 2 the requirements and design parameters of key systems, structures, and components (SSCs) are defined. The third phase of design maturity is system-level design. In Phase 3 the requirements and design parameters of key SSCs are further refined and other plant systems are defined. Finally, the fourth phase of design maturity is component-level design. In Phase 4 the engineering details are finalized for SSCs to allow for manufacturing to begin [8]. The postulated relationship between design phases and TCA requirements is summarized in Table I. Further research is needed on the optimal alignment of the TCA with design maturity.

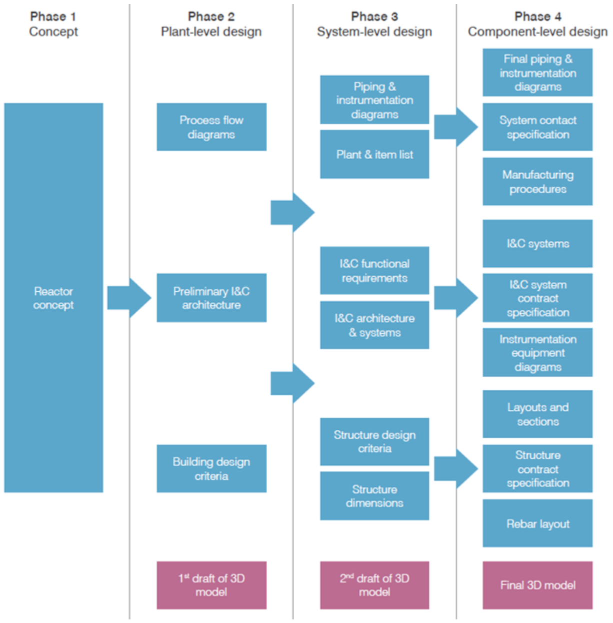

Figure 4: PLANT DESIGN PHASES OF MATURITY [8]

Table I. POSTULATED ALIGNMENT OF DESIGN MATURITY PHASES AND TCA TIERS

Design Phase	TCA Alignment
Phase 1	May begin Tier 1, but cannot complete it
Phase 2	May complete Tier 1
Phase 3	May complete Tier 2
Phase 4	May complete Tier 3

5. ADVANCED REACTOR CASE STUDY

This section presents an abbreviated demonstration of the TCA for a heat pipe microreactor (for a more extensive analysis readers are encouraged to refer to [7]). A microreactor was chosen for this risk-informed cybersecurity analysis for several reasons. First, the dependency on passive and inherent safety features to operate and shutdown the reactor present unique challenges for cybersecurity analysis. Second, microreactors are currently envisioned for deployment to remote geographical areas. The location of microreactors could present unique security challenges compared to the existing LWR fleet. For example, remote locations may necessitate remote monitoring capabilities or autonomous/semi-autonomous operation. Finally, some microreactors designers envision “remote” and/or “autonomous” operation [9].

5.1 System Description

System and operational information were obtained from the Westinghouse eVinci micro reactor Licensing Modernization Project (LMP) demonstration [10]. A physical plant layout and control systems network were not specified in [10], but were developed by using knowledge of nuclear reactor facilities and engineering judgment. Table II provides summary of the demonstration systems selected for the TCA.

Specifically, we focus on the SSC safety classification—that is, safety-related; non-safety-related with special treatment (NSRST); and non-safety-related with no special treatment (NST). A review of the eVinci LMP demonstration, along with other system information, is documented in [11] with further details. For convenience, the microreactor systems along with their safety classification are provided in Table II. Note that the safety classification is derived from a risk-informed analysis, as opposed to a prescriptive or deterministic classification. The safety classification is an important input in the development of the candidate control system network described later in this section.

Table II. EVINCI MICROREACTOR LMP DEMONSTRATION SUMMARY

Function	**System**	**Category**	**Safety Significance**
Reactivity Control	Control Drum Subsystem (CDS)	Active	NSRST
	Emergency Shutdown Subsystem (ESS)	Passive – IAEA Category B	Safety-Related
Decay Heat Removal	Heat Channels in the Core Block Subsystem (CBS)	Passive	N/A – needs further evaluation
	Conduction through CBS	Passive	N/A – needs further evaluation
	Power Conversion System (PCS)	Active	NSRST
Containment	Canister Containment System (CCS)	Passive	Safety-Related
	Secure Vault Subsystem (SVS)	Passive	Safety-Related

The IAEA TECDOC 626 provides an approach to categorize passive systems based on their design and integration with the reactor systems [12]. For the microreactor systems in this study, engineering judgement was applied to determine the passive category for each system. As more system design details are identified, these passive categories should be revisited to ensure accuracy. For simplicity and demonstration purposes within this paper, only the control drum system (CDS) is selected for in-depth evaluation. The control drums (CDs) are rotated in by motors to insert reactivity and rotated out to remove reactivity.

A physical plant layout for the microreactor in this study was developed using knowledge of existing nuclear reactor facilities and engineering judgment. The physical plant layout for the microreactor is shown in Figure 5, with a focused view of the canister containment system shown in Figure 6. Based on design information from eVinci, the canister containment system (CCS) houses the reactor vessel, reactor core, and the I&C equipment needed to support operations [11]. The secure subvault system (SVS) envelopes the CCS to provide passive cooling. Current documentation does not address the modularity or integration of these two systems; therefore it is assumed that the CCS and SVS are decoupled (i.e., constructed separately). Figure 6 also shows the main control elements of the reactor, including the motor controller, sensor aggregation, power, and safety controllers developed using the authors' engineering judgment. Current publicly available documentation does not specify whether they will be inside the CCS.

Not shown in Figure 5 are piping, cables, and control panels that traverse the various boundaries. For example, piping connects the power conversion system (PCS) and the reactor such that the PCS can remove heat from the core via heat pipes. As another example, cables connect the main control room (MCR) to every microreactor system. Current publicly available documentation does not specify these design details, and the physical location of the digital assets may be informed by the cybersecurity analysis.

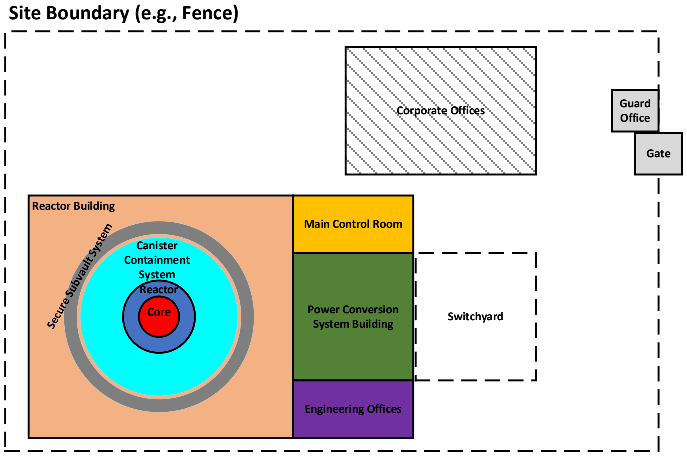

Figure 5: CONCEPTUAL MICROREACTOR PHYSICAL PLANT LAYOUT

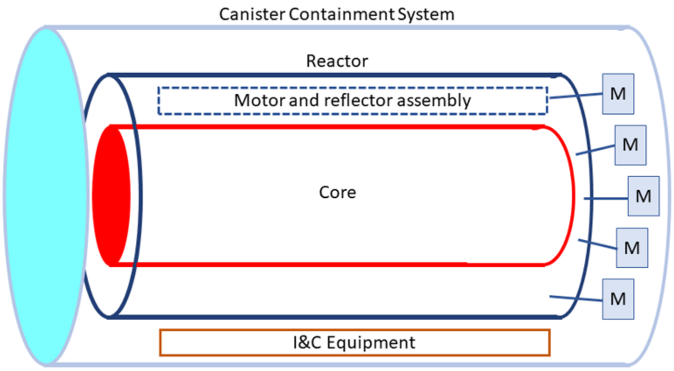

Figure 6. CONCEPTUAL CANISTER CONTAINMENT SYSTEM

The Purdue Enterprise Reference Architecture (PERA) was used as a baseline to develop conceptual control system networks for the microreactor in this study [13]. One important distinction for this implementation of PERA for nuclear reactors is the separation of safety-critical systems. This distinction is highlighted through the control system networks developed here. The network design is summarized in Figure 7. In this network design, the operational technology (OT) system layer is separated from the Internet by a demilitarized zones (DMZ). Within the DMZ a bastion runs only Simple Mail Transfer Protocol (SMTP) and a historian runs SMTP with USB. The OT system layer contains the industrial control devices (i.e., programmable logic controllers (PLCs) and field devices) responsible for non-safety-related systems. Wireless and wired networks are implemented in the OT system layer, and a computer is intermittently connected to the network for updates and maintenance of control devices. A data diode is in place to allow unidirectional data flow from the OT system layer to the DMZ. The safety systems (i.e., ESS, SVS, and CCS) are placed in a separate layer from the other OT networks.

Together, the system selection, safety analysis, physical layout, and control system design can be used to identify cyber-enabled hazards. Cyber-enabled hazards encompass events initiated by a digital asset that then may lead to a hazardous plant state. The goal is to identify unsafe control actions (UCAs) that can potentially be initiated by a cyber adversary. At this stage, we do not identify the causal scenarios or cyber-attack scenarios to determine the likelihood or difficulty of a cyber adversary accomplishing the UCAs. The UCAs are a result of the design itself rather than a cyber analysis. Future analysis is needed to determine the cyber adversary strategies required to access the digital asset and initiate the UCA.

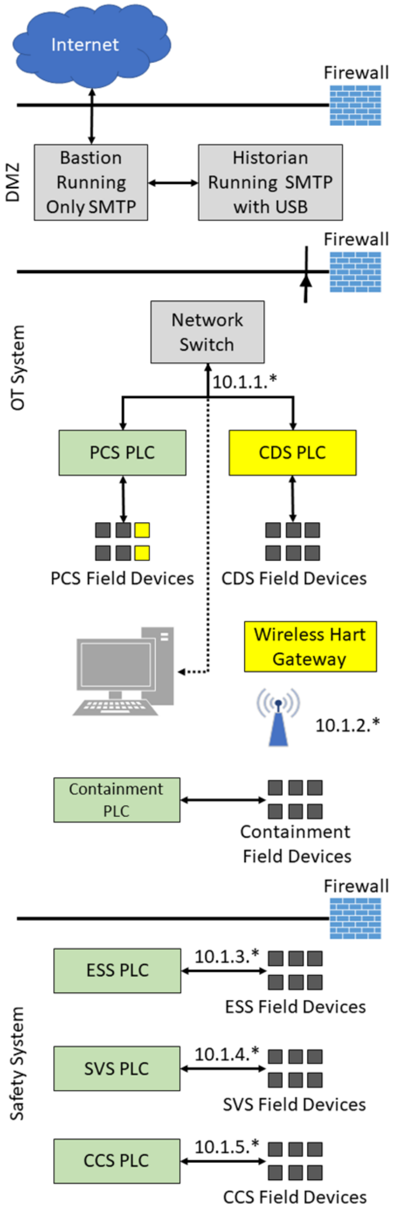

Figure 7. CONCEPTUAL MICROREACTOR SYSTEM ARCHITECTURE

Table III. GENERAL LOSSES FOR NUCLEAR POWER REACTORS

L#	Loss
L1	Release of radioactive material
L2	Loss of power generation
L3	Loss of reputation

Table IV. EXAMPLE REACTIVITY CONTROL HAZARDS FOR MICROREACTOR SYSTEM

H#	Hazard	Loss
H1	Reactivity exceeds $	L1, L3
H2	Reactor inadvertently SCRAMs	L2, L3
H3	Reactivity is too low	L2, L3

Table V. EXAMPLE UCAS FOR THE REACTIVITY CONTROL SYSTEM

CA	UCA (Needed, Not Provided)
CA1: CDS rotates CD in	**UCA1.A1:** CDS does not rotate CD in when reactor power is below desired level [H3]
CA2: CDS rotates CD out	**UCA2.A1:** CDS does not rotate CD out when reactor power is above desired level [H1]
	UA2.A2: CDS does not rotate CD out when neutron flux is too high [H1]

For the microreactor design discussed thus far, Systems-Theoretic Process Analysis (STPA) Steps 1-3 were performed [14]. The results of these STPA steps are summarized in Table III, Table IV, and Table V. The system losses are consequences that are unaccepted to plant stakeholders and the losses for this example are listed in Table III. Hazards are system states that will lead to a loss under a particular set of environmental conditions and the hazards for this example are listed in Table IV. UCAs are control actions that will lead to a hazard under certain conditions, and some examples of UCAs for this case study are listed in Table V. For brevity an exhaustive list of hazards and UCAs cannot be provided in this paper. For more information about STPA, readers are encouraged to refer to [14].

5.2 Case Study Tier 1 Analysis

This Tier 1 analysis uses a system control loop and the assumption that the adversary needs to implement a single UCA. The control loop is valuable in identifying the various points in the process that can be exploited to cause physical harm to the system (e.g., feedback, error correction, actuation). One of the advantages of STPA is that it has already identified these points for reactivity control. This example Tier 1 analysis will focus on the CDS. Three impact scenarios are presented:

1. CD actuation to insert reactivity
2. CD actuation to remove reactivity
3. CDS feedback of CD position

5.2.1 Impact Scenario 1: Control Drum Actuation to Insert Reactivity

Compromise: The adversary prevents the motors from turning the CD in when actual reactivity is greater than needed reactivity. No system constraints have been established that provide a limit to the CD position and the assumed operation based on the system description is that the CD would remain in position and the ESS would eventually be forced to scram the reactor.

Unsafe action resulting from compromise: Based on the STPA UCAs, this compromise would lead to the reactor exceeding power and inadvertent scram.

Design Basis 1.1: Motor speeds exceeding the motor's operational capacity are not considered. If the adversary can instantly move the CD into position and keep it there for a prolonged amount of time, they are in control of the physical harm that results from the attack (note that this specific scenario is an extension of the original UCA of preventing CD rotation). The motor shall be limited to a minimum rotation speed to turn in the CD (which may not be the same speed for turning the CD out).

Design Basis 1.2: A range of CD positions shall be physically limited for reactor operations in all modes to ensure no drum position that could lead to hazardous plant states can be enabled by cyber-attack.

Design Constraint 1.1: The rate of change in voltage sent to the CDS motors should be constrained. This would limit the amount of reactivity insertion that can be achieved by a cyber-attack. While this constraint does not eliminate the cyber-attack, it would slow down the reactivity increase to allow sufficient time for operator intervention.

Design Requirement 1.1: Include a design requirement for a voltage regulator to keep motor speed limited.

Design Requirement 1.2: Include a design requirement for a physical mechanism to set the boundaries for the CD position in each operation mode.

While the design features resulting from this impact analysis do not prevent the potential for harm, they do delay the system's response to the cyber compromise and provide more time to respond following detection. Tier 2 analysis is still required for reactivity control via CDS.

5.2.2 Impact Scenario 2: Control Drum Actuation to Remove Reactivity

Compromise: The adversary prevents the motors from turning the CD out when actual reactivity is below needed reactivity. This forces the neutron flux to remain low or decrease while the reactor is at normal operating conditions. The CD would remain in a turned-out position and other systems would be forced to intervene.

Unsafe action resulting from compromise: Based on the STPA UCAs, a failure of this kind would lead to the reactor decreasing in power output. This attack, performed once, would likely lead to safe shutdown assuming other safety systems are not compromised. However, an adversary could find this type of attack attractive if the goal is to degrade equipment or heat pipes over time by cycling the reactor power. Anomalous behavior such as power cycles would likely be detected and lead to scram, but this would result in a large monetary loss to the operator, especially if the cause of the cycle is unknown.

Design Basis 2.1: Motor speeds exceeding the motor's operational capacity are not considered. If the adversary can instantly move the CD into position and keep it there for a prolonged amount of time, they can control the reactor power level (note that this specific scenario is an extension of the original UCA of preventing CD rotation). It may not be feasible to implement Design Requirement 1.1 on the outward rotation of the motor depending on the required shutdown time for operators. One approach is for the inward and outward rotation of the CD to be driven by two separate motors with different maximum operating capacities, but this adds complexity to the CDS.

Design Constraint: No design constraint for this motor to protect against this compromise.

Design Requirement: Include a design requirement for separation of function in the CDS. One subsystem can control the outward-turning motor with an unconstrained maximum rotation speed, and the other controls the limited motor to slow down reactivity insertion.

Again, the design requirement resulting from this impact analysis does not prevent the potential for harm, it delays the system's response to the cyber compromise. Tier 2 analysis is still required for reactivity control via CDS.

5.2.3 Impact Scenario 3: CDS Feedback of Control Drum Position

Compromise: The adversary sends obfuscated CD position feedback to the controller to keep the CD stuck in its "turned in" position, inserting reactivity when the plant is at power. The ability to insert reactivity in this manner is dependent on the core neutronics at the time of the attack. Given this assumption, the power would continue to increase in the reactor. The assumed operation based on the system description is that the CD would remain in position and the ESS would eventually be forced to scram the reactor.

Unsafe action resulting from compromise: Based on the STPA UCAs, a failure of this kind would lead to the reactor exceeding power and inadvertent scram.

Design Basis 3.1: The adversary can only achieve this compromise if they are able to convince the process controller that the obfuscated position feedback is correct. Defense in depth should be applied here with sensor diversity and redundancy.

Design Requirement: The feedback signal for the CD position shall be collected from multiple polled sensors.

Again, the design requirement resulting from this impact analysis does not prevent the potential for harm - it delays the system's response to the cyber compromise. Tier 2 analysis is still required for reactivity control via CDS.

5.3 Case Study Tier 2 Analysis

The Tier 1 analysis provided a means by which physical design requirements could successfully impede an attack progression, but the design analysis did not eliminate the impact of an attack which targets the reactivity control functions. Therefore, those systems should be analyzed in a Tier 2 analysis to evaluate the access vectors available to an adversary for a given attack sequence.

5.3.1 Adversary Access Scenarios

This section provides two example adversary access scenarios for analysis. Each scenario begins with a postulated level of adversary access and explores how the adversary may cause a UCA.

Wireless Access: It is assumed that the adversary is located at the site but is outside the fence boundary. From the plant parking lot, the adversary can receive an uncontrolled wireless signal and exploit weak wireless policies to authenticate onto the network. The adversary uses software-defined radio to scan across common ICS frequencies (300 MHz to 6 GHz is frequently used in OT networks). Once activity is found, the adversary can use network sniffing [15] and wireless sniffing [16] tactics. These tactics are well known and will expose usernames and passwords from a sensitive wireless network. This allows the adversary access to network traffic as if they were physically located onsite. This gives the adversary access to the 10.1.1.* subnet and the ability to disrupt network traffic to and from the PCS PLC. Once they have access, they could then use a lateral tool transfer technique [17] to upload and move malicious tools in the sensitive OT network to cause damage.

Physical Site Access: It is assumed that the adversary can overcome physical security or access controls at the gate and has access to the site. It is assumed that the adversary's method to enter the site (e.g., stolen badge, social engineering, attacking an access control list to modify their own access) allows them to move throughout the buildings on site, including the control room. The adversary now has physical access to the SCRAM panel, HMI, historian, and reactor building. While Figure 8 shows that many of the OT and safety PLCs and components are contained inside the CCS, the adversary can access the external components and communication lines that penetrate the CCS. A motivated adversary would take advantage of the collocated PLCs to attempt multiple UCAs. This attack vector has one path that allows for digital network traffic access to both networks 10.1.1.* and 10.1.2.*. This access allows for the insertion of a malicious file or malicious software image to change I/O point values [18]. This technique was used by Industroyer [19] and one delivery option is with a programable USB device called a maker diary [20]. These values could improperly influence the reactivity controller input values possibly causing plant malfunction. A recommended mitigation for this would be to filter network traffic and I/O connections to allow only for in-band and/or allowed values, physical access controls, and input validation of PLC I/O values.

5.3.2 DCSA Design

Based on this access scenario analysis, the network architecture defined in Figure 7 is found to lack passive security against an advanced adversary whose goal is to exploit a UCA. This network can be improved by redesigning it with DCSA principles. To do this, the four attributes of DCSA (functions, systems, levels, and zones) need to be defined for the facility. This information is given in Table VI and is based on the extended analysis provided in [7]. Note that the DCSA attempts to capture the interdependencies between each critical system, but the level of detail is lower for those outside of the scope of the reactivity control function.

Security Level (SL) 1 contains safety systems and the backup system for functions needed to prevent the adversary's objectives. SL2 contains systems that are important to plant operation, and whose compromise can lead to an unsafe event. SL3 includes auxiliary systems whose compromise would either lead to financial loss or, in the case of the historian, breach of plant operating information. Compromise of SL3 functions do not put the plant in an unsafe state and would result in safe shutdown. SL is reserved for the enterprise network and ensuring that internet access is properly controlled. Note that both reactivity control and heat removal have supporting systems in two security levels. This is appropriate because the systems that support normal operations are required to communicate with other controllers, while the safety systems should be more isolated.

Table VI. DCSA LEVELS, ZONES, FUNCTIONS, AND SYSTEMS

SL	Functions	Security Zones
4	• Engineering and business support	• Internet • SZ4A: IT network and engineering workstations
3	• Power generation	• SZ3A: Turbine and generator • SZ3B: Historian
2	• Reactivity control (normal operations) • Heat removal (normal operations)	• SZ2A: CDS (turn in) and CDS (turn out) • SZ2B: CCS • SZ2C: PCS
1	• Emergency reactivity control • Decay heat removal • Containment	• SZ1A: ESS (rod 1) • SZ1B: ESS (rod 2) • SZ1C: SVS

The policies that apply for each level are summarized below:

SL1 Policies:

- SL1 has the highest level of physical security. Entry to this an area containing an SL1 zone should have strict physical barriers in place.
- Network communication between SL1 and a lower security zone is prohibited. Systems that are used for maintenance in SL1 are not permitted move between security levels (e.g., using the same maintenance laptop to run updates on SL1 and SL2 PLCs).
- Wireless communication prohibited in SL1.
- Routine monitoring for detection of rogue wireless access points is required.
- Staff access to an SL1 system should be highly-monitored and records should be audited regularly.

SL2 Policies:

- Physical access to devices in this region is strictly controlled and monitored.
- Only one-way network communication between SL1 and lower security zones is allowed.
- Wireless devices are allowed but must only be used for sensing and cannot have an impact on the control system. The wireless network must be separate from any process-critical control networks.

SL3 Policies:

- Physical access to devices in this region is controlled and monitored.
- Bidirectional communication between SL3 and lower-security zones is not prohibited for zones which contain digital I&C components.
- Wireless devices are allowed for non-I&C communication.

SL4 Policies:

- Internet connection is allowed and controlled.
- Wireless communication is allowed and controlled.
- Access control lists are reviewed periodically.

5.4 Case Study Tier 3 Analysis

The application of Denial of Task analysis is dependent on the device implementations in the microreactor facility and the adversary tasks that must be denied after Tier 2 analysis is complete. This tier of analysis can leverage existing threat attack frameworks such as MITRE ATT&CK for ICS [21], MITRE ATT&CK [22], and MITRE D3FEND [23]. The MITRE D3FEND matrix is a taxonomy of cybersecurity countermeasures grouped into tactics based on their purposes. Each countermeasure is connected to at least one technique in the MITRE ATT&CK matrix. For example, the Protocol Metadata Anomaly Detection countermeasure can be used to detect the adversary's Application Layer Protocol and User Execution techniques [24]. In consideration of the component-level assumptions that would be required for Tier 3 analysis, Tier 3 analysis will not be conducted in this paper.

6. CONCLUSION

The TCA provides an efficient graded approach for the design of digital I&C systems. As a performance-based approach, the TCA could be used to reduce the costs associated with implementing cybersecurity programs, while potentially improving the security posture of the facility. These benefits are of particular importance for advanced reactor applications. By first crediting SeBD features, then crediting passive cybersecurity measures provided by DCSA, the costs of active cybersecurity controls can be minimized. Further research on the alignment of the TCA with phases of design maturity will enable optimization of cybersecurity analysis as part of the AR design process.

ACKNOWLEDGEMENTS

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan.

REFERENCES

[1] U.S. Nuclear Regulatory Commission, "Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities," Rockville, MD, 2010.

[2] U.S. Nuclear Regulatory Commission, "DRAFT 10 CFR Part 73, Section 10: Technology Neutral Requirements for Protection of Digital Computer and Communication Systems and Networks," in *U.S. Code of Federal Regulations*, Rockville, MD, 2022.

[3] J. Jauntirans, I. Garcia and M. Rowland, "U.S.A. Regulatory Efforts for Cyber Security of Small Modular Reactors/Advanced Reactors," in *IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors*, Vienna, Austria, 2021.

[4] U.S. National Institute of Standards and Technology, "SP 800-37 Rev. 2: Risk Management Framework for Information System and Organizations," Gaithersburg, MD, 2018.

[5] International Atomic Energy Agency, "NSS 17-T: Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, Austria, 2021.

[6] U.S. National Institute of Standards and Technology, "SP800-39: Managing Information Security Risk," Gaithersburg, MD, 2011.

[7] J. James, J. Mohmand, L. Maccarone, D. R. Sandoval, A. Haddad, M. T. Rowland and A. J. Clark, "Consequence Modeling and Simulation of Hazardous Events for Advanced Reactors," Sandia National Laboratories, Albuquerque, NM, 2023.

[8] World Nuclear Association, "Design Maturity and Regulatory Expectations for Small Modular Reactors," London, UK, 2021.

[9] Westinghouse, "eVinci™ Micro Reactor," Westinghouse, [Online]. Available: https://www.westinghousenuclear.com/energy-systems/evinci-micro-reactor. [Accessed 1 September 2022].

[10] Idaho National Laboratory, "Licensing Modernization Project for Advanced Reactor Technologies: FY 2018 Project Status Report," Idaho Falls, ID, 2018.

[11] Southern Company, "Westinghous eVinci Micro-Reactor Licensing Modernization Project Demonstration," Atlanta, GA, 2018.

[12] International Atomic Energy Agency, "TECDOC-626: Safety-Related Terms for Advanced Nuclear Power Plants," Vienna, Austria, 1991.

[13] S. Mathezer, "Introduction to ICS Security Part 2," SANS, 16 July 2021. [Online]. Available: https://www.sans.org/blog/introduction-to-ics-security-part-2/. [Accessed 13 November 2022].

[14] N. G. Leveson and J. P. Thomas, "STPA Handbook," 2018.

[15] The MITRE Corporation, "Networking Sniffing," 20 September 2022. [Online]. Available: https://attack.mitre.org/techniques/T0842/. [Accessed 1 November 2022].

[16] The MITRE Corporation, "Wireless Sniffing," 27 September 2022. [Online]. Available: https://attack.mitre.org/techniques/T0887/. [Accessed 1 November 2022].

[17] The MITRE Corporation, "Lateral Tool Transfer," 27 September 2022. [Online]. Available: https://attack.mitre.org/techniques/T0867/. [Accessed 1 November 2022].

[18] The MITRE Corporation, "Brute Force I/O," 2022 September 2022. [Online]. Available: https://attack.mitre.org/techniques/T0806/. [Accessed 13 November 2022].

[19] The MITRE Corporation, "Industroyer," 20 October 2022. [Online]. Available: https://attack.mitre.org/software/S0604/. [Accessed 13 November 2022].

[20] makerdiary, "nRF52840 MDK USB Dongle w/ Case," 2022. [Online]. Available: https://makerdiary.com/collections/frontpage/products/nrf52840-mdk-usb-dongle-w-case. [Accessed 13 November 2022].

[21] The MITRE Corporation, "ICS Techniques," 2022. [Online]. Available: https://attack.mitre.org/techniques/ics/. [Accessed 1 November 2022].

[22] The MITRE Corporation, "Enterprise Techniques," 2022. [Online]. Available: https://attack.mitre.org/techniques/enterprise/. [Accessed 1 November 2022].

[23] The MITRE Corporation, "DEFEND," 2022. [Online]. Available: https://d3fend.mitre.org/. [Accessed 1 November 2022].

[24] The MITRE Corporation, "Protocol Metadata Anomaly Detection," 2022. [Online]. Available: https://d3fend.mitre.org/technique/d3f:ProtocolMetadataAnomalyDetection/. [Accessed 1 November 2022].

[25] International Atomic Energy Agency, "Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, Austria, 2021.