Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Model-Based Systems Engineering Cybersecurity Risk Assessment for Industrial Control Systems Leveraging NIST Risk Management Framework Methodology

Alexander Gampel [1] Timothy Eveleigh [1]

[1] Systems engineering and applied sciences (SEAS), George Washington University, Washington, DC 20052, USA

ARTICLE INFO

Article History

Received:	17-04-2025
Revised:	01-06-2025
Accepted:	07-06-2025
Published:	10-06-2025

Vol.2025, No.4

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.4.2

Corresponding author. Email:
eveleigh@gwu.edu

Orcid:

https://orcid.org/0000-0003-1647-1969

ABSTRACT

The realm of cybersecurity is perpetually evolving. Organizations must adapt to changing threat environments to protect their assets. Implementing the NIST Risk Management Framework (RMF) has become vital for the protection and security of industrial control and automation systems powered by SCADA technology. However, cybersecurity professionals face challenges in implementing the RMF, leading to systems operating without proper authorization resulting in non-compliance with standards and regulations. Current RMF-based business practices are inadequate, exposing organizations to cyber threats that compromise consumer personal data and essential infrastructure information. To address these challenges, this research proposes a Model-Based Systems Engineering (MBSE) approach to implementing cybersecurity controls and assessing risk through the RMF process. The study stresses the importance of adopting a modeling approach to streamline the RMF process. MBSE can effectively eliminate erroneous structures, simplifying the acquisition of an Authorization-to-Operate (ATO). Focusing on the practical application of MBSE in industrial control and automation systems can improve the security and safety of operations. This research concludes that MBSE can address the implementation challenges of the NIST RMF process while improving the security of industrial control and automation systems. The research suggests MBSE to be a more effective strategy for implementing cybersecurity controls and risk assessment through the RMF process. The study suggests that the MBSE approach can apply to other domains beyond industrial control and automation systems.

Keywords: Authorization-To-Operate (ATO), Industrial Control Systems, (ICS), Model-Based System's Engineering (MBSE), Risk Management Framework (RMF).

How to cite the article
Gampel, A., & Eveleigh, T. (2025). Model-Based Systems Engineering Cybersecurity Risk Assessment for Industrial Control Systems Leveraging NIST Risk Management Framework Methodology. Journal of Cyber Security and Risk Auditing, 2025(4), 204–221. https://doi.org/10.63180/jcsra.thestap.2025.4.2

1. Introduction

Envision a world where a network of systems, known as industrial control systems (ICS), manages the pulse of a nation's infrastructure. ICS is the backbone of real-time operations that enables the monitoring and control of essential services. Act as guardian and play a critical role in monitoring the infrastructure. However, ICS are also the first point of vulnerability within the operational landscape if left unchecked. In this context, infrastructure includes manufacturing facilities, energy generation plants, life sciences facilities, and water treatment facilities. ICSs are more than just systems; rather, they are critical components of a nation's infrastructure, essential to dictate how we operate in modern society. Beyond these core areas, concerns extend to maritime operations, military defense systems, chemical processing industries, and air quality monitoring. However, if there were a loss of control or operation in the ICS, it could have catastrophic consequences for cities, disrupt essential services, and potentially compromise national security by leaving borders vulnerable [25].

Industrial control systems (ICS) are the foundation of real-time operating environments that are used to control and monitor critical infrastructure. The loss of operation or control of ICS can cause municipalities, large cities, and entire regions to experience loss of revenue, loss of life, irreparable damage to infrastructure, and immeasurable harm [13]. For example, manufacturing facilities, energy generation plants (nuclear and gas), water and wastewater treatment, transportation and maritime, military defense, chemical processing, and air quality monitoring are increasingly vulnerable to both the frequency and severity of attacks [13]. These areas are classified as critical or key infrastructure because they are essential for maintaining a nation's quality of life and ensuring its defense. The loss of operation or control of these ICS would have catastrophic effects on the nation's ability to maintain its cities and defend its borders [25]. Everyday life would be drastically altered if these systems were compromised, and such attacks are increasing over time. The urgency to secure these systems began in 2007 with the discovery of the Stuxnet worm [15]. In 2007, the Stuxnet worm was found as one of the first cyber security weapons and physically damaged Iran's clandestine nuclear program. Stuxnet was designed to hide in the backplane of the key ICS infrastructure targeting programmable logic controllers (PLCs) to report false status messages [15]. Cyberattacks surged in 2022, with ransomware attacks against industrial enterprises increasing by 87%. The Dragos/ICS/OT Cybersecurity year in review revealed that more nation-state groups and cybercriminals were focusing on industrial enterprises, highlighting growing concerns. According to Dragos, of the more than 500 ransomware attacks that were monitored, 437 (72%) targeted manufacturing companies. These attacks were attributed to the Lockbit, Conti and BlackBasta groups [30][25], which expressed the need for improved ICS security and protection.

In protecting vital resources and proactively preparing for breaches or assaults, governments, corporations, and nations can implement ICS defenses. Ivanti, an IT software company specializing in security and administration, became the target of a cyberattack in January 2024. Ivanti serves more than 40,000 clients and its headquarters are in South Jordan, Utah. The China-backed attack by UNC 5325 targeted the US defense sector, exploiting vulnerabilities in enterprise VPN appliances. Attackers exploited vulnerabilities in the Ivanti Connect Secure and Ivanti Policy Secure gateways to compromise private sector organizations. Seventeenhundred of these private organizations supplied equipment to the US military [11]. As a result, the Cybersecurity and Infrastructure Security Agency (CISA) began working with authoring organizations to conduct advisory and ongoing incident response activities. However, the application of Risk Management Framework (RMF) controls to ICS remains a complex and largely manual process [11]. Ineffective implementation of cybersecurity controls continues to have negative consequences for countries, organizations, and infrastructure. These consequences include increased vulnerability, regulatory non-compliance, and ineffective risk management.

The application of Risk Management Framework (RMF) remains a very complex implementation due to the nature of ICE compared to IT systems. The process if tedious and extremely manual causing implementation fatigue and user error. The traditional RMF based cyber security approach lacks the nuanced implementation which is specialized due to the operational requirements of a real time operating enviornment such as a SCADA operational technologies networking. The maintenance of a predominantly IT focused cyber security approach is inadequate in addressing these challenges and needs a more robust implementation which addressed the demands and constraints specific to ICS architectures. Ivanti's study of OT vulnerability events shows the flaws within the current implementation methodology illustrating; despite existing RMF guidelines, the exploitation of known vulnerabilities in widely used security gateways indicates significant gaps in the practical implementation of RMF controls, particularly continuous monitoring, timely vulnerability remediation, and effective configuration management. The need for RMF within critical infrastructure requires a tailored engineering approach specific to the system, and there is a clear disconnect between the IT system implementation and the OT system need for implementation. Implementing MBSE for a robust and non-bias RMF implementation takes into account the modeled system and the specific security controls of interest to the system under protection. The implementation of MBSE is also able to bring in all implementation standards and protocols NIST uses to create the security controls and restructure the implementation creating a more holistic protection of the critical system. MBSE is also able to evolve with the model and transition with the system as the system evolves and changes through modernization maintaining the Authorization to operate toggling the needed security controls for the implementation.

In today's national climate, the demand for cybersecurity professionals to develop effective strategies to improve security and safety measures has never been more critical. The research presented in this article introduces an evaluation model, grounded in the principles of MBSE, to provide a strategic solution to the cybersecurity challenges associated with applying the RMF to ICS[3]. By providing a structured and systematic methodology, tailored cybersecurity controls can be seamlessly integrated into the operational intricacies of ICS, This model demonstrates a significant enhancement of the security posture of these systems while bridging the gap between the IT centric focus of traditional RMF practices and the specialized operational needs of ICS. This approach ensures that cybersecurity measures are relevant and effective in protecting critical infrastructure against evolving cyber threats [15][16].

The proposed model supports the strategic objective of achieving an Authorization-to-Operate (ATO) for ICS by aligning cybersecurity requirements with operational priorities. This alignment facilitates compliance with national and industry-specific cybersecurity standards [15]. The application of an MBSE approach to the implementation of RMF in ICS contexts underscores the need for evolving cybersecurity frameworks and methodologies. This evolution addresses the unique challenges presented by the integration of ICS in national critical infrastructures [18]. It highlights the potential of MBSE to serve as a comprehensive bridge between standardized IT cybersecurity practices and the specialized operational requirements of ICS. This approach contributes to improving national security and economic resilience [15][26]. The SysML models and simulations developed for this research are based on an actual ICS use case, ensuring that the framework's validation is grounded in real-world operational conditions rather than hypothetical constructs.

2. Literature Review

2.1. NIST Methodology

The National Institute of Standards and Technology (NIST) publication, "Risk Management Framework for Information Systems and Organizations" [15], outlines a comprehensive risk management process tailored to address the complex cybersecurity risks facing modern organizations. This publication emphasizes a holistic approach based on risk integrated into the system development life cycle, advocating the creation of inherently secure systems that support organizational missions in a cyber-threat-laden environment. Central to this framework is the principle of continuous monitoring and real-time assessment of security controls, ensuring their ongoing effectiveness amid evolving cyber threats. The NIST Special Publication 800-82 Guide to Industrial Control Systems Security [4] stands out from ISO 27001 and other cybersecurity frameworks by specifically targeting cybersecurity concerns relevant to ICS, a critical information asset within critical infrastructures (CI) [20]. NIST highlights the necessity of embedding a proactive risk management culture within organizations, enabling informed decision-making processes regarding the security and privacy of information systems and their data. The NIST Critical Infrastructure Cybersecurity Framework offers a structured methodology to address security-related risks, tailored to meet the distinct needs of critical infrastructure providers [20]. This approach is vital to maintain the confidentiality, integrity, and availability of information, to foster trust, and to achieve organizational objectives in the digital era. The NIST RMF aims to integrate risk management into organizational processes, promoting informed decision-making and a proactive security posture. By emphasizing preparation, response, and monitoring, the RMF encourages the continuous assessment and adaptation of security controls, facilitating a dynamic approach to risk management critical in today's fast-paced technological environment [22].

2.2. NIST Methodology

The adoption of NIST standards for ICS security offers significant benefits, particularly in establishing a common language and best practices for cybersecurity in different sectors. This is crucial as cyber threats become increasingly sophisticated and cross-sectoral. NIST standards emphasize a risk-based approach, allowing organizations to prioritize security efforts based on the potential impact of different threats, enabling more efficient resource allocation and effective risk mitigation strategies. The focus on continuous monitoring and incident response ensures that organizations can quickly adapt to new threats, minimizing the impact of cyber attacks. High-profile cyber attacks such as the Stuxnet worm [23] underscore the vulnerability of ICS, which are integral to critical infrastructure sectors such as manufacturing, energy, and water treatment. NIST standards, such as the NIST SP 800 series, provide comprehensive guidelines for securing these critical systems [20][25][26], improving cybersecurity posture [20][22], and fostering resilience against threats [4][22]. Although NIST frameworks offer invaluable guidance to improve the cybersecurity landscape, their application to ICS reveals certain limitations, such as discrepancies in operational requirements between Internet Technologies (IT) and Operational Technologies (OT) systems [22] and the need for specialized knowledge to adapt these frameworks effectively [4][20]. The need for a distinction for isolated frameworks is because IT and OT systems have different goals when it comes to operating requirements. An OT system focuses more on having a high availability environment that operates at real-time, because any disruption in operation can have catastrophic repercussions to the system it is controlling. IT systems do not have to worry about such disastrous consequences because they are utilized for data transfer and not system operation.

2.3. NIST Methodology

The NIST RMF has many strengths that establish it as a fundamental element in building resilient and secure information systems within organizations. One significant advantage is its flexibility and applicability in various sectors and information systems, allowing it to serve as a universal blueprint for cybersecurity risk management [27]. This ensures that organizations of varying sizes, complexities, and missions can tailor the framework's principles to their specific security requirements and risk appetites. RMF advocates integrating security and privacy considerations from the system design phase, embedding security inherently within the system rather than as an afterthought. Putting emphasis on continuous monitoring and real-time risk assessments, the framework ensures that security controls remain effective over time, strengthening the organization's ability to protect critical assets and sustain operations in the context of evolving cybersecurity challenges [27].

Despite its comprehensive nature, the implementation of the RMF can present significant challenges. A significant issue is the isolated approach to risk management, which often results in inconsistent application of RMF steps at various organizational levels [18]. Furthermore, the RMF preparation phase often falls short due to inadequate resources, insufficient commitment from senior leadership, or a lack of proper training, which undermines the integrity of the framework from the outset [18]. The complexity of the RMF itself can lead to overburdened systems with excessive controls or vulnerable systems due to under implementation, illustrating a misunderstanding of risk management priorities [3]. Furthermore, continuous monitoring is often less rigorous than required, leading to outdated security controls and systems increasingly exposed to new risks [41]. Privacy risks also require greater attention, as improper implementation of privacy controls can impede system functionality or do not protect privacy rights [33].

With ICS, the fundamental differences between OT and IT present additional challenges. The security controls outlined in NIST SP 800-53, while comprehensive for IT systems, may not be fully applicable to ICS which is an OT system [27]. NIST categorizes ICS to encompass SCADA systems, Distributed Control Systems (DCS), and other related control configurations such as PLCs, taking into account their distinct demands for performance, reliability, and safety [20][21]. Addressing these weaknesses requires organizations to adapt the RMF flexibly and iteratively, reevaluating and updating controls as threats evolve. Explicit acceptance of risk by an authorized official is crucial, involving a thorough assessment of the controls implemented and the responsibility for residual risk [33]. The challenges of implementing RMF practices in ICS environments highlight the need for tailored cybersecurity strategies that align with the unique operational context and ensure the resilience of critical infrastructure systems.

2.4. CYSeMOL

Holm et al. (2013) introduced the Cyber Security Modeling Language (CySeMoL), a tool designed to estimate the likelihood of different cyberattacks succeeding. CySeMoL is beneficial because it allows users without deep security expertise to model their systems and assess security across various IT components, processes, and user attributes. In the power supply sector, CySeMoL helps to understand the complex interdependencies and vulnerabilities of integrated systems, highlighting the need for advanced cybersecurity measures to protect against potential breaches [17].

CySeMoL addresses the challenge of interconnected vulnerabilities within enterprise systems by providing tools to explain these complex relationships. This empowers decision-makers, who often lack a comprehensive understanding of their systems' vulnerabilities, to make better informed cybersecurity decisions. However, the tool faces limitations, such as the prohibitive cost of hiring security experts and the time-intensive nature of conducting thorough literature reviews. Existing network security assessment tools, such as the NETSPA, MulVAL, and TVA tools, often fail to meet the specific needs of power utility managers, constrained by limitations that diminish the practical utility of the tools. This highlights the critical need for tools capable of navigating the unique challenges of the energy sector [17].

2.5. SysML-Sec

SysML-Sec, introduced by Stockman, is a methodology aimed at enhancing collaboration between system designers and security experts at all stages of system development [38]. SysML-Sec integrates a goal-oriented approach to requirements capture with a model-oriented approach to system architecture and threat analysis. The methodology includes phases such as the definition of requirements, the organization of attacks, partitioning, design, and system validation, allowing security professionals to fully evaluate the balance between security and safety [39].

SysML-Sec employs a Y-Chart-based system analysis alongside a software design phase structured around the V-cycle methodology. The V cycle is a model for system engineering that emphasizes a systematic and iterative process of requirements definition, design, implementation, and validation. Each step in the left arm of the ”V” (from system requirements to detailed design) corresponds to a verification or validation activity on the right arm (from unit testing to system validation). This structured approach ensures that requirements, potential attack vectors, and key functions are identified early and are revisited throughout the lifecycle to maintain alignment with safety and performance goals. Despite its rigor, balancing performance with safety and security remains challenging, especially when integrating security protocols that could increase latency or processor load. Tools such as TTool validate that safety and security mechanisms are fully integrated into the design process, ensuring comprehensive consideration of these critical factors [38].

Despite its effectiveness, SysML-Sec must continually improve to address the intricate relationship between safety and security at every development stage. Although the methodology suggests that the relationship between safety and security is addressed early in the development cycle, it is often inadequately assessed during the partition stage in common industry practice. Evaluation of the compatibility of security mechanisms with safety properties using validation techniques is essential during this stage. This underscores the need for a comprehensive toolkit and methodology to ensure that cybersecurity measures do not compromise system performance [38].

2.6. MBSE ICS Security Controls without RMF

To advance the cybersecurity of ICS with MBSE, the distinctive operational and security needs of ICS must address unique challenges that contrast sharply with those of traditional IT systems. These challenges require an innovative approach beyond conventional frameworks, especially in areas of system availability, integrity, and safety the main priorities in operational technologies (OT) that require a different focus compared to IT environments
[35] [38]. To address these specific requirements, the adoption of MBSE, using systems modeling language (SysML) extensions, is emerging as a robust solution. MBSE in ICS allows for a structured methodology to enhance cybersecurity by providing a comprehensive approach to control system security, aligned with the unique characteristics of ICS environments [35] [5].

The SysML extension introduced by Lapon [21] facilitates the extraction and visualization of vulnerabilities within ICS models. This methodology uses the structure of SysML, widely applied in MBSE, enhancing it with security-specific capabilities crucial for ICS environments [21]. By modeling ICS architectures such as PLCs, Human-Machine Interfaces (HMIs), and communication networks, the Security Analysis SysML extension serves as input for a formal reasoning tool. This tool, founded in ICS-CERT vulnerability databases and ICS security standards, identifies potential vulnerabilities within system components and interactions [35][20]. If a communication channel lacks authentication, the SysML Security Analysis extension flags it as a potential spoofing risk. These vulnerabilities are then reintegrated into the SysML model, allowing engineers and cybersecurity professionals to visualize and address these security risks interactively [5] [34]. Primarily designed for IT environments, traditional frameworks often fall short when applied directly to ICS. The Security Analysis SysML extension fills these gaps by automating vulnerability identification tailored to ICS, considering their unique operational context [21]. This approach enables more precise security applications that are suited to the operational demands of ICS, providing a systematic process for vulnerability management and risk mitigation [38]. A SysML-based vulnerability extraction process brings a dynamic, continuous approach to cybersecurity for ICS environments, replacing static assessments with iterative updates. It also exposes critical aspects of the system model to a simulation environment allowing a comprehensive assessment of systems design across many threat scenarios in a probabilistic context. This enables a nuanced assessment of evolving cybersecurity requirements, ensuring that risks are identified, visualized, and mitigated in near-real time as new threats arise [34].

The Security Analysis SysML extension, when applied through MBSE, supports a continuous and adaptive approach to managing cybersecurity risks within ICS environments. Its effectiveness, demonstrated through practical applications, highlights the potential of MBSE to address the unique challenges of ICS cybersecurity [35] [38]. However, there is a missing piece to complete the full integration of an MBSE model to improve cybersecurity posture. The integration of NIST's RMF standards into this framework creates a model that is usable in the field and able to implement the previous ideas that were only theoretical through case studies and practical implementation [35] [38]. RMF is the current cybersecurity landscape model, yet by integrating the findings of Lapon, we achieve a more comprehensive and effective model that we will present in the next section. model shown in the methodology section [5] [34].

2.7. Alternative Methodologies

Alternative methodologies were considered before ultimately settling on a Model-Based Systems Engineering approach as a suitable solution for the integration of cyber security risk mitigation based on the RMF process within the industrial control system implementation. AI based risk assessment was considered to leverage machine learning to implement detect and respond risk mitigation. Organizations which have AI based risk analytics implemented have demonstrated a significant boost within their risk detection capabilities up to a 60% increase in detection [22]. AI based techniques are effective in parsing through large data sets to flag data anomalies within OT network systems. The limitations of AI-driven models are due to the nature of the system under implementation. Industry 4.0 SCADA networks operate on legacy systems and have limited data attributed to them. After iterations of upgrades and implementations the systems are unique to their organizations and usually do not have all the proper data needed to implement effective AI models. Trained AI models need rich data sets and heavily depend on the training data. ICS systems usually lack the needed data and analysis for these kinds of systems causing them to make mistakes within implementation and often reporting on false positives due to the nature of industrial control and real time SCADA networks. Also, Cyber incidents to ICS systems are limited due to proprietary information of the controllers, and the lack of transparency will cause AI models to be incomplete. Lastly, AI models are not decision-based frameworks such as RMF and the decision matrix would still need to be implemented to produce formalized documentation and decision traceability including the rational required by the frameworks for system compliance. Probabilistic frameworks models such as a Bayesian network approach was also considered as an area of interest to solve this problem.

Bayesian network (BN) approaches offer a probabilistic framework for risk assessment and mitigation. In the context of cybersecurity Bayesian networks (BNs) are implemented for their ability to incorporate expert level knowledge and overcome data limitations [11]. Using conditional probabilities for constant system assessment researchers have been able to apply BN to ICS cyber risk models and assess threat scenarios [22]. However, the strength of a Bayesian method lies in their ability to represent complex interdependencies between attack vectors: vulnerabilities, attacks, and defenses. This can be a very useful implementation where real incident data is implemented and controlled experiments are difficult to implement. This makes BN an ideal candidate for cyber risk mitigation, but constructing and maintaining a Bayesian model for a large-scale ICS is labor intensive and complex. The data might also not exist to create a clear model because system experts might not have the complete knowledge based needed for controllers that are 20-30 years old. Each component and interaction must be represented as a node with prior and conditional probabilities including their behavior during normal operation and abnormal behavior including all areas of its implementation; power draw, control behvaior, network communication, and idle state. A Bayesian implementation may require too much of a burden to solve this implementation problem. This is why MBSE was selected as the approach to solve the Risk mitigation framework implementation by creating robust models which can be tailored to the system based on components and system requirements based in implementation and industry standards per controller.

MBSE leverages a systems approach that aligns with engineering processes specific to ICS development, maintenance, and operation. Instead if treating risk assessment as a separate implementation which is done on the system it integrates security implementations within the design of system architecture. It makes it part of the requirement implementation, and authorities the systems creation based on the model's data inputs. The advantages of this system implementation within the

ICS domain are why this methodology implementation was selected for RMF implementation. MBSE facilitates traceability and documentation for every security requirement, control and risk mitigation tying it back to each system element and sub-model. This traceability is something that BN and AI models will not provide within their implementation which directly addresses compliance concerns for maintaining a system's Authorization to operate. MBSE also creates a visual and structural model capturing the system under protection including their real time operations, safety-critical function and availability contrasts. MBSE integration prioritizes early system validation and iterative refinement of security controls that can be simulated and modeled through validation and verification models and use case models. Lapon's SysML-based security extension for ICS can automatically extract and visualize system vulnerabilities identifying system weak points [21]. MBSE's proactive approach building cyber risk assessment within the system's design makes it a better candidate than BN and AI models for anomaly detection. In an ICS environment, collaboration between control engineers, IT security professionals, and compliance officers is essential. A model-based approach offers a definite reference model where system architecture, threat scenarios, and controls are unified, reducing miscommunication.

3. Research Methodology

The integration of NIST RMF into the MBSE methodology for ICS cybersecurity transforms the process into a comprehensive framework. Although MBSE offers significant advances, integrating RMF completes the process, ensuring that cybersecurity is addressed from the earliest design stages through to ongoing operation. This integration creates a complete security posture for ICS environments, aligning it with the critical need for availability, integrity, and safety. A cyber-influenced integration of an RMF framework into a SysML-based MBSE process makes vulnerability identification part of a systematic framework governed by risk management standards. RMF provides a rigorous process for categorizing system components, selecting controls, and evaluating cybersecurity measures, which, when combined with SysML, visualizes vulnerabilities and maps these risks to relevant controls. The integration of RMF into the MBSE SysML model can extract system vulnerability by transforming it into a continuous dynamic risk management process. With RMF, each vulnerability identified through SysML becomes a focal point within a larger, structured framework that ensures compliance with cybersecurity standards while remaining adaptable to emerging threats. For example, if a new cyber threat appears, the SysML model can reflect this updated risk, allowing for rapid re-assessment and control implementation. Figure 1 shows how the model is created through the integration of key security control vectors such as NIST 800-37 (RMF), NIST 800-53 (security controls), and Control Correlation Identifiers (CCI). Using MBSE custom assessment models and requirements analysis, system verification and validation models are created to ensure that the system can maintain its ATO based on its specific requirements.

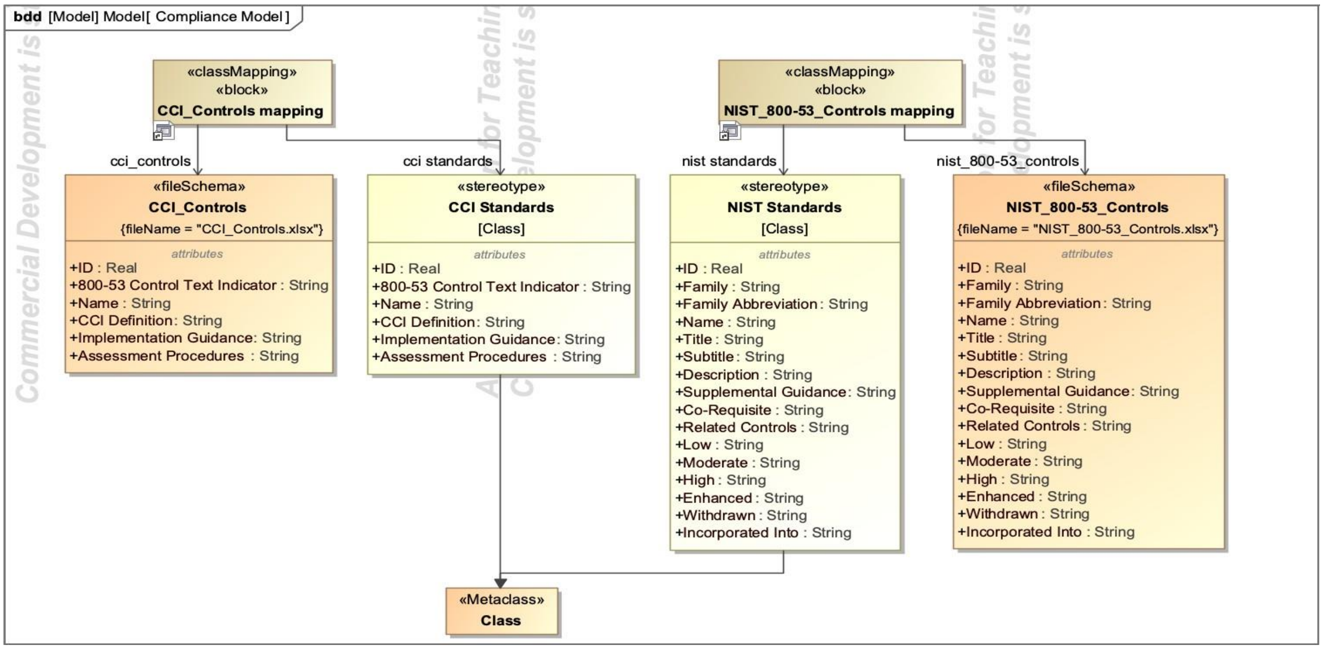


Figure 1. Block Definition Diagram (BDD) diagram of The RMF model's implementation

The integration of MBSE with the RMF introduces a structured and systematic methodology that enhances each phase of RMF with model-driven practices. The six steps of the RMF: categorize, select, implement, assess, authorize, and monitor are inherently aligned with the capabilities of MBSE [27]. In the Categorize phase, MBSE defines information flows, categorizes data, and assesses security impacts. This provides a comprehensive understanding of the boundaries of the system and the interactions of data. These activities also allow the modeler to map the security controls from the Select phase of NIST SP 800-53 for system components to the CCI security controls and system requirements, ensuring a customized and relevant control implementation. During the Implement phase, this approach leverages interface definitions and behavioral models to create actionable implementation plans, reducing the configuration of security controls [31]. Finally, the Assessment phase provides the system simulations to validate and test the efficacy of security measures prior to physical implementation. This allows the system to authorize the use of the model by generating documentation and evidence directly. Lastly, the system can be continuously monitored through the monitoring phase using the built model. This dynamically updates system models with real-time operational data, enabling continuous monitoring, adaptive risk management, and compliance.

The above methodology ultimately creates an improved system level understanding through visual representations such as system context diagrams, interface definitions, and data flow diagrams, which improve collaboration and clarity for RMF stakeholders. MBSE also provides complete traceability, linking requirements from RMF compliance to system implementation and testing. For example, the NIST SP 800-53 requirements [27] can be explicitly traced to their implementation in system components and validated using automated testing models. Behavioral models simulate system operations under various conditions, identifying vulnerabilities, dynamically assessing risks, and informing strategic security adjustments. MBSE streamlines compliance by automating the generation of critical RMF artifacts, such as System Security Plans (SSPs) and Risk Assessments, reducing manual effort while ensuring consistency. These behavioral models further simulate operational scenarios to validate security controls, fill gaps, and reinforce the system's security posture. Using MBSE tools such as Cameo and SysML, now called CATIA Magic Cyber Systems Engineer, within the RMF process can lead to a more effective implementation of cybersecurity controls, allowing a comprehensive assessment of risks and the security of system boundaries [2]. This methodological approach encourages the development of a sophisticated evaluation model capable of determining whether cybersecurity requirements are met for operational authorization, identifying risks at the system boundary, and determining the need for mitigation measures [27] [40].

Through the creation of the RMF model shown in Figure 1 it is overlayed through the initial phases of RMF. The system's information types are assessed and are categorized by their impact levels. Implementing MBSE, the constructed system context and block definition diagrams are used to define system boundaries, information flows, and interconnections within the ICS. The model-based approach allows the security architects to assess the potential impact of the system through the CIA triad confidentiality, integrity, and availability losses per component. For real-time operating environments it is important to capture the operational scenarios to determine risk and impact factor due to cyber incidents, and due to the limitations of the current implementation this is not done. MBSE implementation of RMF security controls will allow the designer to categories the impact of controls not being implemented and their kinetic effect through the system because of the missing security control. MBSE allows for this implementation through the categorization phase of the RMF model as it is baked into the system requirements of operation. The model embeds the impact of the system's operation interconnection the ICS component and its data flow and the NIST 800-37 guidelines [15]. This creates a foundation which can be leverage within the control selection phase. The model in Figure 1 can enhance the process mapping drawn from 800-53 [27] and ICS standards directly into the system model. This control baseline is their tailored to the ICS's modeled components and their data pathways. Figure 1 is the SysML representation of a block definition diagram showing the MBSE implementation of methodology mapping for RMF control requirements for system risk mitigation for cyber security implementation. The associated structures and traceability mapping allow for the CCI and NIST controls to show their relationships and associations to one another. The Figure shows the hierarchical and associative relationships between these two controls sets through inheritance and clear mapping allowing the systems engineer to comply with system requirements and traceability. By explicitly mapping these two identified controls the model can determine which requirements are met by which standard depending on the security implementation of the system under protection. The methodology enhances traceability and provides a robust and ever growing model to evaluate compliance efficacy and risk mitigation. MBSE offers this structured approach with significant advantages including constant update abilities, operating efficiency, improved clarity, and proactive identification of gaps and security risk. Figure 1 is a visual representation of the mapping of the methodologies shortened by key indicators and identification indicators able to be linked through the requirements matrix. Through SysML requirements diagrams and the allocation relationships, the model is linked based on the selected security controls to the relevant system elements i.e. programable logic controllers (PLCs), Human machine interfaces (HMIs), Nodes, and data acquisition units (DAU). Through this process the model can ensure that the chosen controls are appropriate for the ICS operational environment. This is later shown in Figure 3 through AC-2(1) automatic account disabling [17]. The Model's implementation eliminates ambiguity in control implementation only associating the enhancement of the control and system model for the component that are applicable to that system function. Aside from showing the applicable controls on the system components it is also a blueprint model that integrates within the system's design highlighting gaps where applicable controls are not implemented. The security control is visible within integration of the ICS design and the supporting security plan would alight with the organization's operating objectives, NIST, and leading industry standards. The SysML model's the internal block diagrams of the state machine and how those specific security controls are implemented on that system. The security functions are modeled through a detection workflow through the system operation of the protected architecture and the interface definitions allow the operational of the system to be modeled per component. These implementation controls through the model reduces the risk of misconfiguration of the security controls and will flow down the model per the intended operation of the system and the applicable security controls. The model integration allows for early assessment for vulnerability identification and non-compliance operation within a simulated model based on the real application of the production enviornment. The deficiencies are detected and categorized within the model as gaps within the security controls. MBSE then generates the test cases based upon the requirements and the security implementation identifying how controls are identified, validated, and verified through behavioral based models. The model in Figure 1 and the deep dive in Figure 5 show the interdepended relationships and the implementation of the behavioral model for AC-2(1).

The final deliverable of the model is seen within the authorization of the model. The comprehensive implementation of the MBSE model eases the preparation of accreditation artifacts and packages for the final ATO. Since the MBSE approach creates a trace between controls, requirements, and verification in one holistic model it automatically produces the documentation needed for the authorization decision. The System security plan, reports, and risk assessment summaries are derived through the model's data and are delivered through the model's structural views. The implemented controls and their status based on the requirements are provided through the state diagrams and the assessment traceability as seen in Figures 3-5. The Single source of truth is kept up-to-date through the robust model, and the correction and implementation of security controls as specified by the system's requirements. The requirements linking to the security controls toggle which verification and validation procedures need to be implemented based on the system component in question and is done for every component in the system. The model's repository would eliminate the need for rework on repeated elements with the same configuration items maintaining the ATO for the system. MBSE streamlines the paper heavy authorization stems for authorizing officials and stakeholders reviewing the model and consolidating the information on the system. After the authorization stage is completed monitoring of the system and model is done on a continuous basis. Vulnerabilities, control updates, and system changes are inputted into the model and linked back to the system requirements toggling the needed security implementation of the model in Figure 1. This would flag any additional elements which would be out of compliance as the system evolves. The model is periodically reviewed and refined overtime as additional information is needed on the security of the system providing the most up-to-date model. This allows for risk analysis to be conducted in a structured way where the model could show which modifications the system would change a secure zone to a vulnerable one or vice versa.

Supporting this methodology are several MBSE artifacts that align directly with RMF processes. The context diagrams of the system illustrate boundaries, data flows, and dependencies, which guide the categorization and definition of security requirements [15]. Requirements analysis links RMF controls to organizational needs, while interface definitions highlight critical security control points such as encryption and access controls [19]. Data flow diagrams trace sensitive information movements to validate protection mechanisms, and behavioral models simulate system operations to dynamically identify vulnerabilities and validate controls. Compliance verification models ensure traceability and thorough validation of RMF compliance criteria, directly linking them to system requirements and testing outcomes. In the results section, the methodology applied to a system is discussed and demonstrates how the model verifies its security. Using MBSE, the system was modeled with a detailed data flow diagram, interface specifications, and behavioral models addressing authentication, encryption, and monitoring. the implementation of data flows in the next section provide categorization and control selection, while traceability linked controls such as AC-2 (Account Management) to their implementation and validation. When applied to all applicable controls of the system, this approach leads to faster ATO approval, supported by comprehensive traceability, robust risk assessments, and adaptive compliance verification. By combining MBSE and RMF, this methodology establishes a robust framework for secure system development and operation, transforming RMF from a static process into a proactive and dynamic security model.

4. Analysis and Findings

Using the NIST 800-37 and 800-53 standards, a trace categorization was created and implemented within a SysML framework (Figure 2), and a structured and adaptable method was developed to achieve and validate compliance with cybersecurity and operational standards. This approach systematically maps requirements, controls, and assessment practices into a hierarchical structure that takes advantage of NIST standards, improves operational clarity, and streamlines compliance efforts. NIST Trace employs a hierarchical categorization of families, controls, and enhancements that ensure that all aspects of cybersecurity and privacy are addressed in a comprehensive way. In the following example, the categorization of the specific family of Access Control (AC) controls into functional domains provides a high-level perspective. The research development a series of SysML models Figure 2-5 showing the MBSE performance on a real world ICS implementation for access control. Individual controls, such as AC-2 for account management and enhancements, such as AC-2(1) (automatic disabling of inactive accounts), offer actionable refined requirements that can be tailored to specific organizational needs without compromising compliance. This is demonstrated in the implementation of the model in Figure 2. the

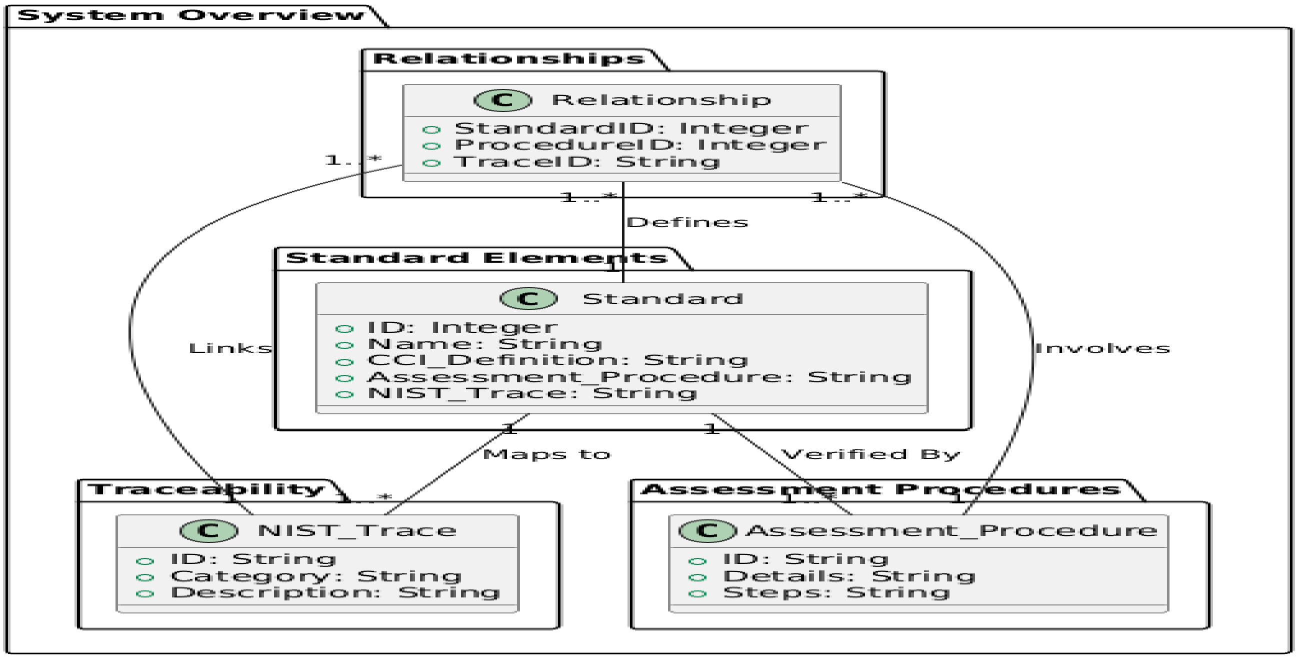


Figure 2. NIST RMF and MBSE implementation

We implemented a SysML framework to improve traceability by enabling precise mapping of NIST controls to organizational requirements, regulatory frameworks, and assessment procedures. This is achieved by uniquely identifying each control and enhancement and linking them directly to audit logs, system configurations, and global compliance standards like ISO 27001 or PCI-DSS. This mapping reduces ambiguity during audits and facilitates seamless validation of compliance through detailed documentation. Additionally, the SysML model integrates the Assessment Procedure Attributes, providing a robust mechanism for verifying the control implementation. For this example, AC-2(1) (application of test session lock) was leveraged as a unique attribute with detailed step-by-step verification instruction. Documentation tracking of the results and corrective actions ensure consistency and reproducibility in compliance assessments. The model links the requirement of AC-s for user account management to correspond to the system element and verification procedure of that component creating traceability. The model is enhanced for the sub-control to be accounted for eliminating the gaps which could be found in manual implementation.

The dynamic relationships between standards, controls, and assessment procedures are visually represented in the UML model, as illustrated in Figure 2. Figure 3 shows the use case diagram integrating the interactions of the user and the system component for the security control group applicable for that device. These relationships highlight dependencies and redundancies, improve risk analysis, and identify potential vulnerabilities. Performing a more detailed evaluation of the process, Figure 5 shows the multiple assessment procedures required for AC-2 which is discussed later to conclude the model. The procedures are discussed in detail below, but dynamic representation allows stakeholders to grasp the interconnectedness of compliance measures, enhancing both decision-making and operational efficiency.

Through this example model, an improved audit readiness and risk mitigation was created by linking audit artifacts directly to standards and controls, creating an unbroken chain of evidence. Structured representations of controls and validation steps simplify both internal and external audits, while regular assessments identify gaps and enable proactive remediation of vulnerabilities. The modularity of this SysML-based NIST trace framework makes it scalable and adaptable to evolving organizational needs, which, in turn, addresses the main concern of sustainability with an ever-growing list of security controls [27]. Controls and procedures can be expanded or modified without disrupting existing compliance structures, making this approach particularly suitable for dynamic environments subject to rapidly changing regulations or emerging cybersecurity threats.

Building upon the foundational framework discussed earlier and leveraging the NIST trace-based SysML representation, session lock functionality was implemented, a critical control for maintaining system security and user accountability. As illustrated in Figure 3, the hybrid use case diagram integrates user interactions with operational requirements, such as verifying login banners, accepting access terms, and responding to inactivity triggers. This integration ensures that session lock functionality not only addresses security compliance, but also enhances usability and adaptability. The session lock workflow begins by monitoring user activity and, upon detecting inactivity, activates a lock screen requiring re-authentication through credentials such as passwords, PINs, or biometrics. An activity diagram is used to elaborate on Streamlining Cybersecurity Risk Assessment for Industrial Control and automation Systems: Leveraging NIST’s Risk Management Framework (RMF) implemented using Model-Based System’s Engineering (MBSE) the specific use cases for each scenario. This ensures only authorized users can resume access, maintaining compliance and reinforcing security. Figure 3 is created as a hybrid use case diagram to illustrate the user requirements for a widget, focusing on user interactions such as verifying a log-in banner, accepting access terms, and responding to inactivity triggers. These interactions are central to implementing session-lock mechanisms.

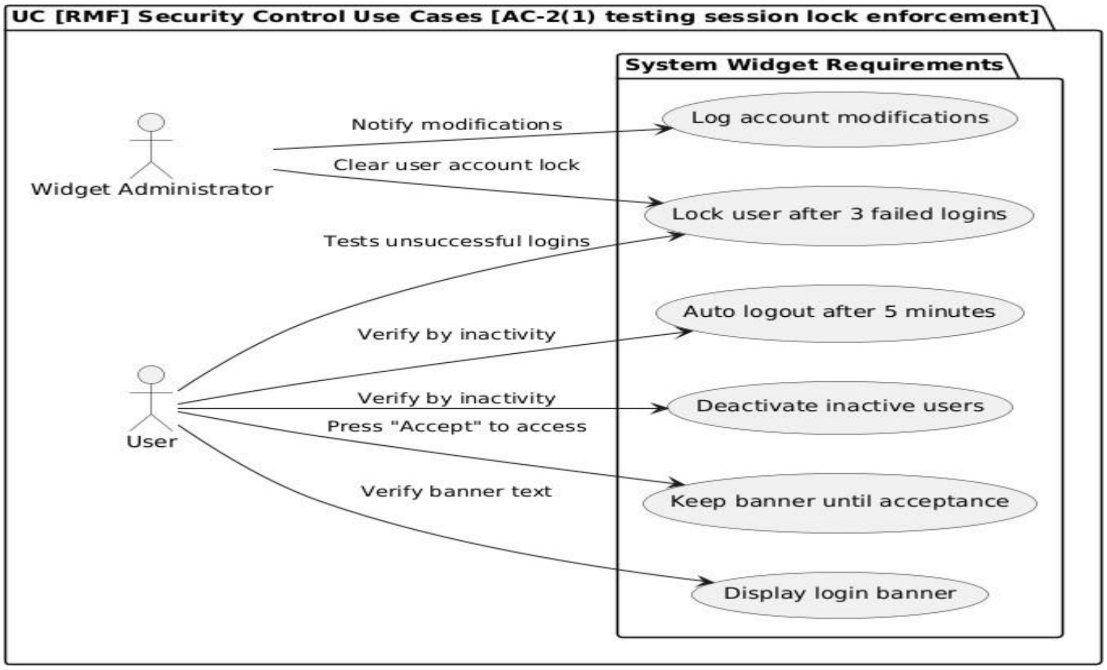

UC [RMF] Security Control Use Cases [AC-2(1) testing session lock enforcement]
System Widget Requirements
Widget Administrator
User
Notify modifications
Clear user account lock
Tests unsuccessful logins
Verify by inactivity
Verify by inactivity
Press "Accept" to access
Verify banner text
Log account modifications
Lock user after 3 failed logins
Auto logout after 5 minutes
Deactivate inactive users
Keep banner until acceptance
Display login banner

Figure 3. Use Case Diagram for AC security group

The operational use case diagram outlines the session lock beginning with session initiation, during which user activity is monitored via mouse movements, keystrokes, or touchscreen input. If the system detects no activity within the configured timeout period, it activates the session lock. This involves displaying a lock screen, often with re-authentication prompts, as represented by the ’Display login banner’ and ’Keep banner until acceptance’ use case in Figure 3. User notifications, including countdown warnings prior to session lock, enhance usability by providing users with an opportunity to maintain their session before being locked out. Once the session is locked, users must reauthenticate using credentials such as passwords, PINs, or biometrics. This process not only reinforces security but also ensures compliance with organizational policies and standards such as NIST SP 800-53 (AC-11: Session lock) [28]. AC control groups specifically 2,5,8,9 are the security controls analyzed showing the implementation of the MBSE model to be valid using the proper procedures are requirements of NIST. Organizations can tailor inactivity timeout durations, authentication methods, and user notifications to balance security with usability. The integration of session lock functionality into broader organizational policies ensures alignment with security frameworks such as ISO 27001 and compliance requirements for environments with sensitive data. The use cases for session lock functionality range from securing workstations in public spaces to protecting shared devices and sensitive environments. Secure environments can rely on session lock mechanisms to comply with rigorous standards, further enhancing system accountability through audit logging of lock and unlock events. Logs capturing timestamps, user IDs and device identifiers provide an unbroken chain of evidence, reinforcing compliance and audit readiness [27].

To validate this functionality, an extensive test of the AC security group was performed using the login / lockout verification procedure. Functional tests confirmed that sessions locked after the specified timeout period, supported manual locks, and required valid re-authentication credentials. Security tests evaluated the robustness of the lock screen against bypass attempts, while usability tests ensured the interface was intuitive and warnings were adequate. This is achieved by creating the model shown in Figure 4 to elaborate the use cases shown in Figure 3. Together, an accurate picture of all the available system behaviors can be analyzed. These activities traced to the requirements in Figure 5 show whether the system complies with its requirements and can receive an ATO based on the requirements of the specific system.

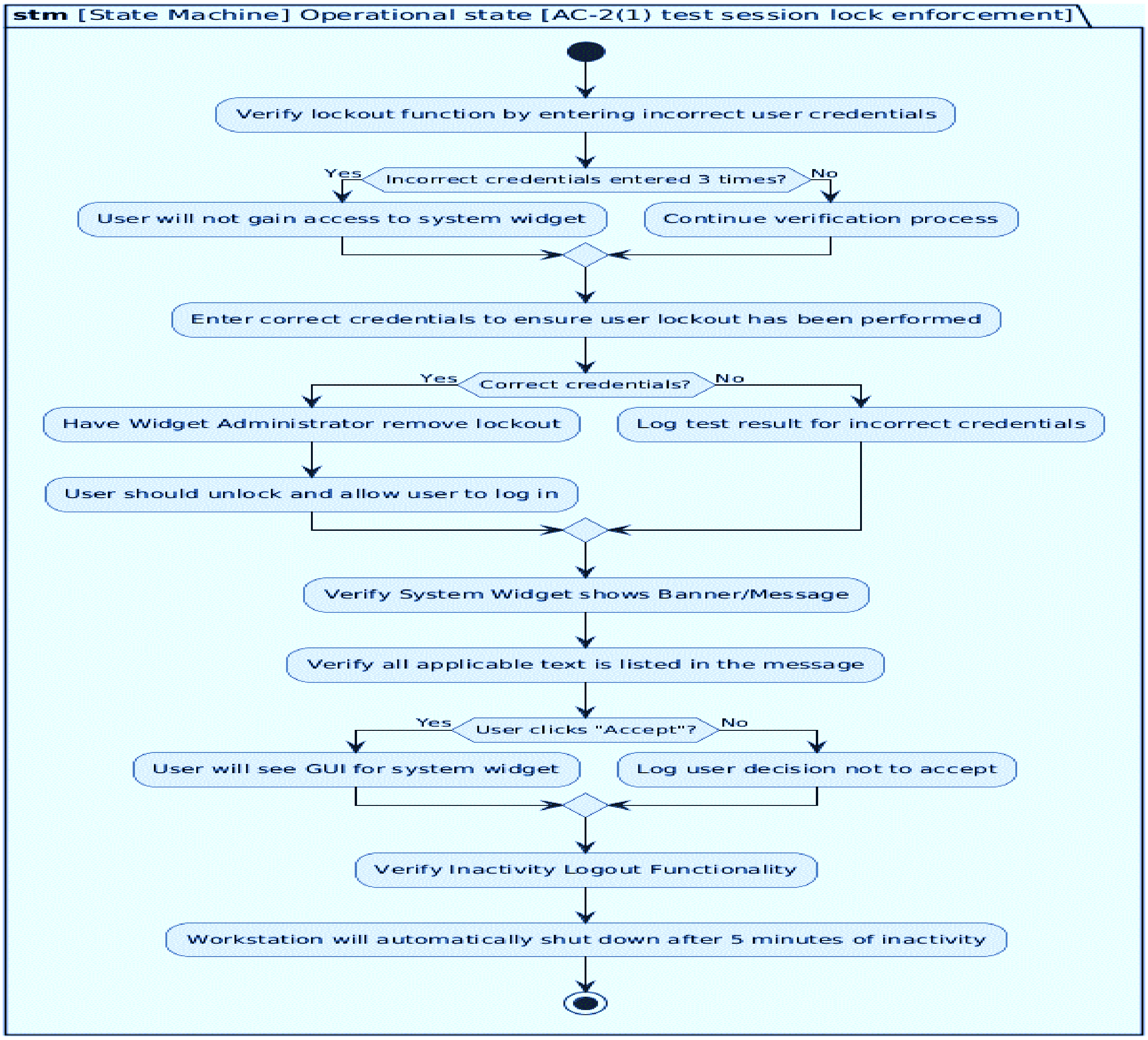

stm [State Machine] Operational state [AC-2(1) test session lock enforcement]
Verify lockout function by entering incorrect user credentials
Yes
Incorrect credentials entered 3 times?
No
User will not gain access to system widget
Continue verification process
Enter correct credentials to ensure user lockout has been performed
Yes
Correct credentials?
No
Have Widget Administrator remove lockout
Log test result for incorrect credentials
User should unlock and allow user to log in
Verify System Widget shows Banner/Message
Verify all applicable text is listed in the message
Yes
User clicks "Accept"?
No
User will see GUI for system widget
Log user decision not to accept
Verify Inactivity Logout Functionality
Workstation will automatically shut down after 5 minutes of inactivity

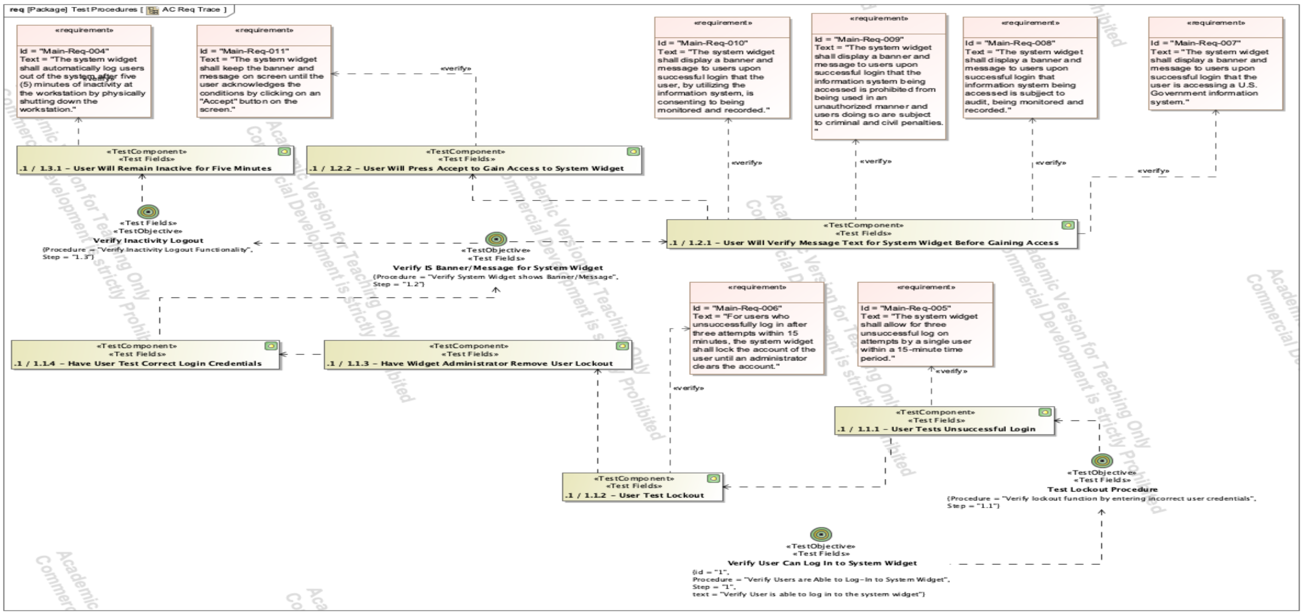
Figure 4 . State Diagram Login/Logout Verification

Based on the previous model of session lock functionality, the verification and operational workflows of the lockout activities represented in Figure 4 were reviewed. This figure provides a systematic description of the steps involved in validating account lockout functionality, focusing on both security effectiveness and user experience. Using a structured methodology, the demonstration illustrated how properly implemented lockout controls prevent unauthorized access, improve configurability, and ensure usability, all while adhering to security compliance standards.

Figure 4 show the modeled dynamic behavior of the system under security stress condition. Using a State Machine for login/lockout the model is used to simulate a vulnerability that would need to be patched based on the system's need. The invalid login attempts would trigger a lockout of the system, and the validation steps are shown in Figure 4 for the validity of implementation. The results show that 3 incorrect attempts would transition the model to lockout based on AC-7 control policy [28]. This model further tests a brute-force attack sequence where the model is consistently enforced based on improper password attempts. This model-based validation is a power form of empirical evidence when implementing and creating your system requirements and cyber security assessment as well as your risk mitigation strategies showing where your gaps could potentially be based on the vulnerabilities of your system under protection.

The lockout mechanism begins by verifying the system's ability to enforce lockout thresholds, as seen in the initial activities of Figure 4. For example, when incorrect credentials are entered three consecutive times, the system denies further access, effectively blocking unauthorized attempts. This was further validated through simulated brute-force attacks, where the system consistently locked out accounts after the defined threshold was exceeded. The workflow also incorporates a post-lockout verification step, ensuring that locked accounts remain inaccessible even with valid credentials until the lockout period expires or a manual reset is performed by a widget administrator. These steps underscore the robustness of the lockout mechanism in mitigating unauthorized system entry.

This model-driven approach also promotes consistency between implementations, reduces errors, and improves the reliability of RMF applications. Figure 4 presents a clear sequence of actions, from lockout enforcement to user reauthentication, ensuring that every scenario is accounted for in a standardized way. The scalability of this framework enables organizations to adapt the lockout process to complex and dynamic environments, such as those with evolving regulatory requirements or increased security risks.


req [Package] Test Procedures [AC Req Trace]
«requirement»
«TestComponent»
«Test Fields»
.1 / 1.3.1 – User Will Remain Inactive for Five Minutes
.1 / 1.2.2 – User Will Press Accept to Gain Access to System Widget
.1 / 1.2.1 – User Will Verify Message Text for System Widget Before Gaining Access
.1 / 1.1.4 – Have User Test Correct Login Credentials
.1 / 1.1.3 – Have Widget Administrator Remove User Lockout
.1 / 1.1.2 – User Test Lockout
.1 / 1.1.1 – User Tests Unsuccessful Login
«TestObjective»
Verify Inactivity Logout
Verify IS Banner/Message for System Widget
Test Lockout Procedure
Verify User Can Log In to System Widget
«verify»

Id = "Main-Req-004"
Text = "The system widget shall automatically log users out of the system after five (5) minutes of inactivity at the workstation by physically shutting down the workstation."

Id = "Main-Req-011"
Text = "The system widget shall keep the banner and message on screen until the user acknowledges the conditions by clicking on an "Accept" button on the screen."

Id = "Main-Req-010"
Text = "The system widget shall display a banner and message to users upon successful login that the user, by utilizing the information system, is consenting to being monitored and recorded."

Id = "Main-Req-009"
Text = "The system widget shall display a banner and message to users upon successful login that the information system being accessed is prohibited from being used in an unauthorized manner and users doing so are subject to criminal and civil penalties. "

Id = "Main-Req-008"
Text = "The system widget shall display a banner and message to users upon successful login that information system being accessed is subject to audit, being monitored and recorded."

Id = "Main-Req-007"
Text = "The system widget shall display a banner and message to users upon successful login that the user is accessing a U.S. Government information system."

Id = "Main-Req-006"
Text = "For users who unsuccessfully log in after three attempts within 15 minutes, the system widget shall lock the account of the user until an administrator clears the account."

Id = "Main-Req-005"
Text = "The system widget shall allow for three unsuccessful log on attempts by a single user within a 15-minute time period."

{Procedure = "Verify Inactivity Logout Functionality", Step = "1.3"}

{Procedure = "Verify System Widget shows Banner/Message", Step = "1.2"}

{Procedure = "Verify lockout function by entering incorrect user credentials", Step = "1.1"}

{id = "1", Procedure = "Verify Users are Able to Log-In to System Widget", Step = "1", text = "Verify User is able to log in to the system widget"}

Figure 5. Requirements Trace for RMF Model

The MBSE-based model, as illustrated in Figure 5, consolidates these workflows by mapping requirements to artifacts and the corresponding validation steps. The diagram unifies the full compliance workflow showing the functional realization, requirements capture and objective verification in one workflow. The upper tier for the pink boxes are the requirements being met each having a unique identifier linked to a test step. The yellow boxes depicts the function of the use case blocks that show the behavior of the activity diagram steps. The boxes are then linked by dashed UML indicators showing that these requirements are satisfied by the action being linked to them. The green test case steps are showing the elements of a passing test criteria, and which requirements and actions are being satisfied by which test causes. Each paired circular pass/fail badge are required as procedural fields, and the outcome is recorded as a step reference. The bidirectional trace delivers key critical advantages which is a benefit of the MBSE model. Early risk exposure is identified through a lack of requirement linkage or satisfaction which would be immediately visible through the gaps. The change-impact analysis propagates through the model showing the associated functions and gaps in tests which are not meeting the validation and verification of cyber security posture. Lastly, Regulatory credibility and stakeholder clarity is improved through model transparency showing a machine readable traceability determined by a set standard i.e. NIST and CCI. The requirement to enforce session locks after five minutes of inactivity (Main-Req-001) is satisfied by AC-2(1) and verified by tests monitoring inactivity. Similarly, the requirement to display accurate messages (MainReq-004) is linked to AC-2(5) and validated through user interaction tests. This traceability ensures that all requirements are accounted for during design, implementation, and testing. The model also simplifies compliance and auditing by providing clear links between requirements, controls, and validation steps, offering stakeholders a detailed and scalable view of the entire security framework. The comprehensive requirements trace shown in Figure 5 demonstrates the full coverage and accountability of the system. AC control group is mapped out within the ICS security profile within the model elements for their controls, use case, and test procedures. Each component is verified through simulation and analysis creating a comprehensive requirements trace demonstrating full system accountability. The model also robustly updates based on the changes to the system and the addition of new security controls as they map to the applicable requirements of the system under protection and the components of that system. The model provides a real-time evident security posture following the appropriate NIST standards and control families through the RMF framework. The result is a model where the security control are realized and verified.

The adaptability of this framework extends beyond the lock and lockout controls. It can be applied to all other RMF controls control families. The model is built to validate all NIST 800-53 and to be robust and grow with the landscape of cyber security controls. Using MBSE, Human factors for cyber security verification is done using models shown in Figure 5 and validated using generated models such as Figure 3 and Figure 4. The complete model presents a comprehensive and scalable MBSE-based framework to implement and validate security controls within the RMF process. By integrating hierarchical categorization, dynamic relationships, and detailed assessment procedures, this approach not only ensures robust compliance but also enhances operational efficiency and adaptability. While session lock and lockout controls serve as the primary examples, the methodology is readily applicable to all security controls, providing a transformative model for secure system development in regulated and dynamic environments.

Using the MBSE framework above and implementing the methodology for any control group would leverage the following steps:

1. **Define Behavioral and State Requirements**: Establish detailed operational and state conditions necessary to comply with the control.
2. **Define Verification Measures**: Identify and formalize validation criteria to ensure the control's requirements are met.
3. **Identify Actors and Use Cases**: Determine stakeholders and operational scenarios pertinent to the control's implementation.
4. **Elaborate Use Cases**: Develop detailed behavioral models to represent control activities, sequences, or state changes, ensuring clarity and precision.
5. **Develop Requirements Diagram**: Create a consolidated visualization to trace control requirements to their implementation and validation processes.
6. **Simulate Use Cases**: Perform simulations of expected scenarios to validate requirements and refine implementation.

To facilitate consistency and scalability, the template model constructed for each control group would be used the same way that the AC group was created. Once developed, the library can be maintained in a centralized repository with the necessary profile extensions to accommodate custom modeling inputs. By systematically addressing these steps, the MBSE-based framework not only ensures robust compliance, but also provides a structured, repeatable, and scalable methodology for implementing and validating security controls within the RMF process. This integration of hierarchical categorization, dynamic relationships, and detailed assessment procedures represents a paradigm shift in the development of secure systems that ensure adaptability and operational excellence in cybersecurity.

5. Conclusion

The integration of MBSE with the NIST RMF represents a transformative approach to improving the security and operational efficiency of ICS. This research validates the implementation of MBSE as a strategic methodology to address the unique cybersecurity challenges faced by ICS environments while simplifying traditionally cumbersome RMF processes. The model and implementation fill the gap within the cyber security implementation that is experienced by all real-time systems. Using MBSE, organizations achieve greater traceability, efficiency, and adaptability, ensuring that security measures are not only effective but also aligned with operational priorities. Implementing the RMF with MBSE enables seamless integration of cybersecurity implementation, validation, and verification, avoiding erroneous security controls by employing the model to dictate applicable controls. Specifically, verification procedures are further linked to security control groups, triggering the model to apply only the applicable controls needed by the system.

One of the most significant findings of this study is the ability of MBSE to streamline the RMF process by offering a model-driven representation of requirements, controls, and relationships. This structured approach addresses key operational challenges, such as reducing redundancy and providing clear mappings of NIST SP 800-53 controls to system components. The integration of MBSE enables precise alignment of security controls with organizational objectives, ensuring that compliance efforts are efficient and robust. For validation the study focused on a field-relevant ICS scenario to demonstrate the model's practicality. Although the validation is limited to AC-2 the security control group can be created to show any implantation of the control group within 800-53. The only reason why more control groups were not displayed was because it is the same implantation style for other control groups. They are built into the model with validation steps aligning with real-world applications. The implementation of this model would create significant cyber security improvements for ICS networks.

There are also four main aspects of the process that are enhanced by the model-based approach compared to the traditional RMF implementation. Traceability is dramatically enhanced due to all the linkage and artifacts that exist in the model that RMF was not previously able to maintain. The MBSE model inherently provides the visual and modular framework needed to directly link the controls to the validation procedures. This traceability not only streamlines audits but identifies compliance gaps in the preplanning stages of system development. The second aspect is that the model can simulate behavioral modeling through behavioral diagrams. The ability to predict the use case behaviors of a system before implementing security controls enables the mitigation of risk, the identification of vulnerabilities, and the assessment of control effectiveness based on the specific system being implemented. This proactive approach enables organizations to identify vulnerabilities and assess the effectiveness of controls before implementation, resulting in a stronger security posture. The third important aspect of the approach is that MBSE automates the creation of critical RMF artifacts, such as System Security Plans (SSPs) and Security Assessment Reports (SARs). By linking RMF controls to operational workflows, MBSE reduces the manual effort traditionally associated with compliance, enabling organizations to achieve ATO more efficiently. Lastly, due to the modularity of MBSE, the implementation is robust and scalable. The implementation can keep pace with evolving security requirements and maintain the ATO without having to recreate the packages required to transition a system through RMF stages 1 to 7. This ensures that, regardless of changes in the cybersecurity landscape, the system remains relevant and provides a proper cybersecurity evaluation.

5.1. Limitations of MBSE

Even though MBSE is an ideal implementation to combat the problem of RMF within industrial control system implementations it is important to identify the limitations of the model and create future innovations. The significant challenges states with the complexity of creating and maintaining detailed system models for large scale industrial environments. The RMF model demonstrated within this paper is the implementation of the selected standards and controls to implement RMF and cyber security controls on to a system. There needs to be a system model to implement these controls on for the implementation to be successful. The development of a full SysML model of an ICS with hundreds of devices, sensors, networks and processes would demand proper expertise and time. The team would also need to be well versed within MBSE and how to properly integrate the RMF model within their enviornment creating their RMF implementation. The model would only be as good as the designer's ability to recreate the enviornment within MBSE to integrate the built RMF model, and this would require interdisciplinary knowledge which would be difficult to transition into for implementation. while MBSE offers a powerful framework for unifying system design and security, practitioners must be mindful of these potential drawbacks such as complexity, learning curve, tool integration, and maintenance effort and address them through careful planning, training, and tool support to fully realize the benefits of MBSE in RMF implementation for industrial control systems

5.2. Future Work

Building on the current research, future work could explore the development of a classification and dependency framework for network equipment that supports automated RMF analysis. This framework would classify devices based on defined security properties, such as hardware-enforced versus software-enforced security features, and maintain a selective list of key dependencies. The existing network landscape of the system would be able to tag the traffic traversing the system, and by means of traffic analysis, a model could be generated to automatically feed into this MBSE RMF implementation. Such a classification system could simplify the RMF analysis for complex systems, enabling system architects to differentiate between varying risk profiles associated with hardware and software implementations. Leveraging Software Bill of Materials (SBOM) data or a tailored dependency list, the framework could automate the identification of devices potentially compromised by newly published threats. This implementation would very easily alleviate the need to create system models and have the models be created through the traffic analysis process. Leveraging machine learning tools this could automatically be fed into a SysML model. Specific hardware and software combinations could also trigger the procedures that would need to be implemented for system verification and validation. Using this process, it could be seen that integrating the model out of band from the system in the future, creating a real-time cyber auditing system to mitigate risks through real-time resolution.

Extending this concept to include consistent tagging of device features, dependencies, and vulnerabilities would improve traceability and support Realtime risk assessment. This could address the gaps identified in previous work, where system architects struggled to quantify differences in risk profiles between various security mechanisms. A robust device classification model could offer a unified approach to assessing similar security environments, providing actionable insights, and ensuring that security strategies remain dynamic and responsive to emerging threats. Future research could further refine and extend the capabilities of MBSE in RMF applications, creating a comprehensive toolset to secure critical systems by creating a system that can leverage classification, dependency mapping, and automated analysis.

Corresponding author

Alexander Gampel
alex.gampel@gwu.edu

Acknowledgements
Not applicable.

Funding
No funding.

Contributions
A.G.S; T.E; Conceptualization, A.G.S; T.E; Investigation, A.G.S; T.E; Writing (Original Draft), A.G.S; T.E; Writing (Review and Editing) Supervision, A.G.S; T.E; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] Ayub, A., et al. (2023). *How are industrial control systems insecure by design? A deeper insight into real-world programmable logic controllers* (Vol. 21). Los Alamitos: IEEE.
[2] Aleksandraviciene, A., & Morkevicius, A. (2021). *MagicGrid book of knowledge*. Kaunas: Vitae Litera.
[3] Amaghionyeodiwe, L. A. (2017). Risk Management Framework (RMF) and the implementation challenges. *Proceedings of the Northeast Business & Economics Association*.
[4] Jillepalli, A. A., Sheldon, F. T., de Leon, D. C., Haney, M., & Abercrombie, R. K. (2017). Security management of cyber-physical control systems using NIST SP 800-82r2. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (p. 186). IEEE.
[5] Al-Maari, A. A., Abdulnabi, M., Nathan, Y., Ali, A., Ali, U., & Khan, M. (2025). Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods. *Engineering, Technology & Applied Science Research*, *15*(3), 22287-22294.
[6] Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. *Engineering, Technology & Applied Science Research*, *15*(2), 21279-21283.
[7] Chan, A. (2023, April 28). Can AI be used for risk assessments? *ISACA*. https://www.isaca.org/resources/news-and-trends/industry-news/2023/can-ai-be-used-for-risk-assessments
[8] Cherdantseva, Y., et al. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27.
[9] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.
[10] Cybersecurity and Infrastructure Security Agency (CISA). (2024, February 29). Threat actors exploit multiple vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways — CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
[11] Chockalingam, S., Pieters, W., Teixeira, A., & Gelder, P. H. A. J. M. (2017). Bayesian network models in cyber security: A systematic review. In *Cyber Security and Critical Infrastructure Protection* (pp. 105–124). Springer. https://doi.org/10.1007/978-3-319-70290-2_7
[12] Vavra, C. (2022, March 4). Consequence-driven ICS risk management. *Control Engineering*. https://www.controleng.com/articles/consequencedriven-ics-risk-management/
[13] Eckhart, M., et al. (2023). QualSec: An automated quality-driven approach for security risk identification in cyber-physical production systems. *IEEE Transactions on Industrial Informatics*, *19*(4), 5870–5881.
[14] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, *22*(4), 1448.
[15] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors*, *22*(6), 2112.
[16] Holm, H., Sommestad, T., Ekstedt, M., & Nordström, L. (2013). CySeMoL: A tool for cyber security analysis of enterprises. In *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)* (pp. 1–4). https://doi.org/10.1049/cp.2013.1077
[17] Holmes, A. (2021). Exploring the challenges of the Risk Management Framework implementation for cybersecurity professionals. *ProQuest Dissertations Publishing*.
[18] INCOSE. (2015). *Systems engineering handbook: A guide for system life cycle processes and activities*.
[19] Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. *International Journal of Critical Infrastructure Protection*, *46*.
[20] Lapon, J., et al. (n.d.). A SysML extension for security analysis of industrial control systems. *Electronic Workshops in Computing*. BCS, The Chartered Institute for IT.
[21] Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., & Chatzitheodoridis, F. (2024). The role of artificial intelligence technology in predictive risk assessment for business continuity: A case study of Greece. *Risks*, *12*(2), 19. https://doi.org/10.3390/risks12020019
[22] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022). *Guide to operational technology (OT) security* (NIST SP 800-82r3). National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-82r3
[23] Langner, R. (2011). *Stuxnet: Dissecting a cyberwarfare weapon* (Vol. 9). Los Alamitos: IEEE.
[24] Landau, S. (2008). *Security and privacy landscape in emerging technologies* (Vol. 6). Los Alamitos: IEEE.
[25] Model-based security engineering for cyber-physical systems: A systematic mapping study. (2017). *Information and Software Technology*, *83*, 116–135. https://doi.org/10.1016/j.infsof.2016.11.004
[26] National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations* (SP 800-37r2). https://doi.org/10.6028/nist.sp.800-37r2
[27] Ross, R. (n.d.). *NIST special publication 800-53: Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology.
[28] Papamichael, M., Dimopoulos, C., Boustras, G., & Vryonides, M. (n.d.). Performing risk assessment for critical infrastructure protection: A study of human decision-making and practitioners' transnationalism considerations. *International Journal of Critical Infrastructure Protection*.
[29] Roberts, P. (2023, February 14). Cyberattacks on industrial control systems jumped in 2022. *The Security Ledger with Paul F. Roberts*. https://securityledger.com/2023/02/cyberattacks-on-industrial-control-systems-jumped-in2022

[30] Ramos, A. L., Ferreira, J. V., & Barceló, J. (2012). Model-based systems engineering: An emerging approach for modern systems. *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews, 42*, 101–111.
[31] Romero-Faz, D., & Camarero-Orive, A. (2017). Risk assessment of critical infrastructures – New parameters for commercial ports. *International Journal of Critical Infrastructure Protection, 18*, 50–57. https://doi.org/10.1016/j.ijcip.2015.06.009
[32] Ross, R. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (Special Publication [NIST SP]). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2
[33] Setola, R. (2024). It is the time, are you sufficiently resilient? *International Journal of Critical Infrastructure Protection, 46*, Article 100710. https://doi.org/10.1016/S1874-5482(24)00051-9
[34] Shaked, A. (2023). A model-based methodology to support systems security design and assessment. *Journal of Industrial Information Integration, 33*, 100465. https://doi.org/10.1016/j.jii.2023.100465
[35] Smart electrical grids more vulnerable to cyber attacks. (2017, August 16). *ECN*. https://www.proquest.com/trade-journals/smart-electricalgrids-more-vulnerable-cyber/docview/1929257720/se-2
[36] Stockman, M., Dwivedi, D., Gentz, R., & Peisert, S. (2019). Detecting control system misbehavior by fingerprinting programmable logic controller functionality. *International Journal of Critical Infrastructure Protection, 26*, 100306.
[37] Upadhyay, D., Ghosh, S., Ohno, H., Zaman, M., & Sampalli, S. (n.d.). Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. *International Journal of Critical Infrastructure Protection*.
[38] Vasan, D., Alqahtani, E. J. S., Hammoudeh, M., & Ahmed, A. F. (2024). An AutoML-based security defender for industrial control systems. *International Journal of Critical Infrastructure Protection, 47*, 100718. https://doi.org/10.1016/j.ijcip.2024.100718
[39] Weilkiens, T. (2016). *Systems engineering with SysML/UML: Modeling, analysis, design*.
[40] Knowles, W., Prince, D., Hutchison, D., Pagna Disso, J. F., & Jones, K. (2015). A survey of cybersecurity management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*(C), 52–80.
[41] Wilson, B., Arena, M. V., Mayer, L. A., Heitzenrater, C., Mastbaum, J., & Connolly, K. J. (2022). *A methodology for quantifying the value of cybersecurity investments in the Navy*. RAND Corporation. https://www.rand.org/pubs/researchreports/RRA13.html
[42] Roudier, Y., & Apvrille, L. (2015). 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)* (pp. 655–664).
[43] Yousaf, A., Amro, A., Kwa, P. T. H., Li, M., & Zhou, J. (2024). Cyber risk assessment of cyber-enabled autonomous cargo vessel. *International Journal of Critical Infrastructure Protection, 46*, 100695. https://doi.org/10.1016/j.ijcip.2024.100695

Biographies

Alexander Gampel is a doctoral candidate with GWU's Systems Engineering and Applied Sciences department with an area of study in System's Engineering MBSE and Cyber security framework implementation. He is a cyber security professional working for the navy within the Cyber Engineering & Digital Transformation directorate (SEA 03) alex.gampel@gwu.edu; https://orcid.org/0009-0000-1268-3580

Tim Eveleigh developed and teaches GWU's Model Based Systems Engineering and Enterprise Systems Engineering and Architecting courses at the masters and doctoral levels. He is director for Systems Engineering for Orano Enrichment USA's Project Ike Nuclear Enrichment plant and brings 45 years of experience in defense and intelligence community systems and enterprise engineering endeavors eveleigh@gwu.edu; https://orcid.org/0000-0003-1647-1969