Proceedings of the ASME 2024
International Design Engineering Technical Conferences and
Computers and Information in Engineering Conference
IDETC-CIE2024
August 25-28, 2024, Washington, DC

DETC2024-143713

IMPLEMENTING THE RISK MANAGEMENT FRAMEWORK FOR ADDITIVE MANUFACTURING SECURITY: A MODEL-BASED APPROACH

Duncan W. Gibbons[1,2,*], Joshua Lubell[2], Paul Witherell[2]

[1]Stellenbosch University, Stellenbosch, South Africa, 7599
[2]National Institute of Standards and Technology, Gaithersburg, MD, 20899

ABSTRACT

Metal additive manufacturing machines are complex and inherently digital and often cyber-physical systems. As the adoption of this manufacturing technology increases and it becomes increasingly industrialized, concerns about security are evermore prevalent. Both cyber and non-cyber related attacks on critical infrastructure such as additive manufacturing production systems are causes for concern for industry and government. Both the public and private sectors need to focus on securing their information systems to reduce the risk of security attacks and their adverse effects. This research aims to apply the National Institute of Standards and Technology's Risk Management Framework to the metal additive manufacturing production scenario. The Risk Management Framework defines a rigorous, yet flexible and repeatable, process for managing security risk. A model-based assessment approach is proposed to leverage the digital nature of this manufacturing technology. A case study is performed to demonstrate this approach for a commercial laser powder bed fusion machine in its operating environment. This case study focuses on the technological security risks. This study demonstrates how a model-based approach maximizes the benefits of the Risk Management Framework by improving information and decision traceability for addressing metal additive manufacturing security risks.

Keywords: Additive Manufacturing, Information Security, Risk Management

NOMENCLATURE

AM Additive Manufacturing
DoD Department of Defense
FMEA Failure Modes and Effects Analysis
IDEF0 Integrated DEFinition for Function Modeling
LPBF Laser Powder Bed Fusion
MBSE Model-Based Systems Engineering
NDT Non-Destructive Techniques
NIST National Institute of Standards and Technology
RAAML Risk Analysis and Assessment Modeling Language
RMF Risk Management Framework
SoI System of Interest
SysML Systems Modeling Language
UAF Unified Architecture Framework

*Corresponding author: duncan.gibbons@nist.gov
May 23, 2024.

1. INTRODUCTION

Additive manufacturing (AM), commonly called 3D printing, is the joining of materials to build parts layer by layer from 3D model data [1]. AM is an inherently digital manufacturing technology and process. AM machines are systems that transform data and physical material into a product and its associated data. Such digitally connected and often cyber-physical systems are prime targets for cyber threats and attacks. AM machines, like other digital manufacturing equipment, often communicate with other digital or cyber information systems. For example, an AM machine may receive build files, transmit build reports and monitoring data, or provide machine health information to a diagnostics application. Unlike other digital manufacturing technologies, AM's layer-by-layer manufacturing process enables newfound design complexity and business models. These benefits, however, also introduce new opportunities for adversaries to attack AM machines and processing workflows [2].

AM's vulnerabilities to attacks have been shown to be exploitable, yet the state of AM security is lacking. Yampolskiy et al. [3] identified AM attack vectors of concern including supply chain attacks, software and firmware updates, code injections, modification of 3D models, and manufacturing process specifications [4]. A 2021 United States Department of Defense (DoD) Inspector General audit [5] reported that AM systems at five DoD sites did not adequately protect computer-aided design data confidentiality and integrity. The audit determined that the sites had incorrectly assumed that air gapping the systems made

them "standalone". Instead, because the AM systems consumed computer-aided design data, used that data to manufacture parts, and generated a lot more data during the manufacturing process, they should have been treated as "information systems" with the appropriate security controls implemented for protecting that information. In a subsequent analysis of the DoD Inspector General report, Cotteleer et al. [6] illustrated how DoD could have used the Risk Management Framework (RMF), introduced in Sec. 2.1, to correctly establish the AM systems' security requirements. A 2020 survey of the AM industry highlighted the increasing attention being provided to the security aspects of AM production [7]. This survey concluded that the current state of the AM industry is not sufficiently prepared to detect or prevent AM-specific attacks [7]. Of the surveyed AM users, only 41% had dedicated AM security programs in place [7].

This research proposes a repeatable methodology for applying the National Institute of Standards and Technology (NIST) RMF concepts and principles to metal AM production systems. Specifically, a model-based approach is developed to standardize the RMF *prepare* task for metal laser powder bed fusion (LPBF). Although security risk management can be applied to multiple system dimensions and at various levels, this research is scoped to the AM machine lifecycle from procurement through to production use and the directly related product aspects. Additionally, only technological security risks are addressed. Other risks related to political, environment, social, economic, and legal aspects, although important, are beyond the scope of this study. The system of interest (SoI) in this research is the LPBF machine, a cyber-physical system.

2. BACKGROUND

2.1 Risk Management & Security

Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [8, 9]. Risk measures the extent to which an asset is threatened by a potential circumstance or event [8]. Risks are related to, but not synonymous with, threats. A threat is a potential cause of unacceptable asset loss and the undesirable consequences or impact of such a loss [9]. Risk measures the extent to which a potential circumstance or event threatens an asset. Risk-based security is a process for identifying, assessing, and responding to risk with respect to a system and the information the system produces, consumes, or transmits [8]. A systems approach to risk management considers a specific system, its assets and associated information, and potential threats that exist in the system's operating environment. The goal is to reduce risk to a level acceptable to the organization and society as a whole.

The NIST RMF is aimed at federal organizations and their associated information systems, both digital and non-digital [10]. The NIST series of risk management publications are aligned with international standards such as ISO 31000 and the ISO/IEC 27000 series, with the aim of extending the concepts and principles of these standards specifically for United States government organizations and their contractors [11]. The RMF provides a repeatable process for managing risk that is applicable to any type of organization and adaptable to new threats and changes to organization mission or business functions. The RMF process consists of seven steps, described in Table 1, with each step containing multiple tasks. The first seven tasks of the *Prepare* step are performed at the organizational level. The remaining *Prepare* tasks, and all tasks belonging to steps other than *Prepare*, are performed at the system level.

TABLE 1: Risk Management Framework steps [10]

Step	Description
Prepare	*Prepare* the organization/system for security and privacy risk management
Categorize	*Categorize* the system and information processed, stored, and transmitted based on an impact analysis
Select	*Select* the set of security controls to protect the system based on risk assessment(s)
Implement	*Implement* the controls and document how they are deployed
Assess	*Assess* to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Make a risk-based decision whether to *authorize* the system (to operate)
Monitor	Continuously *monitor* control implementation and risks to the system

2.2 Metal AM Security Risks

Metal AM production has become a popular technology for the manufacture of high-value structures in critical industries such as aerospace and medical [12, 13]. This technology allows for the design and manufacture of computer-generated and digital designs that can be optimized to save material and produce lightweight structures. Metal AM technologies typically require metal feedstock in either powder or wire forms.

A particularly useful benefit of metal AM production is its ability to facilitate distributed manufacturing whereby design and manufacturing operations can be distributed over geographic regions and even between multiple organizations. This capability is beneficial to the defense and mining industries where replacement parts are often required in remote locations and with short lead times. This also allows for reduced inventory stockpiles as parts can be manufactured when needed.

Metal AM machines are classified as complex cyber-physical systems consisting of multiple subsystems and that interact and interoperate with internal and external entities. Figure 1 illustrates the metal AM production scenario and highlights some of the entities internal and external to the AM machine's environment of operation that can be sources of security risks and attacks [4]. Internal entities appear inside the box with rounded corners in Figure 1, and external entities appear outside of the box. The powder-based AM machines such as LPBF systems come with additional complexity. These systems have many parameters and settings that need to be understood and controlled to ensure quality products are manufactured. These parameters and settings vary between the different machine makers and models, although

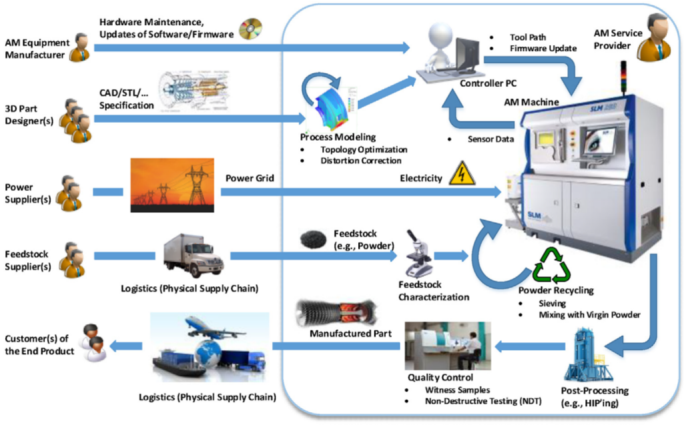

FIGURE 1: Potential sources of AM security attacks. From Yampolskiy et al. [4].

it is said that there are over 50 key process parameters that are critical to quality [14]. Many of these are digital parameters that specify instructions for the machine control system. Additional risks and cybersecurity challenges are added when in situ monitoring is used and digital twin concepts are applied [15].

In a recent survey of attacks on AM systems, Milaat and Lubell [16] include the following sabotage attacks whose methods are unique to LPBF technology. By altering laser power parameters in a build file, Carrion et al. [17] were able to selectively modify layer thickness. The resulting manufactured part's quality was adversely impacted, yet the induced defect was not detectable by non-destructive techniques. Graves et al. [18] were able to degrade a part's mechanical properties (difficult to detect using non-destructive techniques) by attacking the power delivery system during the part's manufacture. Zinner et al. [19] manipulated the flow of shielding gas to an LPBF machine's build chamber, resulting in reduced part quality. This was the first example to the authors' knowledge of an attack whose adverse effects exhibit stochastic fluctuations. Such attacks, although challenging for the attacker to execute successfully, are difficult to detect.

3. RESEARCH METHODOLOGY

A systems engineering methodology was applied to address the requirements of the NIST RMF framework for the *Prepare* step. The applicability of a systems engineering approach for risk management and privacy engineering is justified by the NISTIR 8062 [20]. The NIST RMF does not mandate tools, techniques, or approaches for performing risk management activities and is agnostic to the implementation thereof. The NIST RMF does not impose an ordering of tasks within a step or workflow, although it does suggest certain inputs and outputs to tasks. This research used the sequence of tasks presented in Figure 2 as its workflow.

The NIST RMF was selected as the focal risk framework for this research instead of other security frameworks from international standards organizations because the RMF is widely used within the United States government and voluntarily used by non-federal and private sector entities worldwide [21]. The United State Office of Management and Budget published a circular on managing information as a strategic resource stating that federal

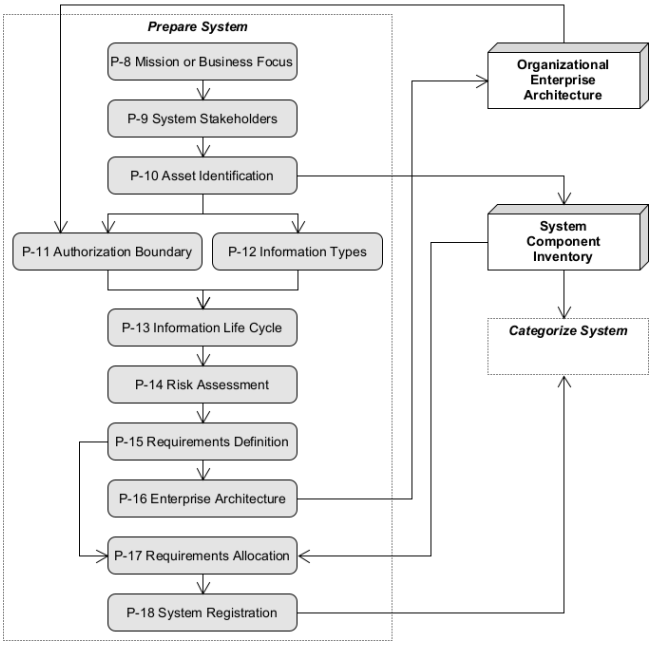

FIGURE 2: Workflow for preparing a system per the NIST RMF.

agencies shall consult NIST publications as part of their information risk management strategy [8]. In addition, these agencies are required to develop and maintain an enterprise architecture that defines baselines, targets, and a transition plan [8]. Furthermore, we note that the RMF does not exist in isolation. The RMF's system life cycle process and use of systems engineering terminology are derived from ISO/IEC 15288, a systems engineering standard covering processes and life cycle stages [22]. Additionally, the RMF process is compatible with any of the standardized catalogs of security controls.

Our research methodology utilizes standardized modeling language notations to represent outputs of some of the RMF *Prepare* tasks. This is consistent with, but not a requirement of the RMF. The RMF guidance stresses *procedure* by emphasizing the risk management process (steps and tasks comprising each step) and *accountability* by assigning roles and responsibilities. Although it recommends outputs for task (some of which are suggested as inputs to other tasks), the RMF leaves it up to organizations to choose their own formats for documenting task outputs. In practice, these formats are often spreadsheets or word processor templates. Such output formats lack a formal syntax for representing key system elements and their relationships. By representing outputs in standardized languages, our approach enables formal notations with agreed-upon semantics. Such formality is necessary for a better understanding of risk management for AM. It can also lead the way toward better tools for automating the risk management process and documenting RMF outputs [23].

Systems theory focuses on the arrangement of relationships between parts or elements of a system and its environment. The relationships and interfaces between parts is where security threats and attacks are focused. Hence addressing the prob-

lem by applying systems thinking principles and focusing on the interfaces and integration of the LPBF machine with its wider operating environment is a fitting approach. All systems in the real world are open systems and analysts need to account not only for the parts of the system but also the environment the system is operating within. Systems engineers are faced with the challenge of justifying to how many levels wider and within they should design and analyze a system. For this research the LPBF machine is analyzed to one level of abstraction above (context).

Dandashi [24] notes that model-based and analytical approaches to risk analysis provide consistent and repeatable assessments. The information system, in this case a cyber-physical system, was modeled using the open-source model-based systems engineering (MBSE) software Papyrus 6.6.0 in accordance with the Systems Modeling Language (SysML) 1.6 specification [25]. SysML is a systems modeling language and is beneficial for modeling system architectures, linking systems and components, defining use cases, and identifying stakeholders. Information types and flows were modeled using AIØ WIN in accordance with the Integrated DEFinition for Function Modeling (IDEF0) language and notation [26]. IDEF0 diagrams focus on activities and information flow and are easy to interpret. IDEF0 diagrams distinguish between an activity's inputs, the conditions needed for its transformation to occur, and mechanisms specifying how the transformation is executed. This distinction helps stakeholders to better understand the activity [27]. The risk assessment was conducted in accordance with the The Risk Analysis and Assessment Modeling Language (RAAML) [28]. This language was specifically created to be conformant with SysML and provides a unique means for incorporating risk in the systems development lifecycle. To demonstrate this approach, a case study was performed focusing on a commercial LPBF machine and its operating environment.

4. RESULTS

This analysis focuses on the LPBF machine (the SoI) and technology as the focal information system, not on the role of the enterprise or of the machine within the enterprise. The primary concern with regards to security risk for LPBF machines is related to product quality. The concern this analysis aims at addressing is that LPBF machines can be compromised or attacked resulting in reduced or altered product quality, which in turn can lead to poor product safety. A secondary concern is the loss of intellectual property whereby critical information is accessed by an outside entity. Each subsection heading corresponds to a *Prepare* task from Figure 2. The italicized text below each subsection heading is a brief task description from [10].

4.1 TASK P-8: Mission or Business Focus

Identify the missions, business functions, and mission/business processes that the system is intended to support.

Figure 3 presents the use case diagram for the LPBF machine. Use cases and actors are identified for the lifecycle of the system. These use cases are representative of what a production organization can feasibly control. Other use cases and activities that occur before the machine arrives at the facility or after the machine is removed from the facility are excluded from the scope of this analysis.

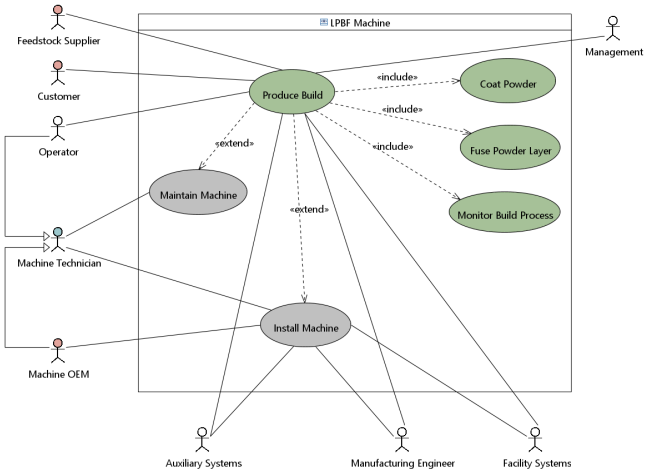

FIGURE 3: ***LPBF Machine Use Case Diagram***

The mission of the system is driven by its use case/s. The primary mission of the LPBF machine is to *Produce Build/s*, as highlighted in green as the main use case in Figure 3. The production of LPBF builds can be performed for different reasons, be it for prototyping, qualification, or industrialized production. It shall be noted that although the impact of a threat at these different phases of production may differ, the threat remains the same. The initial risk assessment should be performed before the LPBF machine is installed in a facility, and ideally before installation qualification is performed [29].

4.2 TASK P-9: System Stakeholders

Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

The system stakeholders are also identified in the use case diagram in Figure 3. Stakeholders, termed actors in this case, can exhibit multiple roles. For instance, an *Operator* may or may not also be a *Machine Technician*. Each role is associated with different use cases and can pose different security risks to the system. Primary actors are actors connected to the primary use case/s of the system. Actors are also categorized by their relationship to the wider enterprise. Internal actors are identified by the white stick figures in Figure 3, whereas external actors are highlighted in red.

4.3 TASK P-10: Asset Identification

Identify assets that require protection.

An asset is defined as an item, tangible or intangible, that provides some value to the organization [9]. The primary assets of concern are the LPBF machine and its produced material. These assets interact with other assets in the facility that can be sources of risk. The interaction with these assets changes over the lifecycle of the LPBF machine. Figure 4 presents a block definition diagram with the external systems and entities that make up the system context. All these assets are potential sources of security risk and need to be assessed accordingly. The

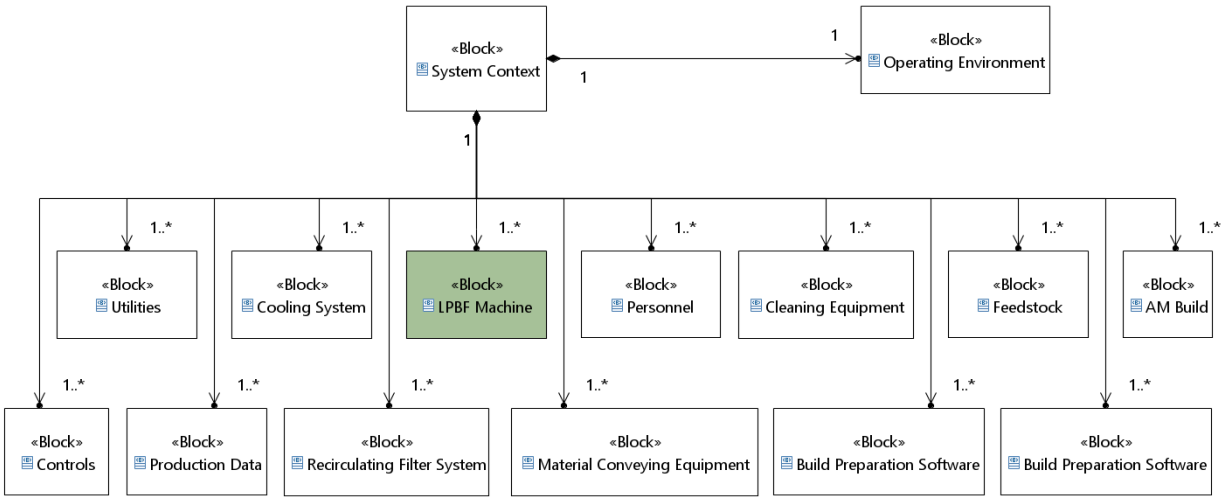

FIGURE 4: ***Block Definition Diagram of External Entities.***

LPBF machine is made up of subsystems and critical components that are required for the system to function correctly. These assets are attractive attack targets. Such subsystems include the machine control system, power supply, powder dosing system, laser system, process chamber, and monitoring system/s.

4.4 TASK P-11: Authorization Boundary

Determine the authorization boundary of the system.

The system authorization boundary is seen as the scope of protection for the SoI [10]. This is modeled using an internal block diagram to model the SoI in its context and operating environment. Figure 5 presents the internal block diagram with the SoI highlighted in green. Interfaces with the machine are modeled using ports and these are connected to the relevant external entities and systems. These interfaces are modeled with directionality or as generic interfaces in the case of the interfaces with the *Operating Environment*.

The NIST RMF notes that defining clear authorization boundaries is especially important when external providers are responsible for system operations or maintenance [10]. This is often the case with LPBF machines, whereby the machine original equipment manufacturer performs periodic maintenance and calibration activities. The *Personnel* external entity represents all human type entities that interact with the *LPBF Machine*.

4.5 TASK P-12: Information Types

Identify the types of information to be processed, stored, and transmitted by the system.

To identify the information types to be processed, stored, or transmitted by the SoI, the activities and processes that the SoI performs need to be modeled. The core functions of the LPBF machine are modeled in the IDEF0 diagram in Figure 6. The focus of this IDEF0 model is on the activities and their interaction with the data items. An additional *Recondition Powder* activity is modeled to represent the reconditioning of powder for reuse in subsequent builds. This activity is performed using the *Material Conveying Equipment* which interfaces with the LPBF machine through the *ChamberDoor*, as modeled in the previous figures. This represents the activities and information associated with the AM work cell. The information or data types that are categorized as critical digital data flows related to the product or part are color-coded in red, the physical data flows related to the material are color-coded blue, resources are color-coded magenta, and additional data items are color-coded black. Red and blue data items are the most critical in terms of part or product quality and safety.

4.6 TASK P-13: Information Lifecycle

Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.

The data items modeled in the IDEF0 diagram in Figure 6 are used to create a data flow diagram whereby the focus is on the data items and how they are processed, stored, or transmitted by the SoI. This diagram represents the transformation of digital and physical inputs to the AM work cell into outputs. This is representative of when the SoI is in operation and is manufacturing parts. Figure 7 illustrates how the data is transformed and changes state. This diagram includes both the physical and digital threads related to the AM product, which in terms of the AM work cell is the *P.2.2: AM Build*. All such data items are created or generated by physical entities, in this case a cyber-physical system. Critical data items that occur within the data model presented in Figure 7 are defined in Table 2. These items are critical to the quality and conformance of AM parts and products.

4.7 TASK P-14: Risk Assessment

Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.

To illustrate how the system model can be leveraged for performing risk assessments, a risk assessment is performed on one of the system inputs, the *Scan Strategy*. This data item is isolated and its dependencies are identified as presented in Figure 8. A failure modes and effects analysis (FMEA) is performed for one cause and these results are modeled in accordance with RAAML. The element in orange identifies the FMEA item and is associated

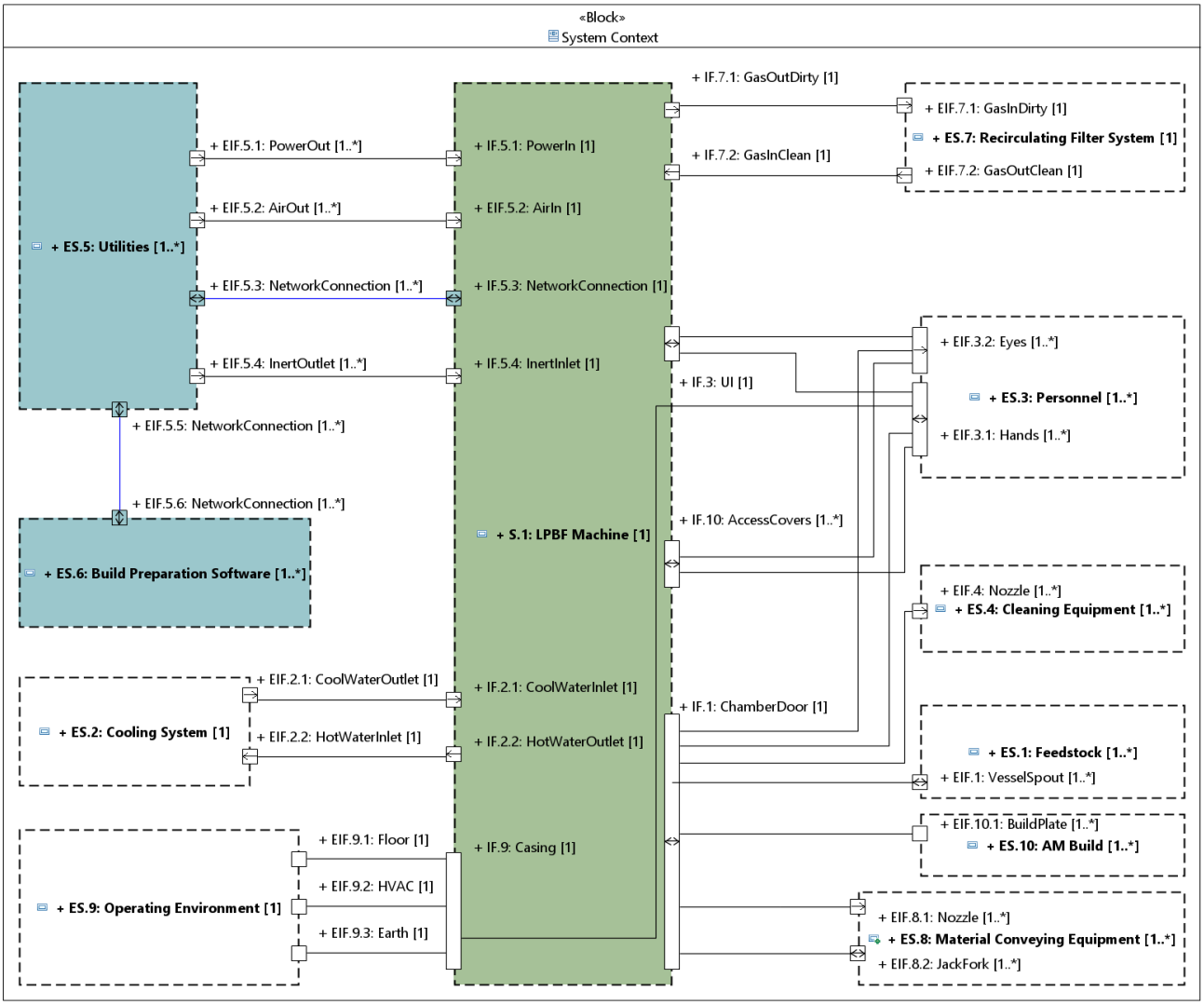

FIGURE 5: ***Internal Block Diagram of Machine Interfaces.***

with the *Scan Strategy*, the elements in red are components of the FMEA analysis and identify the different aspects of a FMEA analysis. An altered build file can result from a threat that originates either internally or externally to the enterprise. This failure mode can be caused by an intentional, i.e. malicious, or unintentional action.

Risk assessments should not be performed one time only. Instead they should be performed periodically and when changes to the SoI occur or are being planned. With digital models of the SoI developed and implemented, the burden of such risk reassessments is greatly reduced. These digital models can also facilitate configuration management principles and automate cause and effects analyzes, as illustrated by the model-based FMEA in Figure 8.

4.8 TASK P-15: Requirements Definition

Define the security requirements for the system and the environment of operation.

This task requires analysts to define requirements to control the risks identified during the previous task. Not all risk may require security and privacy requirements. If the risk is low enough that it can be accepted, security and privacy requirements may not be needed. For the risk assessment presented in Figure 8, a requirement is defined that requires the verification of all build files used in a production setting. This requirement is driven by the cause of a potentially altered build file. Build file verification can include toolpath simulation, review by an engineer, or computer-aided manufacturing quality checks. It shall be noted that additional requirements can be defined that apply to systems outside the context of this SoI such as additional security requirements for the enterprise IT systems.

4.9 TASK P-16: Enterprise Architecture

Determine the placement of the system within the enterprise architecture.

An enterprise architecture is a multi faceted model that defines the strategic information of the enterprise and can be modeled by conforming to architecture frameworks such as the Unified Architecture Framework (UAF) [30]. These architectures address the enterprise from a higher level of abstraction, typically the sys-

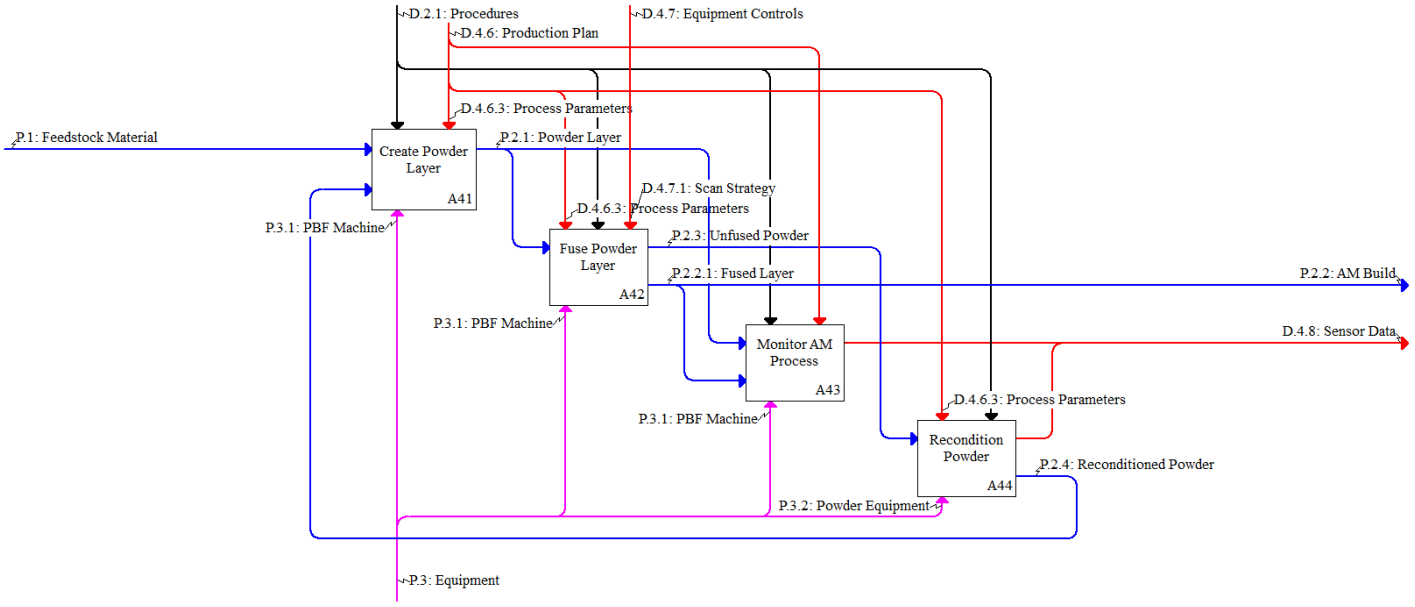

FIGURE 6: ***A4: Manufacture AM Workpiece***

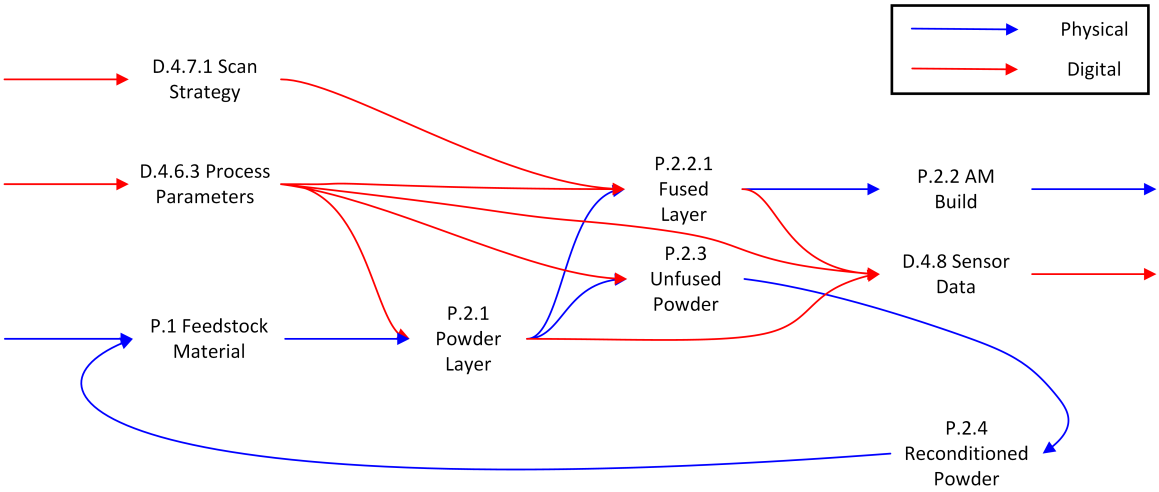

FIGURE 7: Physical and Digital Thread for ***A4: Manufacture AM Workpiece***

tem of systems perspective, and define missions, requirements, and links between the enterprise systems.

The placement of the LPBF machine is located within a manufacturing work cell and is modeled in the use case and block definition diagrams in Figures 3 and 4. The actors and external enterprise assets that interact with the SoI are defined in these diagrams. The architectural models presented in this paper address the physical, functional, and information aspects of the SoI and its links, interactions, and associations to other enterprise assets. These models contain information that can be generalized to LPBF machines, and to a certain degree, other AM technologies.

4.10 TASK P-17: Requirements Allocation

Allocate security and privacy requirements to the system and to the environment of operation.

The requirement defined during P-15 is allocated to the *Build Preparation Software* as illustrated in Figure 8. This allocation applies to the wider environment of operation of the SoI. An altered build file is a critical risk and should be flagged before the build file is sent to the LPBF machine.

4.11 TASK P-18: System Registration

Register the system with organizational program or management offices.

Registration of the SoI with the organizational program is authorized by the *Management* stakeholder modeled in the use case diagram in Figure 3. Authorities and use case scenarios are defined in the use case diagram. This information is important for informing the organization of the purpose and key characteristics of the system that can be detailed in the relevant management system (e.g. enterprise resource planning systems) [10]. The

TABLE 2: Critical Digital and Physical Data Items for *A4: Manufacture AM Workpiece*

Data ID	Name	Criticality
P.1	Feedstock Material	Feedstock quality affects produced material quality.
P.2.1	Powder Layer	The powder layer affects the quality of the produced material.
P.2.2	AM Build	The AM build is what is processed into a functional part.
P.2.2.1	Fused Layer	The fused layer that forms a part over successive layers within the build.
P.2.3	Unused Powder	Powder that can be reclaimed and reconditioned for subsequent production runs.
P.2.4	Reconditioned Powder	Powder that has been reconditioned and used as feedstock for production.
D.4.6	Production Plan	Decomposed by D.4.6.3.
D.4.6.3	Process Parameters	Process parameters provide instructions for the LPBF machine to perform operations.
D.4.7	Equipment Controls	Decomposed by D.4.7.1.
D.4.7.1	Scan Strategy	Specifies where the LPBF machine shall fuse material to form a part.
D.4.8	Sensor Data	Contains information about the AM process that can be used to evaluate material conformance.

system shall not be placed online until it has been authorized (see Table 1).

5. DISCUSSION

The use of MBSE tools and techniques for performing the NIST RMF *Prepare* step and associated tasks has proved beneficial in various ways. This approach facilitates the development of an authoritative definition of the SoI and its operating environment. When standardized modeling languages and notations are used, communication amongst stakeholders, both humans and computers, is improved. System vulnerabilities can be identified and their effects analyzed offline in the model-based environment as opposed to online in the real world, ultimately saving time, reducing costs, and improving security [31] [32]. This approach also facilitates configuration management and information reuse. Reusable information and models can be instantiated for other applications and even other systems that exhibit similarities. Table 3 maps the NIST RMF *Prepare* tasks to MBSE modeling techniques and diagrams. Some of these techniques and diagrams can be used to address multiple tasks, as demonstrated in this research. The NIST RMF states that organizations should maximize the use of automation when performing the RMF steps and tasks [10]. The approach presented in this paper allows for such automation in terms of authorization package preparation, cause and effects analyzes, definition and allocation of controls, and continuous risk assessments and monitoring throughout the lifecycle of the SoI.

Oates et al. [33] notes that it is difficult to preempt attacks that rely on subverting the design of the system, such as supply chain attacks. The approach presented in this research aims to address these supply chain attacks whereby security risk are analyzed not only for the system itself, but the wider system

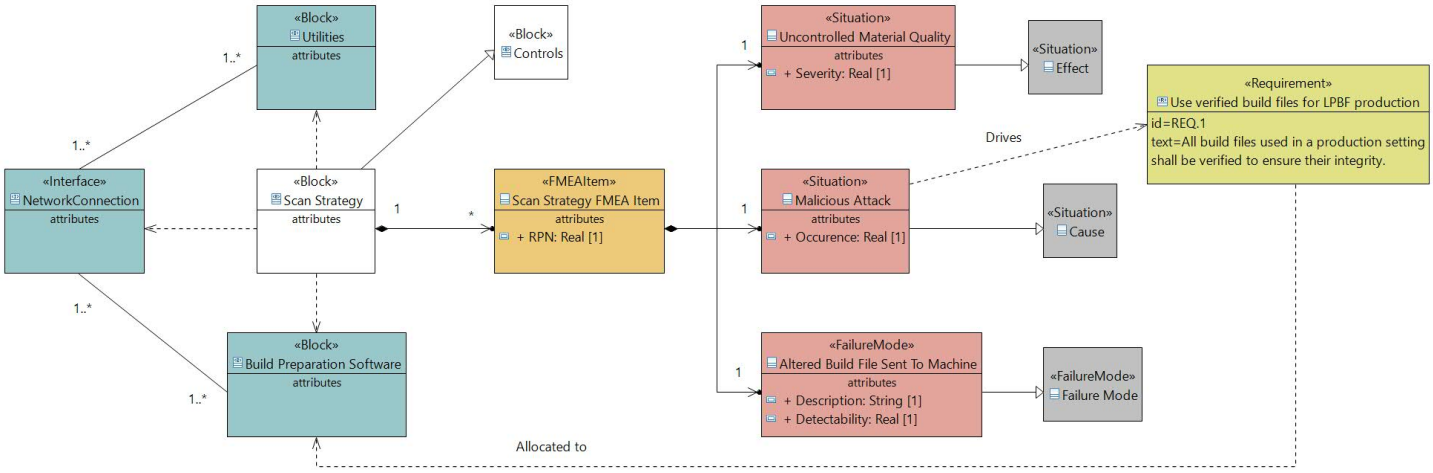

FIGURE 8: FMEA Risk Assessment of Scan Strategy

TABLE 3: Applicable Techniques for Performing RMF *Prepare* Tasks

	Use Case Diagram	Block Definition Diagram	Internal Block Diagram	IDEF0	Data Flow Diagram	Activity Diagram	Sequence Diagram	RAAML	Requirements Diagram	UAF
P-8: Mission or Business Focus	✓			✓		✓				
P-9: System Stakeholders	✓	✓								
P-10: Asset Identification		✓	✓							
P-11: Authorization Boundary	✓		✓				✓			
P-12: Information Types		✓		✓						
P-13: Information Lifecycle				✓	✓	✓	✓			
P-14: Risk Assessment		✓						✓		
P-15: Requirements Definition	✓	✓							✓	
P-16: Enterprise Architecture	✓	✓	✓							✓
P-17: Requirements Allocation	✓	✓	✓						✓	✓
P-18: System Registration	✓	✓								✓

context and environment. This paper's analysis of use cases and actors across the system lifecycle and demonstration of deriving security requirements from the analysis are key to addressing such supply chain risks.

The NIST RMF is centered around tasks and roles, but does not dictate tools, technique, method, or specific requirements for inputs or outputs. Additionally, the NIST RMF is inherently use case and application agnostic. This research has demonstrated how to apply the RMF for metal AM following a model-based approach. Such demonstrations provide valuable insights for industry and demonstrate how frameworks such as the RMF can be applied. Further work is needed to identify and detail potential metal AM security threats that can be leveraged by industry for application-specific risk analyzes and management implementations. Application-specific guidance on applying the other NIST RMF steps to metal AM, such as *Categorize* and *Monitor*, would be beneficial. Although technological security risks are a major cause for concern, there is the potential for security risks related to other domains such as political, legal, economical, environmental etc. that should also be investigated and controlled.

6. CONCLUSION

This research investigated how the NIST RMF can be applied to AM applications to address security risks. A model-based approach was proposed and demonstrated for addressing security risks associated with LPBF systems. This approach allows for information and decision traceability, requirement definition and allocation driven by risk assessments, and interoperability with enterprise architectures.

7. DISCLAIMER

Certain commercial and third-party products are identified in this paper. Such identification does not imply recommendation or endorsement by NIST, nor does it imply that the products identified are necessarily the best available for the purpose.

REFERENCES

[1] "Additive manufacturing - General principles - Fundamentals and vocabulary (ISO/ASTM 52900)." (2021).

[2] Adkins, Chris, Thomas, Stephan and Moore, Daniel. "Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing Platforms." *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*: pp. 61–65. 2021. ACM, Virtual Event Republic of Korea. DOI 10.1145/3462223.3485622.

[3] Yampolskiy, Mark, Schutzle, Lena, Vaidya, Uday and Yasinsac, Alec. "Security Challenges of Additive Manufacturing with Metals and Alloys." Rice, Mason and Shenoi, Sujeet (eds.). *Critical Infrastructure Protection IX*. Vol. 466. Springer International Publishing, Cham (2015): pp. 169–183. DOI 10.1007/978-3-319-26567-4_11. Series Title: IFIP Advances in Information and Communication Technology.

[4] Yampolskiy, Mark, King, Wayne E., Gatlin, Jacob, Belikovetsky, Sofia, Brown, Adam, Skjellum, Anthony and Elovici, Yuval. "Security of additive manufacturing: Attack taxonomy and survey." *Additive Manufacturing* Vol. 21 (2018): pp. 431–457. DOI 10.1016/j.addma.2018.03.015.

[5] Inspector General. "Audit of the Cybersecurity of Department of Defense AM Systems (DODIG-2021-098)." Technical Report No. DODIG-2021-098. US Department of Defense. 2021.

[6] Cotteleer, Mark J., Goldenberg, Simon S., Wing, Ian, Alliyu, Oyindamola, Kania, Stephen, Mujumdar, Veda and Sniderman, Brenna. "Cybersecurity Requirements for AM Systems: New Enforcement in DoD Environments, and

Resources for Implementation." *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*: pp. 49–60. 2021. ACM, Virtual Event Republic of Korea. DOI 10.1145/3462223.3485624.

[7] Yampolskiy, Mark, Bates, Paul, Seifi, Mohsen and Shamsaei, Nima. "State of Security Awareness in the Additive Manufacturing Industry: 2020 Survey." Shamsaei, Nima, Hrabe, Nik and Seifi, Mohsen (eds.). *Progress in Additive Manufacturing 2021*. ASTM International100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959 (2022): pp. 192–212. DOI 10.1520/STP164420210119.

[8] "Circular No. 130: Managing Information as a Strategic Resource." Circular Circular No. 130. Office of Management and Budget (OMB). 2016.

[9] "Committee on National Security Systems (CNSS) Glossary." Technical report no. Committee on National Security Systems (CNSS). 2022.

[10] "Risk Management Framework for Information Systems and Organizations (NIST SP 800-37)." Technical Report No. NIST SP 800-37r2. National Institute of Standards and Technology, Gaithersburg, MD. 2018. DOI 10.6028/NIST.SP.800-37r2. Accessed 2024-01-25, URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[11] Joint Task Force Transformation Initiative. "Guide for Conducting Risk Assessments (NIST SP 800-30)." Technical Report No. NIST SP 800-30r1. National Institute of Standards and Technology, Gaithersburg, MD. 2012. DOI 10.6028/NIST.SP.800-30r1. Accessed 2024-02-22, URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Edition: 0.

[12] DebRoy, T., Wei, H.L., Zuback, J.S., Mukherjee, T., Elmer, J.W., Milewski, J.O., Beese, A.M., Wilson-Heid, A., De, A. and Zhang, W. "Additive manufacturing of metallic components – Process, structure and properties." *Progress in Materials Science* Vol. 92 (2018): pp. 112–224. DOI 10.1016/j.pmatsci.2017.10.001.

[13] Associates, Wohlers (ed.). *Wohlers report 2022: 3D printing and additive manufacturing global state of the industry*. Wohlers Associates, Fort Collins (Colo.) (2022).

[14] Spears, Thomas G. and Gold, Scott A. "In-process sensing in selective laser melting (SLM) additive manufacturing." *Integrating Materials and Manufacturing Innovation* Vol. 5 No. 1 (2016): pp. 16–40. DOI 10.1186/s40192-016-0045-4.

[15] Voas, Jeff, Mell, Peter and Piroumian, Vartan. "Considerations for Digital Twins Standards (NISTIR 8356 (Draft))." preprint NISTIR 8356 (Draft). National Institute of Standards and Technology. 2021. DOI 10.6028/NIST.IR.8356-draft. Accessed 2024-02-07, URL https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8356-draft.pdf.

[16] Fahad Ali Milaat and Joshua Lubell. "Layered Security Guidance for Data Asset Management in Additive Manufacturing." *J. Comput. Inf. Sci. Eng.* Vol. 24 No. 7 (2024): p. 071001.

[17] Carrion, Patricio E, Graves, Lynne M, Yampolskiy, Mark and Shamsaei, Nima. "Evaluation of a Cyber-Physical Attack Effectiveness in Metal Additive Manufacturing by Selectively Modifying Build Layer Thickness." .

[18] Graves, L., King, W.E., Carrion, P., Shao, S., Shamsaei, N. and Yampolskiy, M. "Sabotaging metal additive manufacturing: Powder delivery system manipulation and material-dependent effects." *Additive Manufacturing* Vol. 46 (2021): p. 102029. DOI 10.1016/j.addma.2021.102029.

[19] Zinner, Theo, Parker, Grant, Shamsaei, Nima, King, Wayne and Yampolskiy, Mark. "Spooky Manufacturing: Probabilistic Sabotage Attack in Metal AM using Shielding Gas Flow Control." *Proceedings of the 2022 ACM CCS Workshop on Additive Manufacturing (3D Printing) Security*: pp. 15–24. 2022. ACM, Los Angeles CA USA. DOI 10.1145/3560833.3563565.

[20] Brooks, Sean, Garcia, Michael, Lefkovitz, Naomi, Lightman, Suzanne and Nadeau, Ellen. "An Introduction to Privacy Engineering and Risk Management in Federal Systems (NISTIR 8062)." Technical Report No. NIST IR 8062. National Institute of Standards and Technology, Gaithersburg, MD. 2017. DOI 10.6028/NIST.IR.8062. Accessed 2024-02-22, URL https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[21] Efe, Ahmet. "A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT." *Journal of Auditing and Assurance Services* Vol. 3 No. 2 (2023): pp. 185 – 205.

[22] Zemrowski, Kenneth M. "NIST Bases Flagship Security Engineering Publication on ISO/IEC/IEEE 15288:2015." *Computer* Vol. 49 No. 12 (2016): pp. 86–88. DOI 10.1109/MC.2016.373.

[23] Lubell, Joshua. "A Document-based View of the Risk Management Framework.pdf." *Balisage: The Markup Conference 2020*, Vol. 25: p. 20. 2020. Washington, D.C.

[24] Dandashi, Fatma. "Modeling Security Views with Unified Architecture Framework, Risk Assessment and Analysis Modeling Language, and Systems Modeling Language." Technical Report PRS-22-0326. The MITRE Corporation, McLean, VA. 2022.

[25] "OMG Systems Modeling Language (OMG SysML™)." (2019).

[26] "Information technology - Modeling Languages - Part 1: Syntax and Semantics for IDEF0 (ISO/IEC/IEEE 31320-1)." (2012). DOI 10.1109/IEEESTD.2012.6363476. ISBN: 9780738180014.

[27] Tangkawarow, I. R. H. T. and Waworuntu, J. "A Comparative of Business Process Modelling Techniques." *IOP Conference Series: Materials Science and Engineering*, Vol. 128: p. 012010. 2016. DOI 10.1088/1757-899X/128/1/012010.

[28] "Risk Analysis and Assessment Modeling Language (RAAML) Libraries and Profiles, v1.0." (2022).

[29] "Machine Qualification for Fusion-Based Metal Additive Manufacturing (SAE AMS7032)." (2022).

[30] "Enterprise Architecture Guide for UAF (Informative)." (2022).

[31] Lemaire, Laurens, Lapon, Jorn, De Decker, Bart and Naessens, Vincent. "A SysML Extension for Security

Analysis of Industrial Control Systems." *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*. 2014. BCS Learning & Development. DOI 10.14236/ewic/ics-csr2014.1.

[32] Birch, Dustin S., Narsinghani, Jayesh, Herber, Daniel and Bradley, Thomas H. "Human factors hazard modeling in the systems modeling language." *Systems Engineering* Vol. 26 No. 3 (2023): pp. 328–343. DOI 10.1002/sys.21659.

[33] Oates, Robert, Thom, Fran and Herries, Graham. "Security-Aware, Model-Based Systems Engineering with SysML." 2013. DOI 10.14236/ewic/ICSCSR2013.9.