Advanced Reactor Safeguards & Security

Security-Inclusive Model-Based Systems Engineering: Demonstration using the MARVEL Reactor

Prepared for
US Department of Energy

Shannon Eggers, Kevin O'Rear,
Ross Hays, and Peter Suyderhoud

Idaho National Laboratory

September 2024
INL/RPT-24-80756

INL/RPT-24-80756

Security-Inclusive Model-Based Systems Engineering: Demonstration using the MARVEL Reactor

**Shannon Eggers, Kevin O'Rear,
Ross Hays, and Peter Suyderhoud**

Idaho National Laboratory

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

http://www.inl.gov

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

Page intentionally left blank

EXECUTIVE SUMMARY

Formal model-based systems engineering (MBSE) merges a model, systems thinking, and systems engineering to graphically represent the boundaries, context, and behavior of interconnected systems to enable successful design, development, and use of engineered systems throughout the project lifecycle. These tools, however, often are focused on functionality, performance, and safety and do not incorporate additional concerns introduced by use of operational technology. Nuclear reactor vendors are using MBSE to design and develop new advanced and small modular reactors, however they are not incorporating digital risk management and cybersecurity-by-design capabilities into their MBSE ecosystems. Therefore, the motivation for this multi-year research is to integrate digital risk management and cybersecurity into the early design stages of an MBSE project for a microreactor to demonstrate the benefits of considering security, safety, and performance requirements together. Specifically, this project is intended to answer the research questions, "can cybersecurity and digital risk management be integrated into a nuclear reactor vendor's MBSE process?" and "what are the impacts of integrating cybersecurity and digital risk management into this MBSE ecosystem in early systems engineering lifecycle phases?"

This research uses the requirements, design, and partially developed MBSE project developed for the Microreactor Applications Research Validation and EvaLuation (MARVEL) microreactor as a starting point. This real-world application provides a first-of-a-kind opportunity to demonstrate the benefits of integrating digital risk and cybersecurity into the MBSE design process of a nuclear reactor. During the first part of this research, the MARVEL MBSE project was updated to include (1) a larger set of requirements for the reactor design, (2) asset diagrams for each system and subsystem, and (3) connections between requirements and functions to their applicable asset. Additionally, visualization was provided to differentiate between analog and digital connections, digital specific requirements were identified for a generic reactor design, and a subset of these digital requirements were linked to networking components. Further, it was determined that the application's risk diagram was ineffective for the intended purpose; instead, an approach using function chains for misuse and unsafe control actions was developed.

Planned future work includes expanding the MARVEL MBSE model to include the full set of functions and requirements for the entire design, adding additional action diagrams, improving visualization of digital pathways, identifying options for redesigning the defensive architecture, and identifying how digital risk requirements can be traced and verified in MBSE throughout the systems engineering lifecycle. Additionally, further work will be undertaken to evaluate improved methods for integrating digital risk management into the MBSE ecosystem, with a focus on how it can be used to evaluate the impacts of risk treatments (e.g., redesign, simplification, mitigation) on digital risk.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

ARCADE	Advanced Reactor Cyber Analysis and Development Environment
CAD	computer-aided design
CD	control drum
CIA	central insurance absorber
CS	control system
DCSA	defensive computer security architecture
DFS	drum forcing subsystem
DOE	U.S. Department of Energy
ECS	engine cooling subsystem
EPS	electrical production subsystem
FCS	fuel and core system
HARDENS	High Assurance Rigorous Digital Engineering for Nuclear Safety
HMI	human-machine interface
I&C	instrumentation and control
ICS	instrument and control system
INL	Idaho National Laboratory
MARVEL	Microreactor Applications Research Validation and EvaLuation
MBSE	model-based systems engineering
MRS	MARVEL reactor structure
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OOSEM	object-oriented systems engineering method
P&ID	piping and instrumentation diagram
PCS	primary coolant subsystem
PGS	power generation system
PRA	probabilistic risk analysis
R&D	research and development
RCS	reactivity control system
RIM	reliability and integrity management
RIS	reactor instrumentation subsystem
RPS	reactor protection system
SCGS	secondary gas coolant subsystem
SCS	secondary coolant subsystem

STPA	systems theoretic process analysis
SysML	Systems Modeling Language
TPN	TREAT private network
TREAT	Transient Reactor Test Facility
T-REXC	TREAT microreactor experiment cell
UCA	unsafe control action
UML	Unified Modeling Language
VFD	variable frequency drive
V&V	verification and validation

Page intentionally left blank

Security-Inclusive Model-Based Systems Engineering: Demonstration using the MARVEL Reactor

1. INTRODUCTION

With the existing U.S. nuclear fleet, cybersecurity controls became "bolt-on" Nuclear Regulatory Commission (NRC) requirements due to regulatory changes resulting from the terrorist attacks on September 11, 2001. While this approach was necessary to secure existing nuclear power plants (NPPs) from cyber-attacks, a different approach is warranted with the development of new reactors, regardless of whether they are generation III+ reactors, advanced reactors, small modular reactors, or microreactors. The goal of Cyber-Informed Engineering and cybersecurity-by-design frameworks is to "build in" security starting at the earliest stages in the systems engineering lifecycle. Cybersecurity-by-design practices, such as simplifying designs, establishing defensive architectures, hardening instrumentation and control (I&C) systems, and including security controls and detection capabilities in the design, are techniques that can reduce overall digital risk prior to installation and implementation. For the purposes of this paper, digital risk is defined as risk against digital technology due to adversarial threats from a bad actor and non-adversarial threats such as human performance errors, equipment failures or degradation, and environmental conditions.

One concern with the design and construction of new reactors is that design teams will not address (or will not know how to address) cybersecurity and digital risk early enough in the systems engineering lifecycle. Another concern is that large, multi-teamed design projects will not bring in cybersecurity and digital risk as a separate discipline, which can lead to conflicts with requirements, potentially leading to functional, safety, reliability, or security issues. For example, if cybersecurity engineers have a requirement to install a data diode between two network zones that only allows one-way communication from one zone to another, but I&C engineers require two-way communication flow for operational functionality or safety, there is a conflict or gap that must be addressed. Model-based systems engineering (MBSE) helps identify these gaps between competing stakeholder requirements and competing objectives by providing a single source of truth [1], thereby enabling the project team to recognize, evaluate, and adjudicate the discrepancy. Organizations that use MBSE, however, are often focused on functionality, performance, and safety; they do not incorporate additional risk concerns introduced by use of digital I&C.

The use of MBSE has been evaluated in the nuclear industry. For instance, the NRC supported the High Assurance Rigorous Digital Engineering for Nuclear Safety (HARDENS) project by Galois to demonstrate the use of rigorous digital engineering for a reactor trip system [2]. The HARDENS project used model-based engineering to specify, examine, validate, and verify the system from requirements to design to manufacturing [2]. While this was a first-of-a-kind demonstration project for nuclear engineering, it was focused primarily on ensuring the ability to design and manufacture a safety system to NRC requirements. Another project, sponsored by the U.S. Department of Energy (DOE) Regulatory Development Program for Advanced Reactors, evaluated the use of MBSE for reliability and integrity management (RIM) [3]. Similar to the HARDENS project, this study focused on using MBSE to establish a RIM process for use on a generalized model of a reactor cavity cooling system and did not include security requirements [3].

At the beginning of this research, a questionnaire was sent to industry partners to gauge the use of MBSE for cybersecurity in new reactor projects. Results of this study, as described in Appendix A, identified that a gap exists in using MBSE's capability to evaluate digital risk and implement appropriate risk treatments. Therefore, the motivation for this multi-year research study is to integrate digital risk management and cybersecurity into an MBSE ecosystem for early systems engineering lifecycle stages of a microreactor project to demonstrate the evaluation and decision process necessary when considering security, safety, and performance requirements together. Specifically, this research study is intended to

answer the research questions, “can cybersecurity and digital risk management be integrated into a nuclear reactor project’s MBSE process?” and “what are the impacts of integrating cybersecurity and digital risk management into this MBSE ecosystem in early systems engineering lifecycle phases?”

The requirements, design, and partially completed MBSE project developed for the Microreactor Applications Research Validation and EvaLuation (MARVEL) microreactor is used as the starting point for this research. This real-world application provides a first-of-a-kind opportunity to demonstrate the benefits of integrating digital risk and cybersecurity into the design process of a nuclear reactor.

The remainder of this paper describes the first part of this research project. Section 2 provides a brief background on MBSE and an overview of the MARVEL microreactor. The methodology for this initial work is outlined in Section 3 with results provided in Section 4. Section 5 provides a discussion before conclusions and future work are addressed in Sections 6 and 7.

2. BACKGROUND

2.1. Model-Based Systems Engineering

MBSE is a formalized use of models as the central tool for designing and implementing complex systems throughout the systems engineering lifecycle, from conceptual design to decommissioning or disposal [1]. Rather than using documents in the systems engineering process, MBSE merges a model, systems thinking, and systems engineering to graphically represent the boundaries, context, and behavior of interconnected systems to enable successful design, development, and use of engineered systems throughout the lifecycle. The model represents the entire system or system of systems to provide a visual representation of requirements, structure, behavior, and more. As shown in Figure 1, using a digital thread as the single source of truth [1], the larger digital engineering ecosystem can integrate risk analysis, simulation and analysis techniques (e.g., multi-physics, computational fluid dynamics, finite element analysis, digital twins), computer-aided design (CAD), piping and instrumentation drawings (P&ID), tradeoff analyses, performance testing, verification and validation (V&V), configuration management and version control, requirements management, and project management capabilities.

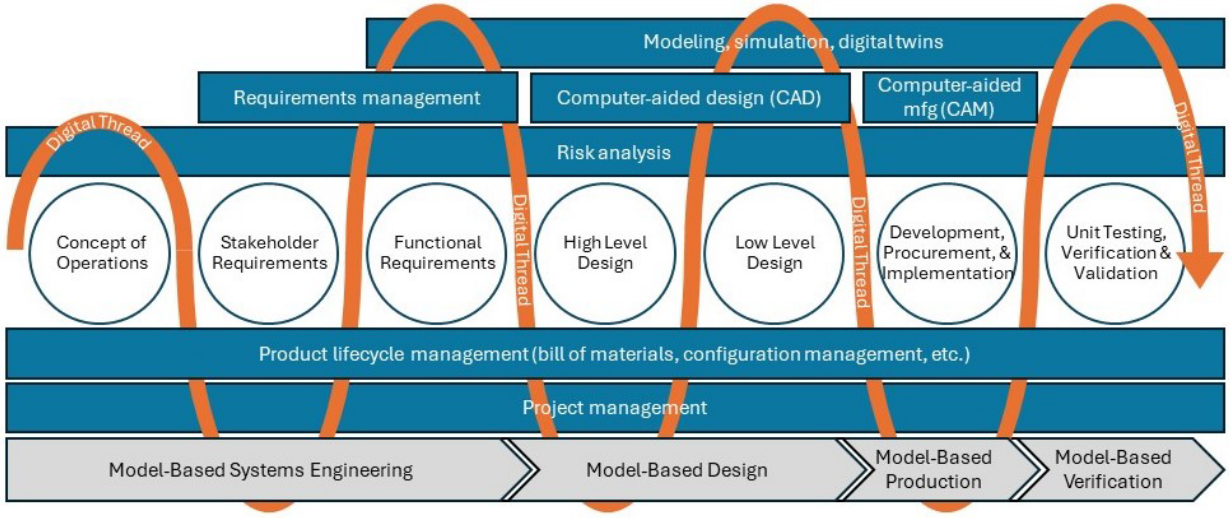

Figure 1. Example digital engineering ecosystem.

MBSE provides a common language for communication between all stakeholders in the lifecycle; all disciplines involved in the project can view the complex relationships in a system to better make informed decisions. This traceable, single source of truth provides a holistic view of individual components, along with their interactions and dependencies, enabling better communication of complex ideas across diverse

teams and disciplines. Additionally, this convergence of information from multiple domains and subsystems can prevent costly rework by facilitating identification of inconsistencies and defects during the modeling process so that they can be more quickly addressed or eliminated early in the lifecycle [4]. MBSE can similarly improve engineering efficiency and improve project performance [4].

There are three primary elements in MBSE: modeling language, methodology, and framework. The most common languages include Systems Modeling Language (SysML) and Unified Modeling Language (UML); the most common tool-neutral methodology is object-oriented systems engineering method (OOSEM); and there are numerous commercial and open-source frameworks that integrate the language and methodology.

2.2. MARVEL Microreactor

The MARVEL microreactor is designed as a nuclear applications test bed to provide researchers with the capabilities of combined heat and power for evaluating end-user technologies [5]. It is also designed to provide a platform for testing advanced control systems, such as autonomous control, remote operation, and digital twins [5]. The MARVEL systems and interfaces are illustrated in Figure 2. The primary purpose of the fuel and core system (FCS) is to create and sustain nuclear fission chain reaction, transfer heat to fuel cladding, and support decay heat removal. The primary purpose of the MARVEL reactor structure (MRS) is to remove heat from the core, transfer heat to end user systems, and transfer decay heat to the ultimate heat sink [6].

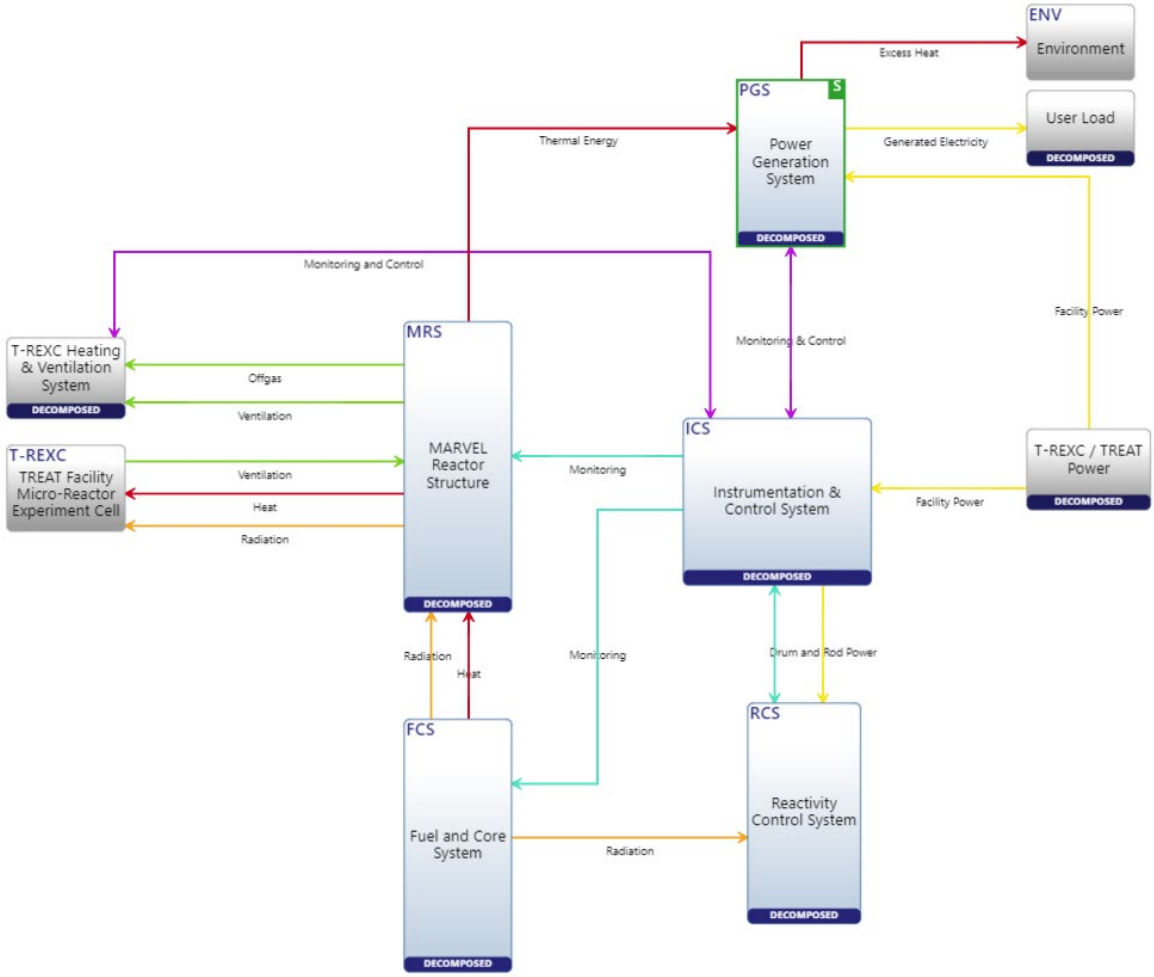

Figure 2. MARVEL systems and interfaces.

The power generation system (PGS) contains two subsystems, the engine cooling subsystem (ECS) and the electrical production subsystem (EPS). The EPS contains Stirling engines that absorb high-grade heat from the MRS secondary coolant subsystem (SCS) which absorbs heat from the MRS primary coolant subsystem (PCS) [5]. AC power from the Stirling engines is delivered to the engine controllers which also receive engine position and frequency data for monitoring and control [5].

The reactivity control system (RCS) provides reactivity control during normal operation and controlled shutdown as well as reactor trip upon signal from the reactor protection subsystem (RPS) in response to abnormal or postulated design basis accidents [5]. The RCS consists of four rotatable control drums that are evenly distributed about the core periphery and one translatable central insurance absorber (CIA) rod in the center of the core [5]. The drum forcing subsystem (DFS) receives a position request from the instrument and control system (ICS) control system (CS) to move a control drum (CD) and/or the CIA rod. Additionally, upon a trip signal from the RPS, the CD clutch and CIA electromagnet are deenergized to rotate the CDs to their shutdown position and drop the CIA rod to its shutdown position [5].

As shown in Figure 3, the ICS contains the CS, reactor instrumentation subsystem (RIS), RPS, and human machine interface (HMI). RIS measures critical operating parameters which are then sent to the CS. The RPS initiates a reactor shutdown upon signals from seismic sensors, manual trip button, loss of power, or shutdown from the RCS [5]. The CS also receives information from multiple subsystems for monitoring and control functions. CS data is sent to the HMI for operator monitoring. Operators can also interface with the HMI to send control requests to the CS [5]. The interlocks ensure that only one CD or the CIA rod are moved at a time.

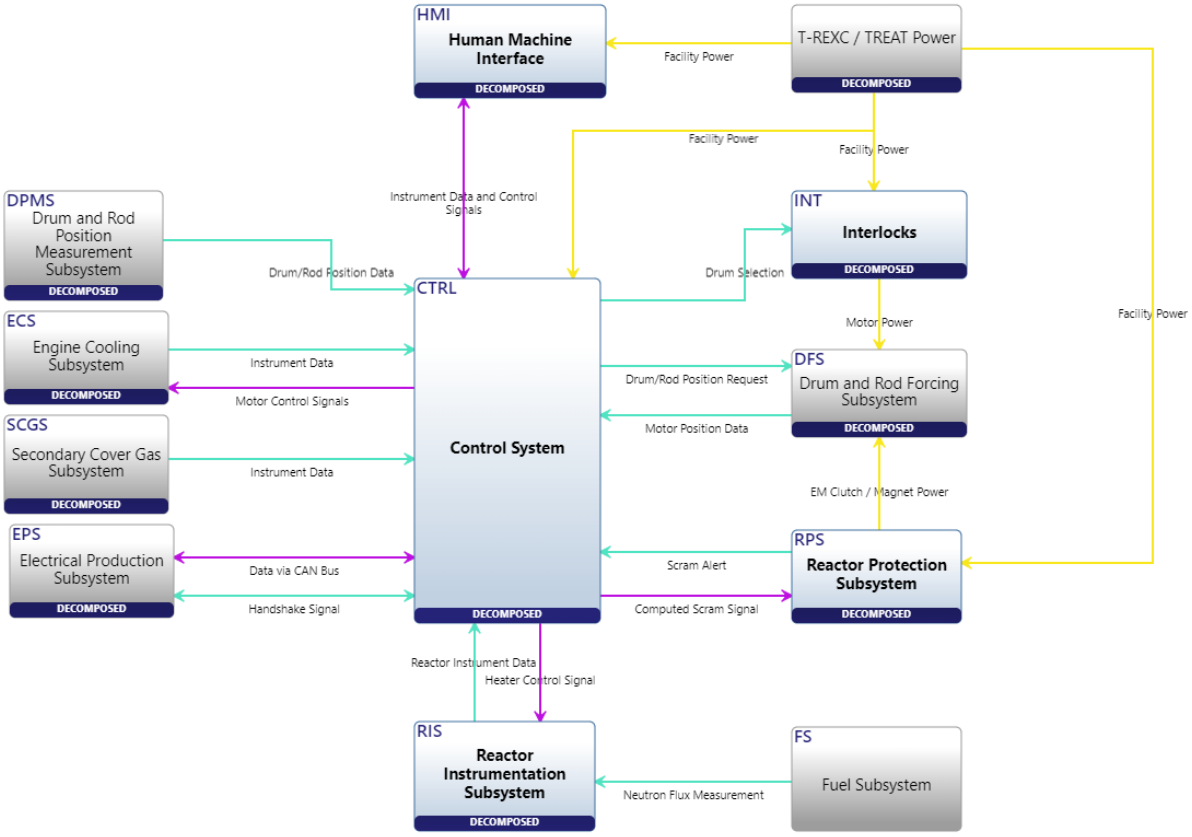

Figure 3. MARVEL ICS architecture and interfaces.

The TREAT microreactor eXperiment Cell (T-REXC) ventilation system provides the ventilation for temperature control, contamination removal, and exhaust gas removal for MARVEL. The ventilation systems consist of two separately controlled systems: a filtered upper confinement system and an unfiltered main system. These two systems provide ventilation of the T-REXC and are located in the TREAT north high bay. The ventilation systems are modulated via variable frequency drives (VFDs) controlled and monitored by the MARVEL HMI [5].

2.3. Innoslate MBSE solution

Innoslate is an MBSE solution by Spec Innovations that is SysML compliant and includes requirements management, test and evaluation, modeling and simulation, and risk management. Innoslate is a typical MBSE platform that provides traceability and gap analysis and maintains the authoritative single source of truth with integration between diagrams, documents, and reports. Figure 4 demonstrates a generic Innoslate process for MARVEL. After requirements are added, assets (e.g., systems, subsystems, and components) are identified which perform an action to satisfy the requirement.

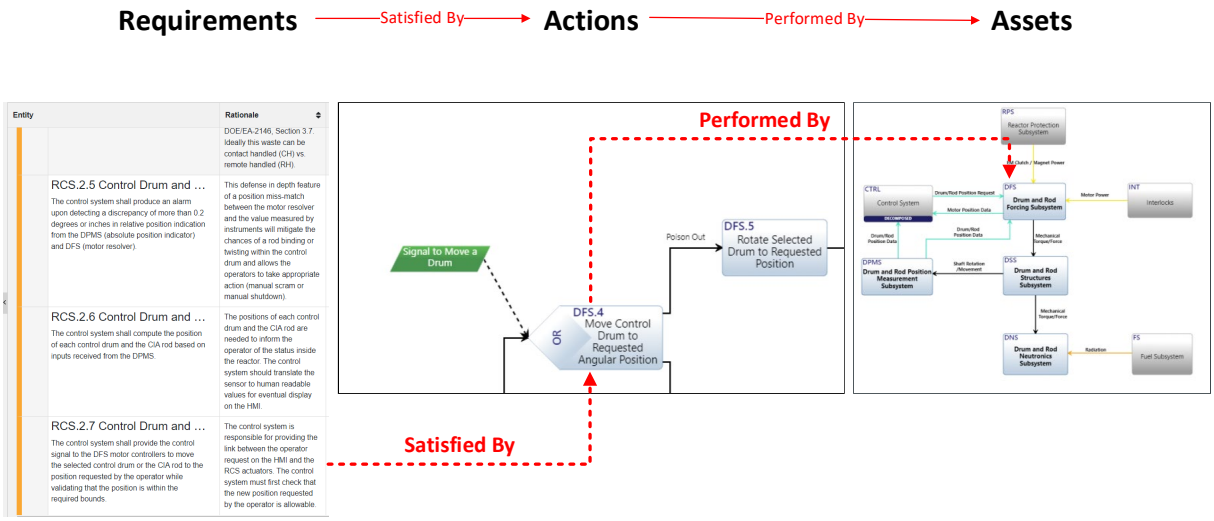

Figure 4. Generic MBSE process for MARVEL.

3. METHODOLOGY

3.1. MARVEL Innoslate Project Update

The MARVEL engineering team initially developed an MBSE project using Innoslate for the microreactor project, however the engineering team migrated away from using MBSE and focused specifically on maintaining a requirements database. For this research, a separate project instance was copied from the original Innoslate project into a new project. To update the MARVEL Cyber MBSE project, the following steps were performed:

1. Imported all current MARVEL requirements and functions into the project instance.
2. Added asset subcomponents for the ICS, RCS, PGS, and FCS to the architecture diagrams.
3. Developed system models for supporting systems that could potentially be cyber-critical (e.g., HVAC).
4. Assigned requirements and functions to components where applicable.
5. Identified analog and digital connections along with their signal type.
6. Added networking components to the diagrams.

3.2. Incorporation of Digital and Cybersecurity Requirements

The following steps were performed to add digital and cybersecurity requirements into the MARVEL MBSE Cyber project:

1. Developed a set of requirements from NRC 10 C.F.R. § 73.54 [7] as level 4 non-functional requirements and added the requirements as a new requirements document in Innoslate.
2. Developed a set of requirements derived from NRC Regulatory Guide 5.71 revision 1 [8], preliminary NRC draft regulatory guidance DG-5075 [9]. NEI 08-09 revision 7 [10], NEI 13-10 revision 7 [11], and nuclear I&C system design best practices as level 3 functional and level 4 non-functional requirements. Added these requirements as a new requirements document in Innoslate.
3. Added traceability of the requirements to digital assets in the network architecture.
4. Identified revision opportunities to further improve security of the network architecture.

3.3. Incorporation of Digital Risk Management

The following steps were taken to evaluate the use of digital risk tools in the MBSE ecosystem:

1. Identified risk analysis methods for evaluation.
2. Identified techniques for incorporating the methods into Innoslate.
3. Evaluated the capabilities, including challenges and gaps, of using MBSE to include digital risk management.

4. RESULTS

4.1. MARVEL Innoslate Project Update

4.1.1. Requirement and function import

Requirements and system functions for MARVEL were developed in IBM's DOORS Next software as part of the MARVEL design. The artifacts from this database were exported from DOORS for use within the MARVEL Innoslate project. Innoslate allows bulk import of artifacts from various file types, including .CSV files. The export from DOORS was cleaned up to remove superfluous information and then imported using Innoslate's Import Analyzer tool. Importing the information allowed the artifacts from DOORS to be mapped to Innoslate's schema and for relationships between requirements and functions to be maintained for traceability. An example of these relationships is shown below in Figure 5.

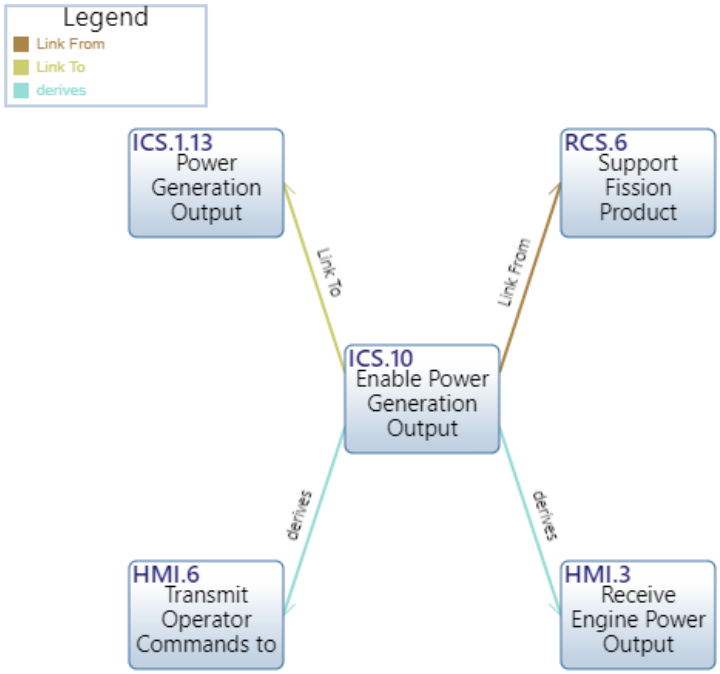

Figure 5. Relationships imported from the DOORS Next application.

Once in Innoslate, the requirements were placed within documents sorted by system for ease of access and viewing. While not necessary for linking and using requirements, the document view provides a more concise way to ensure traceability of requirements. Requirement documents were generated for the ICS, RCS, and PGS systems. Figure 6 shows a portion of the ICS requirements document from Innoslate.

Entity	Rationale
ICS.1 Level 2 Requirements	N/A
ICS.1.1 Instrumentation and Control Maintenance and Replacement Accessible ICS system equipment shall include provisions for maintenance and removal/replacement while minimizing radiation dose to personnel to the extent practical (ALARA).	If I&C equipment fails it should be able to be replaced and returned to service while ensuring worker doses are ALARA. This does not include instruments installed inside the reactor.

Figure 6. An example of a requirements document in Innoslate.

The functions (called actions in Innoslate) were placed in system action diagrams. These action diagrams were based on the functional architecture of the systems taken from DOORS and the MARVEL design [5]. Functional diagrams were created for RPS, DPMS, CS, RIS, PGS, HMI, RCS, and ICS. Figure 7 shows the functional diagram for the RPS.

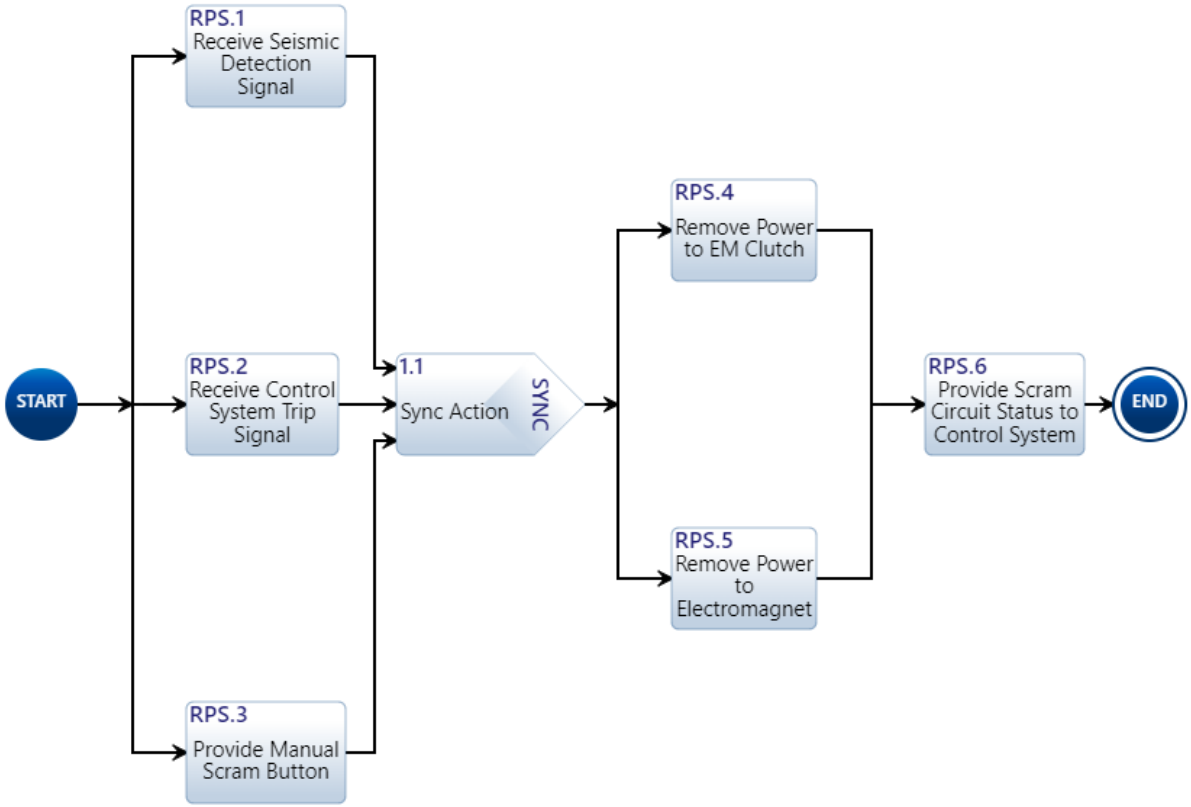

Figure 7. An example of a system functional diagram.

4.1.2. Asset diagrams (I&C systems)

MARVEL system drawings were used to populate architecture diagrams called asset diagrams. The approved drawings and component identifiers were used to create the Innoslate diagrams, when available, to mirror the MARVEL design. Systems in which the assets were populated focused on I&C systems and interfaces. More systems were created in Innoslate as asset diagrams than had corresponding requirement documents or action diagrams. This is due to the number of external interfaces between relevant I&C systems/components and the number of potential systems impacting digital assets. Asset diagrams focus on the physical or cyber-physical connections between components. They show interfaces, called conduits, between assets to denote relationships. While asset diagrams provide the interfaces between components, they do not provide the logic for system operation.

The populated systems include RCS, EPS, ECS, DPMS, SCGS, RIS, CTRL, HMI, DFS, RPS, T-REXC Ventilation, PCS, SCS, and Reactor Interlocks. Innoslate asset diagrams consist of components marked as internal to the currently opened diagram and components marked external. The external components are shaded in gray as shown in the figures below. These components are typically marked external when they are part of another system, such as the control system or instrumentation system. This allows for the connection of one system diagram to another. Figure 8 is an example of a full system asset diagram (ECS), while Figure 9 shows a magnified portion of the system for readability.

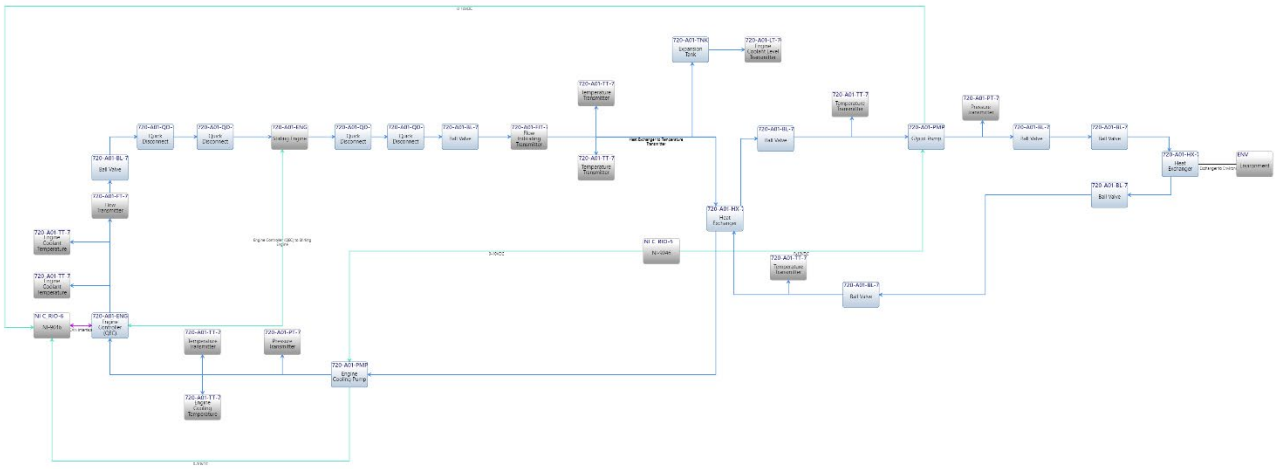

Figure 8. An example illustrating the breadth of the full ECS asset diagram.

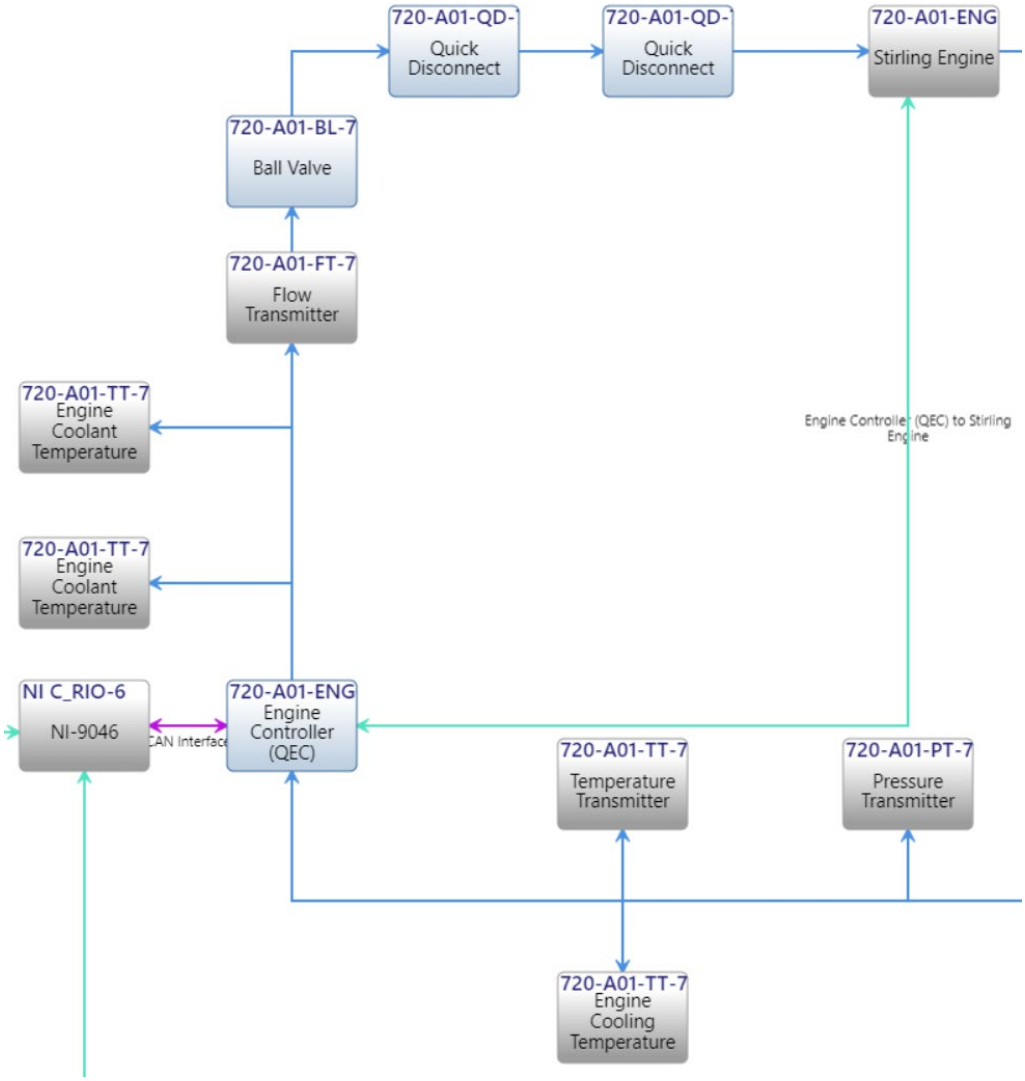

Figure 9. Magnified view of the ECS asset model.

4.1.3. System models for supporting systems

Supporting systems that interface with or could potentially impact the function of digital assets in the MARVEL design were also modeled. These systems, such as the T-REXC ventilation system or Secondary Cover Gas Subsystem, were modeled to provide potentially cyber critical components that do not otherwise perform a critical function. Similarly to the modeled I&C systems, these system models were developed utilizing the MARVEL design documentation [5]. Figure 10 shows the system diagram for the T-REXC ventilation.

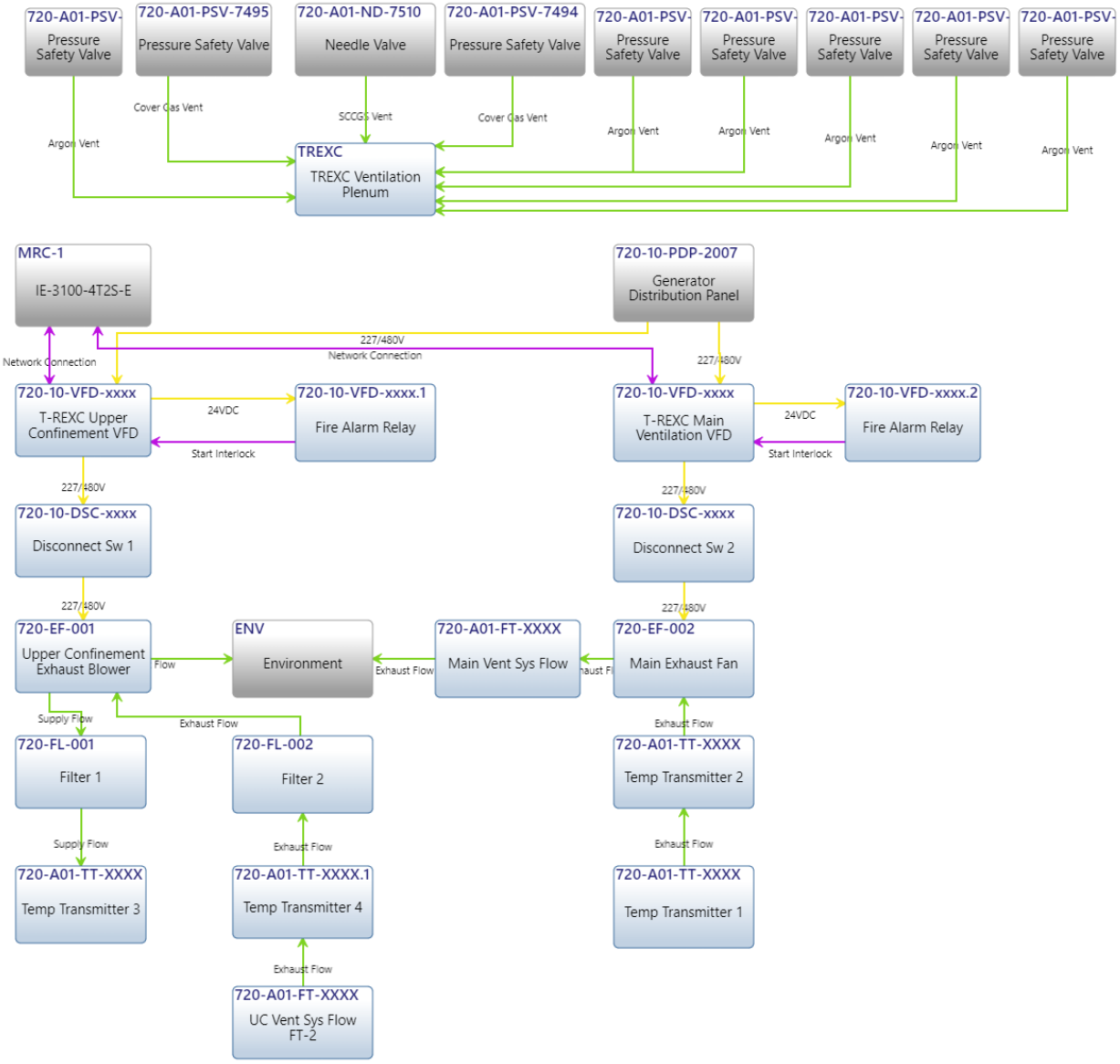

Figure 10. T-REXC ventilation system model.

4.1.4. Requirement and function assignment

Functions from system functional diagrams were associated with their performing assets. Functional assignment helped to identify the desired operation of each asset, their intended states, and their importance to the overall MARVEL design. Assignment of functions allows for an understanding of not

only the desired operation of the system but also the potential impacts and risks associated with control equipment capabilities.

Additionally, requirements for the PGS were assigned to assets in various systems. Portions of the ECS, EPS, and CS received these PGS requirements. Requirement assignment to assets allows for the validation and verification of the MARVEL design. This assignment is also used in the digital context to apply digital-specific requirements to assets within Innoslate. Requirements specific to digital components and systems are further discussed in Section 4.2.

Figure 11 shows an example requirement and function assignment for a temperature transmitter in the ECS. The left menu shows connections with other assets and diagrams as well as the assigned actions (functions) and requirements.

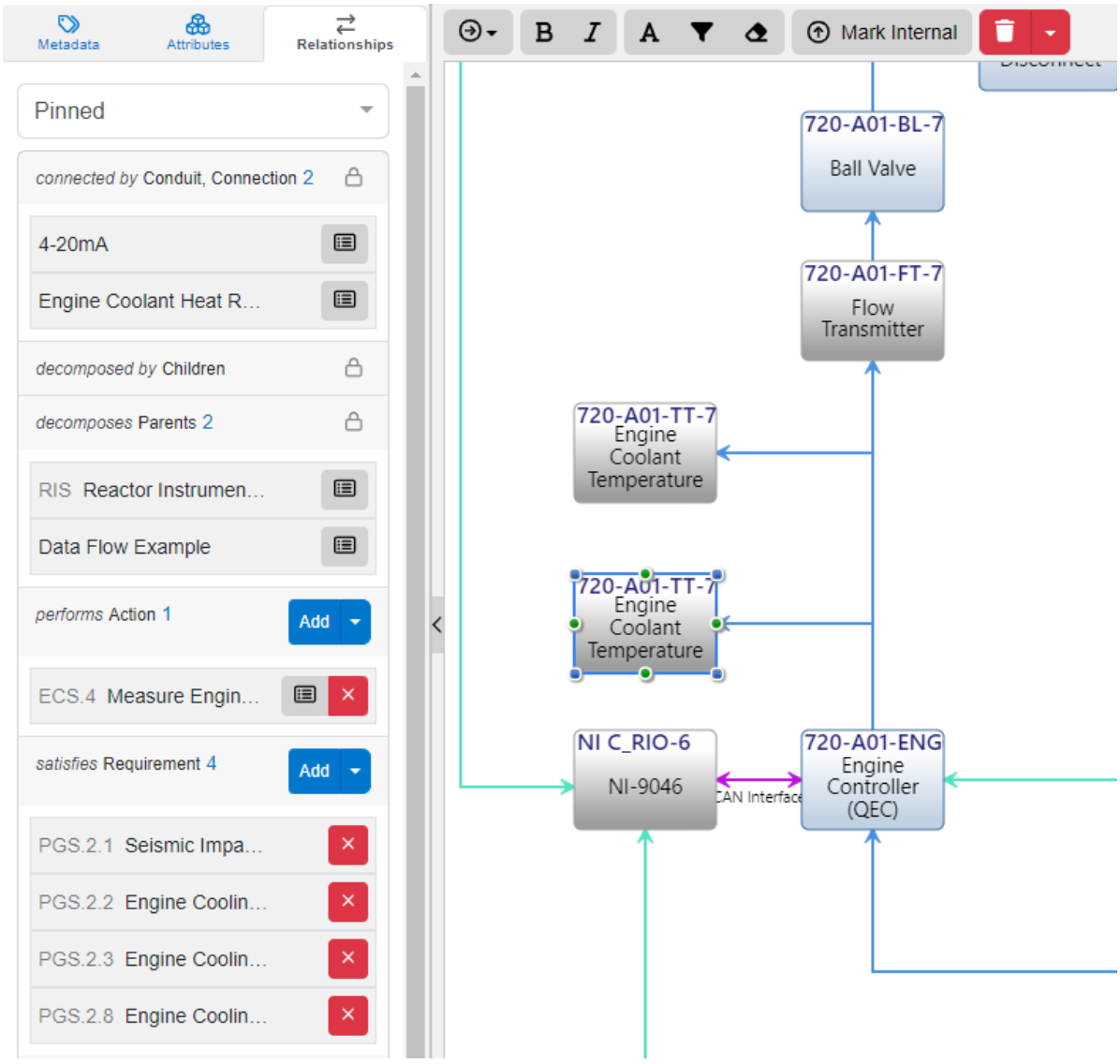

Figure 11. Assigning functions and requirements to assets.

4.1.5. Analog and digital signals

Components in asset diagrams were connected to one another as identified in the MARVEL drawings. I&C components were connected to one another based upon the system single line and wiring

diagrams. An identification of the type of signal being sent/received was included for the purposes of assessing cybersecurity and digital risk. Additionally, a color scheme for the diagrams was developed that identifies analog (turquoise) and digital (purple) signals in the Innoslate diagrams. Electrical connections, physical connections, and flow paths for piping, gas removal, or heat removal were also color coded and included. Digital communications were separated from analog for components when both signal types existed between the same two end points (i.e., digital and analog signal lines were shown when both were present). Figure 12 shows an example of analog and electrical connections between components in the control system.

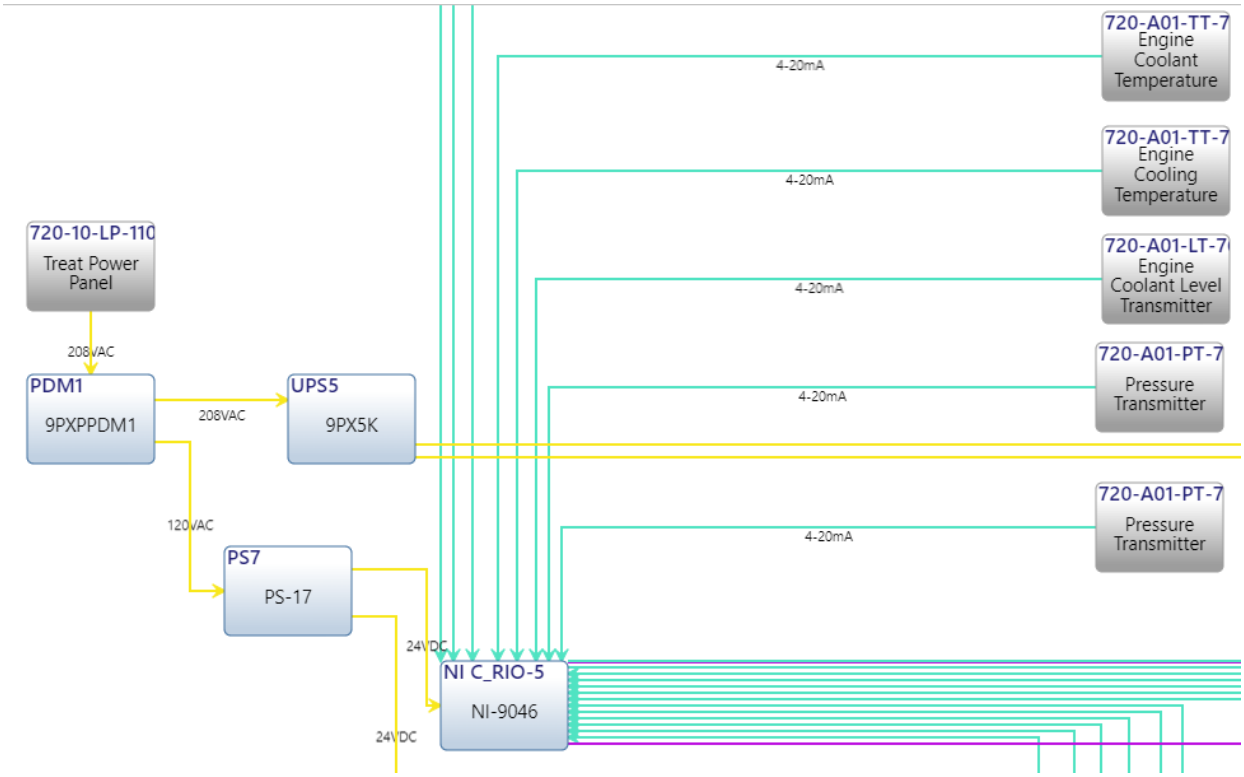

Figure 12. Identification of analog and electrical connections.

Identification of digital connections were included for any digital data sent between MARVEL devices and shown in purple. Figure 13 shows an example of digital connections.

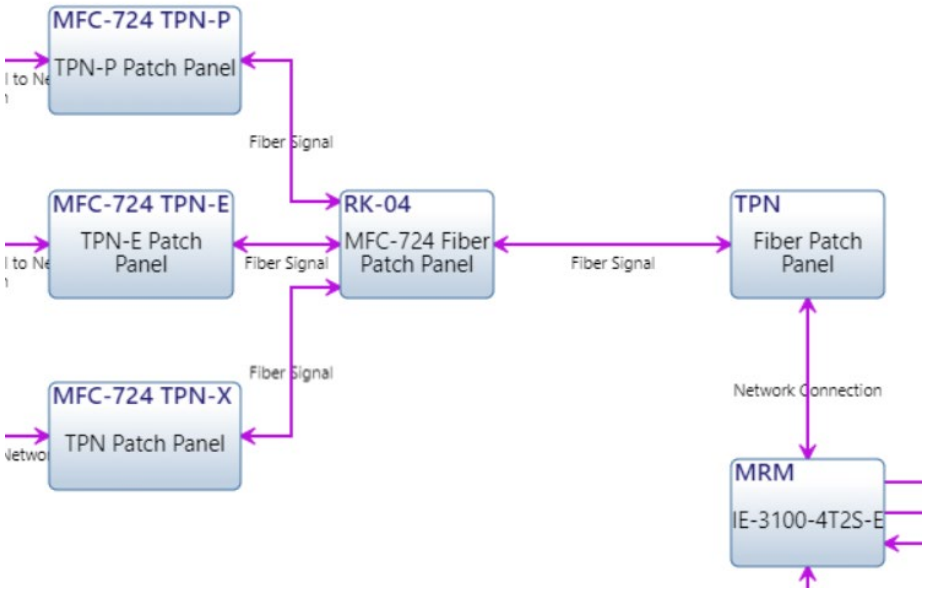

Figure 13. Identification of digital signals.

4.1.6. Network architecture

System network pathways from the instrumentation and instrument modules were identified using MARVEL network and I&C drawings. These connections represented the flow path from the field device, such as temperature transmitters and controllers, to the control room device. The MARVEL control system information did not include separate layers for network traffic. The MARVEL control system interfaces with the TREAT Private Network (TPN). Connections from the local equipment in TREAT to the control room in MFC-724 were included via network switches and fiber connections. These connections provided the traceability of field devices to HMI assets in the control room through links in Innoslate.

Innoslate provides the ability to visualize relationships between assets included in the diagram currently viewed and one level of external connections to identify cross-system relationships as previously discussed. However, the limitation of a single level of external connections means that an Innoslate user must view the relationships via the database or by stepping through each diagram individually. An example diagram that includes all components in the data flow from HMI to engine controller and engine was created to provide an example of the full network connections. The figure below shows an example of the connectivity inherent to the Innoslate architecture created for this effort. Some connections are hidden for clarity.

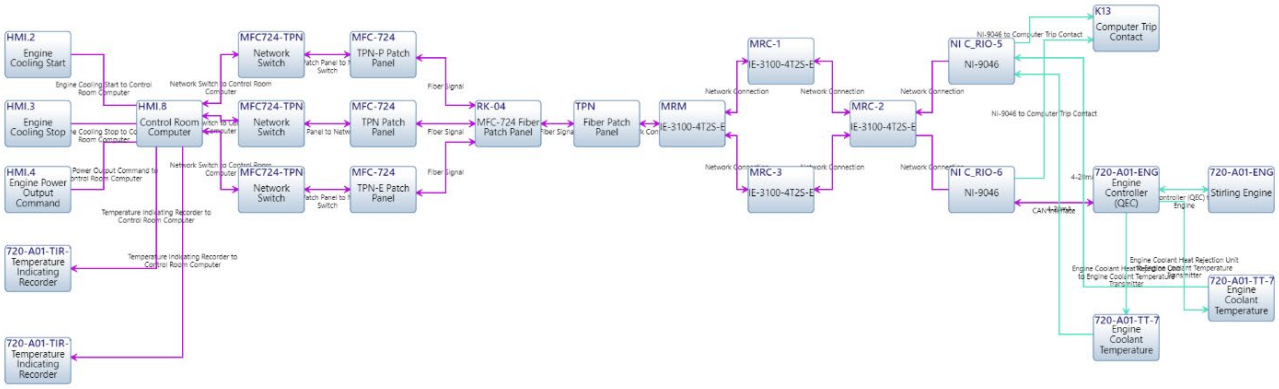

Figure 14. Example of a network architecture.

4.2. Incorporation of Digital and Cybersecurity Requirements

A set of level 3 functional and level 4 non-functional digital requirements were developed as listed in Appendix B. These requirements were included in Innoslate as the "Digital Specific Requirements" document. Level 3 requirements include those for defensive architecture as well as those that may be required for all digital assets (e.g., account management, authentication, physical protection, monitoring). Additionally, a set of level 3 requirements were included at the system level for the PGS. Level 4 non-functional requirements include those for digital risk analysis, design simplicity and system hardening, configuration management, and procurement and product development. An additional requirements document was added for the non-functional requirements outlined in NRC 10CFR73.54. The new preliminary draft guidance for advanced reactors, DG-5075, was reviewed; however no specific cybersecurity requirements were derived from this document.

To initially demonstrate the use of level 3 requirements for the network architecture, the requirements in Table 1 were added to the three network switches in Figure 14 (e.g., MFC724-TPN-P-1, MFC724-TPN-X-1, MFC724-TPN-E-1).

Table 1. Digital requirements added to network switches.

Rqmt #	Description
3.1.9	Unused ports on network switches shall be disabled.
3.1.20	Port blockers shall be used on unused ports on network devices.
3.1.21	Network switch logs should be forwarded to a centralized logging server.
3.1.22	Passive scanning devices should be used to monitor patch levels, installed software, and software versions; and identify rogue devices.
3.1.28	All network switches and routers shall have visual status indications of activity and performance.
3.1.29	Standard grade network devices shall have expected environmental ranges that are suitable for that environment.
3.1.34	The Cisco Discovery Protocol (CDP) shall be turned off on all Cisco switches by placing the "no cdp run" command in each switch configuration.
3.2.1	Default passwords shall not be used on digital assets.
3.2.2	Service accounts shall not be used to access digital assets.
3.2.3	Shared accounts for limited administrative access if there is a valid business need and access activity is logged.
3.2.4	Complex passwords with minimum length of 10 should be used on digital assets, where possible (complex = two of uppercase, lowercase, number, or special character).

Rqmt #	Description
3.2.5	Security rights and roles for digital assets shall be established based on least privilege, where possible.
3.2.6	Accounts should be configured to automatically lock out when 5 (or fewer) failed attempts are logged within 1 hour.
3.2.7	Failed login attempts should be logged, where possible.
3.2.8	Automatic unlocking of account is allowed after 15 minutes if failed login attempt is logged, where possible.
3.2.9	A session lock should be initiated after 30 minutes of inactivity, where possible.
3.2.10	A manual session lock shall be allowed by user, where possible.
3.3.1	Network authentication shall be used, where possible.
3.5.2	Digital assets shall be monitored for anomalous events (e.g., system, event, application logs).
3.7.4	Digital assets shall maintain time synchronization using a trusted time server, as applicable.

4.3. Incorporation of Digital Risk Management

4.3.1. Innoslate risk diagram

Innoslate includes a risk diagram as option. However, the included risk matrix is a heat map to visualize severity of consequence versus likelihood and is generally used in Innoslate for project risk management. While the typical definition of digital risk is the likelihood of a threat exploiting a vulnerability to cause an adverse consequence, determining the likelihood of occurrence is actually very difficult, if not impossible, to evaluate. Since the risk matrix in this application has limited capability to appropriately analysis digital risk, this diagram option was rejected.

4.3.2. Functional chain for misuse and unsafe control actions

Adapting from Navas et al. [12], Table 2 provides a crosswalk of terms from systems engineering to digital risk. The goal is to use identify misuse cases, or unsafe control actions, and impacted functions using the model.

Table 2. Crosswalk between systems engineering and digital risk.

Systems Engineering	Digital Risk / Cybersecurity
Operational entity/actor	Threat source (adversarial & non-adversarial)
Capability/misuse case	Unsafe control action (STPA)
Function	Critical function
Physical component, link	Digital asset
Physical component, link	Supporting asset
Function	Security control/measure

As described in Navas et al., a functional chain is “the specific arrangement of functions and exchanges, forming a path between all possible paths through system data flows, either to describe an expected behavior of the system in a given context, or to express non-functional properties on this path (e.g. latency, criticality, confidentiality, redundancy...)” [12]. Figure 15 illustrates an example of the functional chain for a misuse case in which an adversary uses another user’s logon for a meteorological example in [12].

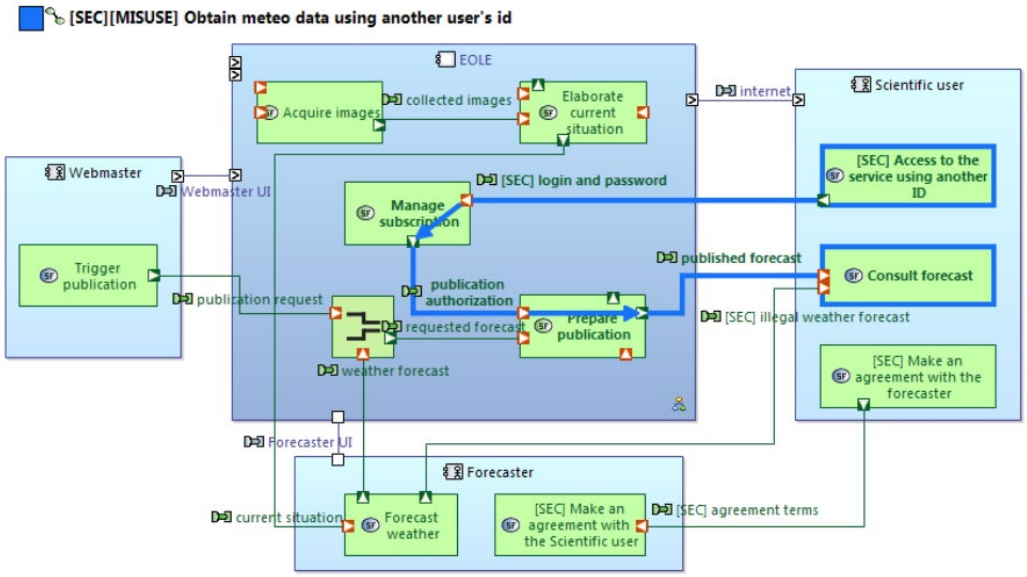

Figure 15. A functional chain (bold blue functional exchanges) describing a misuse case and impacted system functions for the meteorological application considered in [12].

Instead of using misuse cases as described by Navas et al. [12], unsafe control actions were identified for the PGS. Unsafe control actions (UCA) in Systems Theoretic Process Analysis (STPA) are grouped into four categories: (1) required commands are not given, (2) unanticipated commands are given, (3) the timing of commands is incorrect (e.g., too early or too late), and (4) the duration of control actions is incorrect (e.g., too short or too long) [13]. In the PGS, adverse consequences of interest include engine damage, equipment damage, and reactor trip. A critical function is engine control. A preliminary control structure for engine control is shown in Figure 16. Using this control structure, a preliminary listing of threats, or UCAs, that can impact the engine function are listed in Table 3. QEC is the engine control unit.

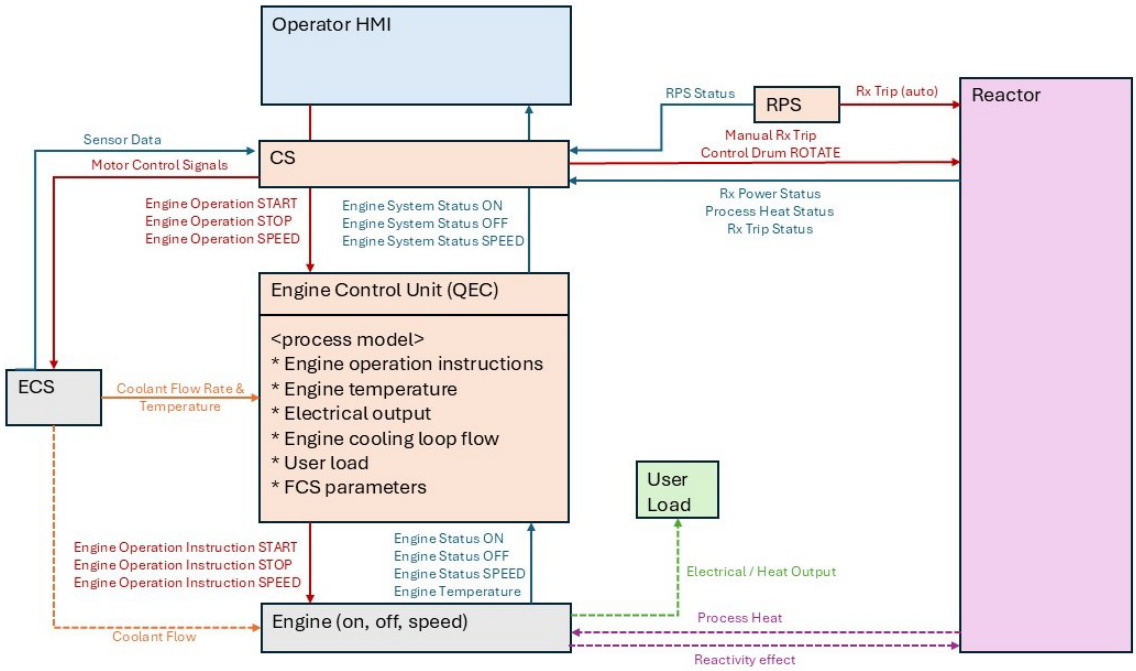

Figure 16. Engine control structure.

Table 3. Preliminary list of threats, or UCAs, for the engine control function.

Threat ID (UCA)	Controlling Action	Pathway	Not Provided (N)	Provided When Shouldn't (P)	Timing (T)			Duration (D)
					Too Early	Too Late	Order	
1	Engine STOP	HMI / QEC to engine	UCA1-N-1: STOP command not given when coolant flow lowers to less than 20 Lpm (when engine not automatically tripped with reactor trip). Hazard: Engine runs without proper coolant flow. Impact: Engine damage	UCA1-P-1: STOP command given when reactor at power. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip.	UCA1-T-1: STOP command given before reactor lowers to specified power level. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip.	UCA-T-2: STOP command given too late after coolant flow lowers below 20 Lpm. Hazard: Engine runs without proper coolant flow. Impact: Engine damage	NA	NA
2	Engine START	HMI / QEC to engine	UCA2-N-1: START command not given when reactor at power. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip.	UCA2-P-1: START command given when coolant flow is less than 20 Lpm Hazard: Engine runs without proper coolant flow. Impact: Engine damage	UCA2-T-1: START command given prior to coolant flow reaching 20 Lpm. Hazard: Engine runs without proper coolant flow. Impact: Engine damage	UCA2-T-2: START command given too late after reactor at power. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip.	NA	NA
3	Engine STOP	Coolant flow & temp sensor to QEC	UCA3-N-1: STOP command not given when coolant flow is less than 20 Lpm. Hazard: Engine runs without proper coolant flow. Impact: Engine damage UCA3-N-2: STOP command not given when coolant temperature is too high. Hazard: Engine runs with coolant too hot. Impact: Engine damage	UCA3-P-1: STOP command given when coolant flow is not less than 20 Lpm. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading reactor trip. UCA3-P-2: STOP command given when coolant temperature is not too high. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading reactor trip.	UCA3-T-1: STOP command before coolant flow lowers to less than 20 Lpm Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip. UCA3-T-2: STOP command before temperature is too high. Hazard: Thermal energy not removed from reactor. Impact: Reactivity increase leading to manual or automatic reactor trip.	UCA3-T-3: STOP command not given when coolant flow is less than 20 Lpm. Hazard: Engine runs without proper coolant flow. UCA3-T-4: STOP command not given when coolant temperature is too high. Hazard: Engine runs with coolant too hot. Impact: Engine damage	NA	NA

The next step in this risk analysis process is to identify scenarios that could lead to these UCAs. As identified in Table 4 for Threat #1, these scenarios may be grouped into several categories. Since the purpose of this project is to integrate risk analysis and risk treatments into MBSE, future work will identify if and how the control structure and scenario analysis can be incorporated into the MARVEL Innoslate project using functional chains.

Table 4. Potential scenarios for threat 1, grouped by category.

Threat ID	Category	Scenario
1	Controller Behavior	Design flaw in QEC (inadequate algorithm) Incorrect modification of QEC Incorrect configuration of QEC Degradation/failure of QEC
	Feedback	Control feedback is incorrect or inadequate Control feedback is missing/unavailable (not sent, not received) Control feedback is delayed Communication with <controller> is incorrect Communication with <controller is missing/unavailable Communication is delayed Inadequate operation of sensor Inaccurate sensor measurement Sensor feedback delayed
	Control pathway	Control action not executed Control action improperly executed Control action delayed
	Controlled process	Component failure Conflicting control actions Out-of-range disturbance Missing process input Incorrect process input

5. DISCUSSION

The adoption of a security inclusive MBSE approach to nuclear digital engineering projects will provide a formal methodology to support the integrated requirements, design, analysis, verification, and validation necessary to integrate safety, security, and resilience from intentional and unintentional digital incidents into the overall functional design. The collaboration with the MARVEL microreactor project has enabled development of an MBSE platform that includes requirements, asset diagrams, and requirements traceability. Updating the MARVEL MBSE model to include the existing system-level requirements, new digital requirements, asset diagrams, and network architecture has provided a persistent, knowledge repository to enhance team communication and enable more effective decision making for digital risk. Setting digital and analog connections to different colors provides immediate visual identification of which connections and components could be impacted by a cyber incident.

The initial asset models were assigned at system and subsystem levels with connections between the process equipment; the network components and connections for digital assets was omitted. Adding these network components and completing the flow path from the field device to the HMI provided a more accurate defensive architecture for digital risk analysis. Further, Innoslate only provides a single level of external connection. As shown in Figure 14, however, these flow paths can be created. Ideally, these digital flow paths can be rapidly viewed (without need for additional diagram creation) to facilitate the

analysis of threat pathways, UCAs, vulnerabilities, and potential for maloperation. Internal block diagram or block definition diagrams in Innoslate or another open source MBSE application may enable this capability.

The set of digital requirements was generically developed for a reactor using existing guidance and prior experience. It was identified that many requirements do not necessarily map to an individual digital asset, so further investigation is necessary to determine how best to incorporate these requirements into the model to ensure they are met (and can be verified and validated in later phases). For instance, requirements related to the defensive architecture design was not readily mapped to a component. However, establishing a separate system for the defensive architecture may allow for this correlation. From a network component viewpoint, initial mapping was performed for requirements specific to network switches. Future work will expand this mapping to understand any gaps or limitations.

It was identified that Innoslate's native risk matrix diagram was unsuitable for use with digital risk. Using prior work from [12] and the concept of UCAs to establish scenarios, the goal is to use the MBSE platform to establish scenarios and functional chains that can lead to maloperation. The early identification of these functional chains can be used to eliminate or mitigate the risks. As the MARVEL network does not include levels, zones, or boundary devices, this toolset should help identify updates to the defensive architecture as suggested for a commercial microreactor as well as trace these requirements throughout the systems engineering lifecycle.

6. FUTURE WORK

6.1. Expansion of Model

This project is in the beginning of a multi-year research study with continued collaboration with the MARVEL program [14]. Longer-term work will focus on expanding the digital requirements for the full reactor design, integrating additional digital twin(s), integrating the model with external entities in an integrated energy system (refer to TREX-C connection in Figure 2, and migrating the project to an open-source platform so that any insights on model development can be more readily shared with industry and interested parties.

6.1.1. Update functions and requirements for other systems

Requirement and function attribution for MARVEL systems was primarily focused on the PGS and its subsystems. Continued development of the MBSE models of MARVEL would include similar development of other systems. The requirements and functions for the ICS and RCS are currently included in the Innoslate project database. These artifacts should be assigned to associated components.

6.1.2. Action diagrams/adversary tactics and I/O of control systems

System physical architecture diagrams have been developed in the form of asset diagrams showing the components and their direct interactions. While this allows for an identification of the interfaces between components it does not fully specify the logic in system operation and interaction, especially among digital components and network interactions. Development of more detailed diagrams such as internal block diagram or block definition diagrams would allow for the identification of process variables, signal operators, setpoint values, and resulting outputs. Requirements could then be verified or validated using these detailed parameters. Additionally, this could be beneficial for the identification of vulnerabilities and emulation of common adversary tactics against the MARVEL systems.

6.1.3. Defensive architecture development

MARVEL design drawings do not identify separation of network levels. Best practices include separation of networks into levels and zones based upon the function and safety significance of the system. Identification of the network level to which each signal in the MARVEL Innoslate diagrams belongs will provide a visual indication of potential conflicts between networked components. In

conjunction with the development of detailed process or logic diagrams, identification of network levels could provide insight into vulnerabilities and level nexus points that do not meet the requirements for the defensive architecture and digital assets.

6.2. Requirements Traceability

Developing digital requirements and linking them to digital assets is an important first step in early systems engineering lifecycle phases. Future work will continue adding requirements to digital assets in the remainder of the systems and evaluate how these requirements are traced throughout the lifecycle, including development of verification and validation plans to ensure that the digital assets meet the requirements.

6.3. Risk Analysis Methods

6.3.1. Functional chain and UCA analysis

Future work will continue to evaluate the capabilities for integrating the functional chain and UCA risk analysis methodology into MBSE.

6.3.2. Other digital risk analysis methodologies

Digital risk analysis includes analysis of threats, vulnerabilities, and consequences. Instead of considering likelihood of successful impact, research is underway in the ARSS program to consider difficulty of a successful adverse impact occurring. Figure 17 illustrates an entity-relationship diagram for digital risk in which it is possible to identify how protections, engineering design, detection & response, and asset condition impacts overall relative digital risk for a function or system by making a successful impact more difficult to occur (adapted from NSS 42-G [15]). Additionally, Figure 18 illustrates a tiered cybersecurity approach adapted from Maccarone et al. [16] and NIST SP800-37 [17] where PRA is probabilistic risk analysis and DCSA is defensive computer security architecture. Future work will evaluate how these "attack difficulty" factors and tiered approach can be modeled in the MARVEL MBSE project to derive a repeatable risk analysis methodology in MBSE.

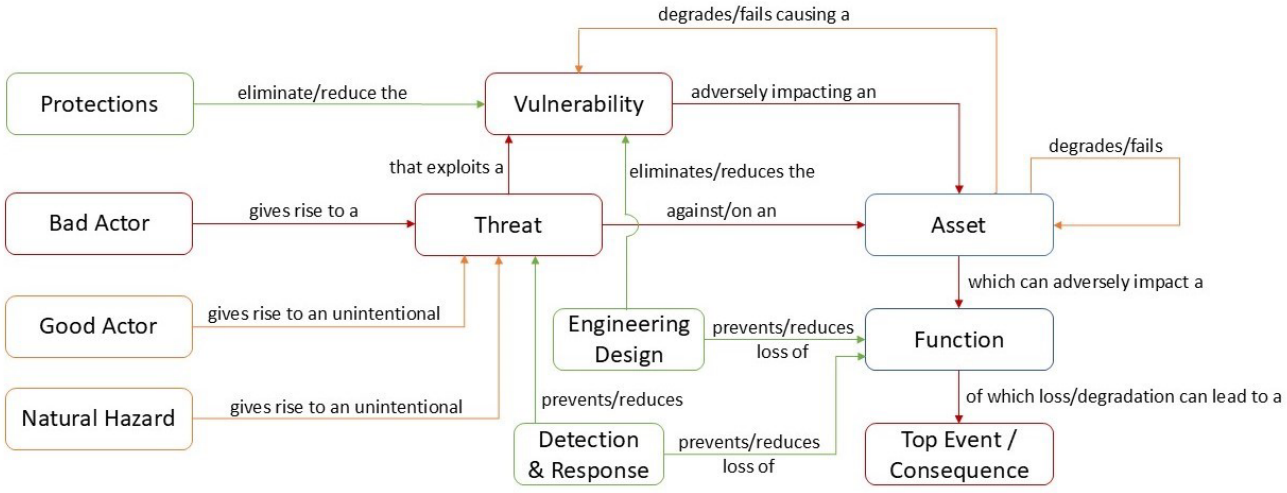

Figure 17. Entity-relationship diagram for digital risk (adapted from [15]).

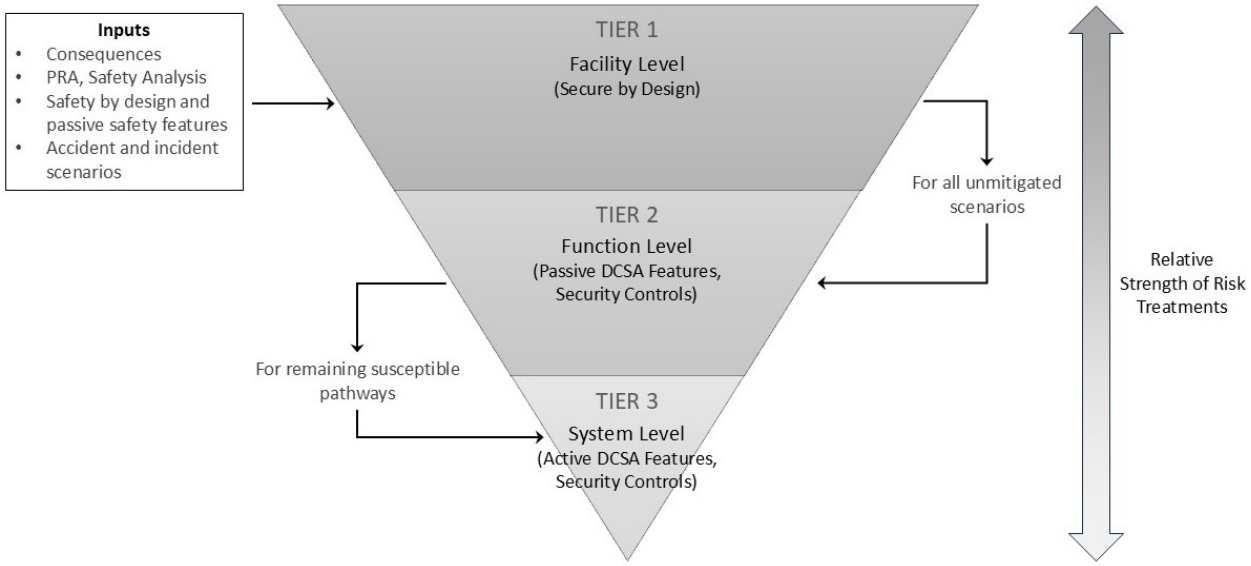

Figure 18. Tiered cybersecurity approach (adapted from [16] and [17]).

One toolset that will be investigated for integration into the MARVEL MBSE project is the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) developed in the ARSS program. ARCADE enables analysis of digital risk through capabilities such as, control system sensitivity analysis, cyber-attack scenario simulation and consequence analysis, investigation of adversary pathways, and comparison of different defensive architectures [18]. The ability to integrate the primary MBSE platform with other simulation tools or digital twins enables multi-disciplinary decision making. For instance, the capability to run a simulation on a given design in the MBSE ecosystem (e.g., I&C defensive architecture) and then re-run the simulation on a different design can provide the project team with insights on how a specific functional requirement may interfere with a security requirement. Additionally, this performance-based simulation capability can be coupled with evaluating how UCAs impact the safety or operation of the system. Future work includes development and testing of pathways and scenarios to evaluate observable impacts, first through use of a digital twin and then through automatic ingestion of network designs and UCAs.

7. CONCLUSIONS

While "all models are wrong but some are useful [19]," the goal of this multi-year research project is to continuing updating the MARVEL MBSE ecosystem to provide a real-world case study for demonstrating the proof-of-concept for integration of digital risk and cybersecurity into the design process for a nuclear reactor. Progress during the first part of this project includes the update of the MARVEL Innoslate project, development and incorporation of digital requirements, and evaluation of different risk analysis integration methods. Work is continuing in FY-25 and will initially focus on expanding the integration of digital risk into the project, establishing the process for visualizing digital pathways, developing maloperation scenarios, and identifying how the risk treatments can be verified and validated by the MBSE ecosystem.

8. REFERENCES

[1] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 5.0*. Hoboken, NJ, USA: John Wiley and Sons, Inc., 2023.

[2] Kiniry, J., A. Bakst, S. Hansen, M. Podhradsky, and A. Bivin, "The HARDENS final report," Galois, 2023, Available: https://github.com/GaloisInc/HARDENS/blob/develop/docs/HARDENS_Final_Report_Jan_2023.pdf.
[3] Mandelli, D. *et al.*, "Investigation and demonstration of reliability target allocation to support Reliability and Integrity Management program," Idaho National Laboratory, 2023, Available: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67610.pdf.
[4] Carroll, E.R. and R.J. Malins, "Systematic literature review: How is model-based systems engineering justified?," Sandia National Laboratories, 2016, Available: https://www.osti.gov/biblio/1561164.
[5] Gerstner, D. and Y. Arafat, "MARVEL 90% final design report," Idaho National Laboratory, 2023, Available: https://www.osti.gov/servlets/purl/2208844.
[6] INL, "MARVEL Functional and Operational Requirements," Idaho National Laboratory, 2023.
[7] *10 C.F.R. § 73.54, Protection of Digital Computer and Communication Systems and Networks*, 2009.
[8] NRC, "Regulatory Guide 5.71 revision 1, Cyber security programs for nuclear facilities," U.S. Nuclear Regulatory Commission, 2023.
[9] NRC, "Draft Regulatory Guide DG-5075," U.S. Nuclear Regulatory Commission, 2023.
[10] NEI, "NRC ML24061A057, Endorsement of NEI 08-09 Revision 7, Cyber security plan for nuclear power reactors," Nuclear Energy Institute, 2024.
[11] NEI, "NEI 13-10 Revision 7, Cyber security control assessments," Nuclear Energy Institute, Washington D.C., 2021.
[12] Navas, J., J.-L. Voirin, S. Paul, and S. Bonnet, "Towards a Model-Based approach to Systems and Cyber Security co-engineering," in *INCOSE International Symposium*, 2019, vol. 29, no. 1, pp. 850-865: Wiley Online Library.
[13] Leveson, N.G. and J.P. Thomas, "STPA Handbook," Massachusetts Institute of Technology, 2018.
[14] Abou-Jaoude, A. and M.W. Patterson, "MARVEL utilization plan," Idaho National Laboratory, 2024, Available: https://www.osti.gov/biblio/2371820.
[15] IAEA, "NSS 42-G, Computer security for nuclear security," International Atomic Energy Agency, Vienna, 2021, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.
[16] Maccarone, L.T., A.S. Hahn, and M.T. Rowland, "System-level design analysis for advanced reactor cybersecurity," Sandia National Laboratories, 2023, Available: https://energy.sandia.gov/wp-content/uploads/2024/01/Maccarone_DCSA-FY23-M2.pdf.
[17] Force, J.T., "NIST SP 800-37. Revision 2. Risk Management Framework for Information Systems and Organizations," *NIST Special Publication,* 2018.
[18] Hahn, A.S., L.T. Maccarone, and M. Rowland, "Simulation based analytical approaches to cyber risk mitigation in advanced nuclear reactors," in *Transactions of the American Nuclear Society*, Las Vegas, NV, 2024: American Nuclear Society.
[19] Box, G.E., "Robustness in the Strategy of Scientific Model Building," in *Robustness in Statistics*: Elsevier, 1979, pp. 201-236.
[20] Roudier, Y. and L. Apvrille, "SysML-Sec: A model driven approach for designing safe and secure systems," in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, 2015, pp. 655-664: IEEE.
[21] Jürjens, J., "UMLsec: Extending UML for secure systems development," in *International Conference on The Unified Modeling Language*, 2002, pp. 412-425: Springer.
[22] de Souza, F.G.R., J. de Melo Bezerra, C.M. Hirata, P. de Saqui-Sannes, and L. Apvrille, "Combining STPA with SysML modeling," in *2020 IEEE International Systems Conference (SysCon)*, 2020, pp. 1-8: IEEE.

Page intentionally left blank

Appendix A

Industry Questionnaire

Appendix A
Industry Questionnaire

A-1. MBSE Landscape Review Methodology

To understand the capabilities of integrating digital risk and cybersecurity into MBSE solutions, we performed a review of twenty commercial and open-source MBSE products. Additionally, to understand the existing use of MBSE within the nuclear industry we sent an informal survey to nine advanced and small modular reactor vendors to learn about their use of MBSE in nuclear engineering projects. The survey included the following questions:

4. Does your organization use an MBSE solution? If so, which one?
5. Does your organization integrate the MBSE solution with other applications (e.g., modeling and simulation engines, digital twins, requirements management, testing, configuration management, etc.)? If so, which one(s)?
6. Does your organization incorporate the entire design into one instance of the MBSE tool or are multiple project instances (not considering iterations) used?
7. How are stakeholder and/or design requirements inputted into the organization's MBSE tool?
8. What disciplines are captured in your organization's MBSE solution (e.g., electrical engineering, mechanical engineering, nuclear engineering, I&C engineering, safety, risk management, regulatory compliance, physical security, cybersecurity)?
9. If risk management is included in the MBSE solution, what classes of risks are considered (e.g., radiological safety, work safety, environmental safety, theft of special nuclear material, physical security, cybersecurity)? If risk management or risk analysis is included, how is it integrated?
10. How does your organization evaluate adversarial cybersecurity risk? Is cybersecurity risk incorporated into the MBSE solution (and, if so, how)?
11. How does your organization evaluate non-adversarial digital risk (e.g., human performance errors, equipment degradation/failure, environmental impacts, etc.)? Is non-adversarial digital risk incorporated in the MBSE solution (and, if so, how)?
12. If your organization evaluates both adversarial and non-adversarial digital risk, are these risks considered simultaneously with other disciplines (question 5) during the design process? If so, how?
13. Is your organization's MBSE solution capable of integrating both adversarial and non-adversarial digital risk considerations within the systems engineering design process?

A-2. MBSE Landscape Review Results

A-2.1 MBSE platform review

We found that there generally are no barriers to adding digital risk and cybersecurity requirements into overall model requirements. While no modeling languages included holistic digital risk (i.e., adversarial and non-adversarial risk), the SysML-Sec modeling language is specifically intended to provide a model-driven approach to promote collaboration between system designers and cybersecurity experts during early systems engineering phases [20]. Similarly, there is a UML-Sec modeling language [21], and System-Theoretic Process Analysis (STPA) can be combined with SysML [22]. There is also a

Risk Analysis and Assessment Modeling Language that can be used in the MBSE ecosystem to conduct safety and quality engineering risk analysis activities.

A-2.2 Reactor vendor survey and gap analysis

Out of the five responses, three vendors indicated they used MBSE, and two vendors indicated it was too early in the project lifecycle to establish a systems engineering approach. Of the three responders who used MBSE, each used a different MBSE framework and incorporated different disciplines into the approach (i.e., nuclear engineering, I&C, safety, compliance, etc.). Additional findings, depending on the vendor, include:

- The primary focus of MBSE was integration of safety, functionality, and performance. Digital I&C risk and/or security was not included. However, there was interest in learning how to integrate cybersecurity into MBSE.
- The primary MBSE project is for a generic site. Separate instances will be updated specifically for each facility.
- Automatic and manual requirements generation are used.
- Several other tools were integrated into the MBSE platform (e.g., simulators, product lifecycle management, requirements management, computational fluid dynamics, one-dimensional analysis, structural analysis).
- Risk management was performed outside of MBSE. Non-adversarial risk evaluation tools used outside of MBSE included probabilistic risk analysis, SPAR-H (Standardized Plant Analysis Risk-Human Reliability Analysis), STPA, and failure mode and effects analysis.

Appendix B

Digital Specific Requirements

Appendix B

Digital Specific Requirements

Number	Name	Description	Rationale
3	Level 3 Functional Requirements		
3.1	Defensive Architecture		
3.1.1		The network shall be segregated into zones and levels commensurate with the function and safety significance of the systems.	
3.1.2		Reactor systems supporting critical functions (e.g., safety systems, control systems) shall be in network level 4.	
3.1.3		Reactor or plant systems supporting non-critical functions shall be in network level 3.	
3.1.4		Business systems shall be placed in network level 2.	
3.1.5		Each system should be placed in one zone where possible. A zone may include more than one system.	
3.1.6		Only one-way data flow from Level 4 to Level 3 shall be allowed.	
3.1.7		A data diode that is physically only capable of sending data in one direction shall be placed between level 4 and level 3.	
3.1.8		Only one-way data flow from Level 3 to Level 2 shall be allowed.	
3.1.9		A data diode that is physically only capable of sending data in one direction shall be placed between level 3 and level 2.	
3.1.10		Data traffic passing through a data diode shall pass through an intrusion detection system on the input or output.	
3.1.11		A boundary device (e.g., data diode, firewall, packet filtering) shall be placed between zones.	
3.1.12		Firewalls credited as boundary devices shall perform stateful inspection.	
3.1.13		Firewalls shall be configured for deny all by default and shall end with a deny all rule	
3.1.14		Firewall rules shall be specific allowing specific source and destination addresses/ranges or specific functions.	
3.1.15		Firewalls shall be managed through a direct connection to the firewall from a management device that is controlled as a PMMD (portable media or maintenance device).	
3.1.16		Direct communication to the firewall shall not be allowed from any of the managed interfaces.	
3.1.17		Firewall logs should be forwarded to a centralized logging server.	
3.1.18		IDS/IPS logs should be forwarded to a centralized logging server.	
3.1.19		Unused ports on network switches shall be disabled.	
3.1.20		Port blockers shall be used on unused ports on network devices.	
3.1.21		Network switch logs should be forwarded to a centralized logging server.	
3.1.22		Passive scanning devices should be used to monitor patch levels, installed software, and software versions; and identify rogue devices.	

Number	Name	Description	Rationale
3.1.23		A centralized logging server shall be used to capture continuous network, system, and asset data.	
3.1.24		Wireless access shall not be allowed on level 3 or 4.	
3.1.25		Remote access shall not be allowed on level 3 or 4.	
3.1.26		The ethernet network shall support IEEE 802.3 compliant devices.	
3.1.27		The network should support standard Ethernet communications including CAN, UDP, TCP/IP, MODBUS/RTU, and OPC, as needed.	
3.1.28		All network switches and routers shall have visual status indications of activity and performance.	
3.1.29		Standard grade network devices shall have expected environmental ranges that are suitable for that environment	
3.1.30		Network switches that have fiber optic ports shall use 62.5/125 micron multi-mode fiber optic cable not to exceed 2000 meters (6560 feet).	[IEEE 802.3u]
3.1.31		Cat5e or higher cable shall be used for 100 Megabit links.	Refer to cable standard ANSI TIA/EIA-568 for additional recommendations.
3.1.32		Cabling shall meet distance limitations per IEEE 802.3.	IEEE 802.3
3.1.33		All cables will be IEEE 383 or UL910 qualified and will not contain PVC jacketing	IEEE 382, UL910
3.1.34		The Cisco Discovery Protocol (CDP) shall be turned off on all Cisco switches by placing the "no cdp run" command in each switch configuration.	
3.1.35		Network time should be maintained with a GPS time server;	
3.1.36		Synchronized time shall be used with digital assets to provide for event correlation.	
3.2	Account management and access control		
3.2.1		Default passwords shall not be used on digital assets.	
3.2.2		Service accounts shall not be used to access digital assets.	
3.2.3		Shared accounts for limited administrative access if there is a valid business need and access activity is logged.	
3.2.4		Complex passwords with minimum length of 10 should be used on digital assets, where possible (complex = two of uppercase, lowercase, number, or special character).	
3.2.5		Security rights and roles for digital assets shall be established based on least privilege, where possible.	
3.2.6		Accounts should be configured to automatically lock out when 5 (or fewer) failed attempts are logged within 1 hour.	
3.2.7		Failed login attempts should be logged, where possible.	
3.2.8		Automatic unlocking of account is allowed after 15 minutes if failed login attempt is logged, where possible.	
3.2.9		A session lock should be initiated after 30 minutes of inactivity, where possible.	
3.2.10		A manual session lock shall be allowed by user, where possible.	

Number	Name	Description	Rationale
3.3	Authentication		
3.3.1		Multi-factor authentication shall be used, where possible.	
3.3.2		Cryptographic ciphers and algorithms used for storage or transmission of authenticators shall be validated by NIST.	Comply with FIPS 140-2
3.3.3		Authentication shall be on the same architecture level as the protected assets.	
3.3.4		Authentication shall be by domain controllers rather than by local authentication, where possible.	
3.3.5		Authentication shall not cross architecture levels.	
3.4	Physical protection. Physical access controls include controlled areas, locked rooms, locked cabinets, and locked devices.		
3.4.1		Safety critical assets located in network level 4 shall be in a vital area in a locked room and locked cabinet.	
3.4.2		Non-safety critical assets located in network level 3 or 4 should be in a locked room and locked cabinet commensurate with the criticality of function protected.	
3.5	Monitoring		
3.5.1		Networks shall be continuously monitored for anomalous events.	
3.5.2		Digital assets shall be monitored for anomalous events (e.g., system, event, application logs).	
3.6	PGS digital system requirements (additions to those captured in the TFR)		
3.6.1	Performance requirements		
3.6.1.1		The system shall handle a minimum of 10 samples per second.	
3.6.2	System interface requirements		
3.6.2.1		The Control System shall be capable of communicating via CAN bus with the engine controller.	ICS TFR
3.6.2.2		The ICS shall be capable of communicating with the T-REXC historian and HMI using TCP/IP ??	
3.6.2.3		Analog hardware shall be used to transmit an operator-induced manual trip in the control room to the reactor trip circuit.	ICS TFR
3.6.3	Human machine interface (refer to ICS TFR)		
3.6.4	Reliability and resilience		
3.6.4.1		Common cause failures shall not adversely impact safety critical digital systems	
3.6.4.2		Critical digital systems shall be fault tolerant.	
3.6.4.3		Safety critical digital systems shall meet single failure criterion.	
3.6.4.3.1		Each safety-related RPS trip circuit shall include redundant relays.	
3.6.4.4		Critical digital assets shall fail safe.	
3.6.4.4.1		All safety-related RPS relays (breakers?) shall release upon loss of power or loss of signal.	
3.6.5	Adaptability		
3.6.5.1		The ICS(?) should be capable of expanding to allow other MARVEL interconnections for research purposes.	

Number	Name	Description	Rationale
3.7	Digital asset capabilities (specific to device; to be updated during high-level design phase)		
3.7.1		Identify and evaluate static and dynamic performance requirements [e.g., availability, processor (% processor time, % usage and paging file, processor queue length), memory, storage] for each digital asset, as applicable. TBD.	
3.7.2		The hardware, software, communication, and HMI/HSI interfaces shall be identified and evaluated for each digital asset. TBD.	
3.7.2.1		Source and destination for input/output shall be identified, as applicable.	
3.7.2.2		Data attributes (range, accuracy, tolerance, units of measure, formats, timing) shall be identified, as applicable.	
3.7.3		Normal and special operations shall be identified and evaluated. TBD.	
3.7.4		Digital assets shall maintain time synchronization using a trusted time server, as applicable.	
3.7.5		Physical constraint requirements TBD.	
3.7.6		Database/Information management requirements TBD.	
3.7.7		Digital assets shall be designed to meet the environmental conditions of the facility, including natural, induced-motion, shock, noise, thermal, and EMI/RFI conditions.	
3.7.8		Abnormal situation and error handling	
3.7.8.1		Audit functions, validity checks, error monitoring shall be available and enabled on digital assets, where possible.	
3.7.8.2		Identify requirements for out-of-range, unexpected values, out-of-sequence, latency, hardware faults, and time-out issues. TBD.	
3.7.9		All assumptions and dependencies shall be captured and evaluated for each digital asset, as applicable. [refer to digital risk analysis]	
4	Level 4 Non-Functional Digital Requirements		
4.1	A digital risk analysis shall be performed for each system and subsystem		
4.1.1		A consequence analysis shall be performed to identify any adverse impacts to critical functions (e.g., safety-related and important-to-safety) from unsafe control actions.	
4.1.2		A consequence analysis should be performed to identify any adverse impacts to non-critical functions that will result in reactor trip or equipment damage from unsafe control actions.	
4.1.3		A pathway analysis shall be performed to identify logical and physical pathways that may allow faults or compromises to occur or propagate.	
4.1.4		Unacceptable digital risks shall be eliminated through engineering design or mitigated through controls.	
4.2	Design Simplicity and System Hardening		
4.2.1		System design shall be simplified to reduce the digital footprint.	
4.2.2		Digital assets should be designed, built, and/or procured such that unused functionality is not included.	
4.2.3		Digital assets shall have unused ports disabled and/or blocked.	
4.2.4		Digital assets should have unnecessary software, protocols, services, or functionality disabled or removed.	
4.3	Configuration management		

Number	Name	Description	Rationale
4.3.1		The digital bill of materials (hardware, software, firmware) shall be captured and stored for each digital asset, including make, model, version.	
4.3.2		The hardware, software, and firmware configuration for each digital asset shall be captured and stored upon initial design and every modification.	
4.3.3		Disaster recovery instructions shall be developed and stored for each digital asset.	
4.3.4		Backup and disaster recovery media shall be stored in a secure, fireproof storage.	
4.3.5		Modifications to digital assets shall be controlled by engineering change processes.	
4.4	Procurement and product development		
4.4.1		Software shall be developed using secure software development techniques.	
4.4.2		Hardware shall be developed using secure hardware development techniques.	
4.4.3		Software development and modification shall follow the software quality assurance (SwQA) program.	
4.4.4		Develop the list of limitations or constraints for procurement (e.g., regulatory constraints, hardware limitations, application interfaces, parellel operation, audit functions, control functions, signal protocols, SQA, safety and security).	