# Towards a Method for Secure Management of Manufacturing-as-a-Service Platforms

Kaspars Ābelnīca[1,*]

[1]Institute of Information Technology, Riga Technical University (RTU), Zunda krastmala 10, Riga, LV-1048, Latvia

**Abstract**

Manufacturing-as-a-Service (MaaS) is a new approach to manufacturing where orders are distributed between multiple manufacturers based on their capacity and available manufacturing time. The MaaS model is an example of a cyber-physical system where IT (information technology) and OT (operational technology) converge as cloud computing is used to plan and execute orders in a production line. Due to the different parties and technologies required to implement MaaS, security management is a high priority to ensure confidentiality, integrity and availability of all connected systems. While state-of-the-art solutions exist for securely managing individual components that make up MaaS, there is no single method that guides MaaS operators through the key security management steps. This paper proposes the design of a new method for MaaS security management. It outlines the plan for future research by summarizing current related research, identifying research gaps and defining the research problem and research questions. The plan for using the design science research method is also described. Results already published in other studies are presented by the author along with a plan for future research that is still required to answer the specified research questions. Challenges and limitations in the current research have also been analysed by the author with recommended next steps to finish the proposed research.

**Keywords**

Manufacturing-as-a-Service, security management, design science research, risk management, cyber-physical systems

## 1. Introduction

*Manufacturing-as-a-Service* (MaaS) is a new manufacturing model that uses high technologies such as the internet of things (IoT), cloud computing and digital twins to facilitate more efficient utilization of manufacturing capacity [1] through the convergence of information technology (IT) and operational technology (OT) [2]. It aims to reduce manufacturing line standstill by allowing providers to sell their free manufacturing time as a service (thus the name of the model). Successful implementation of MaaS improves provider profit margins and allows clients to place personalized orders without needing to rely on their own manufacturing infrastructure.

These platforms face various security challenges due to the different services and components that are necessary to implement the connections between different providers, clients and marketplaces. Cybersecurity risks such as unsecured legacy manufacturing systems [3], different edge network configurations and the exchange of intellectual property between different providers [4] need to be effectively managed throughout the lifecycle of the platform.

The aim of this paper is to propose the design of a new method for the security management of MaaS platforms. It explores existing research, identifies gaps and describes a new research problem. The author also describes how design science research (DSR) is used to construct this new method and how its implementation will be instantiated as part of a new MaaS framework MEDUSA. The published results of already completed research are also summarized along with the planned future research that still needs to be explored. The results described are based on currently ongoing doctoral research.

The paper is structured as follows. Section 2 describes the background of MaaS security management and identifies research gaps. Section 3 specifies the research problem tackled by the planned doctoral

*Baltic DB&IS 2026 Conference Forum and Doctoral Consortium, 28 June - 1 July 2026, Tartu, Estonia*

*Corresponding author.

Kaspars.Abelnica@rtu.lv (K. Ābelnīca)

0009-0006-9044-7536 (K. Ābelnīca)

research and lists proposed research questions. Section 4 describes the research methodology and expected results. Section 5 summarizes current research results and outlines the plan for future research. Section 6 concludes the paper, identifies limitations and lists the challenges that still need to be tackled to successfully complete the research.

## 2. Background

In order to develop a new method for the security management of MaaS platforms, it is necessary to identify the key security challenges for this approach and analyse the current industry state-of-the-art to see if there are any existing gaps that need to be addressed.

### 2.1. Security challenges for the MaaS model

MaaS platforms are cyber-physical systems [1] and involve a variety of different elements that greatly expand its cybersecurity landscape, compared to regular manufacturing systems. A MaaS platform usually incorporates the following:

1. A **marketplace** (one or several) to place and receive manufacturing orders
2. **Manufacturers** that provide their infrastructure to meet marketplace orders
3. **Customers** that place manufacturing orders through the marketplace
4. The **infrastructure** (physical and virtual) to facilitate manufacturing
5. Networking and **secure data exchange**

Cybersecurity threats and IT distribution have been highlighted as the main threat to business continuity, as companies digitalize their operations and business processes (of which MaaS is an example). Cyberattacks have emerged as one of the most critical threats to continuous operation [5]. Ransomware, data breaches, and other cyber incidents can bring business to a standstill by crippling IT systems or compromising vital data.

Furthermore, the very nature of MaaS (several interconnected parties with manufacturing data distributed among them) poses challenges for non-compliance and data breaches [6]. Relying on various third parties for manufacturing may also be unreliable [7] and risk production delays that disrupt the supply chain [4] if one of the manufacturers is unable to fulfil promised orders.

MaaS platforms are also an example of IT and OT convergence [2] that requires connecting previously independent manufacturing systems to the cloud to exchange data. Such legacy systems are vulnerable to cyberattacks that can disrupt manufacturing lines [3]. A data breach in such a case can take months to discover [8], providing opportunities for attack by external actors. Legacy systems also rarely have clear standards and protocols for further integration [9].

### 2.2. Current approaches for the secure management of MaaS platforms

The term MaaS itself is currently not the only one used to describe this model of manufacturing. Relevant research may also use other terms such as *cloud manufacturing* [4, 6, 7, 10] or *digital manufacturing* [3] to describe similar approaches. At the same time, MaaS also implements the technologies linked to *smart manufacturing* [2, 11]. This poses a challenge with clearly identifying previous studies that are relevant to MaaS security management.

The reason for implementing security management for MaaS platforms is to ensure the confidentiality, integrity and availability [12] of its different components. Surveys have identified the typical threats faced by the technologies used by MaaS platforms such as digital twins [13] and those required by Industry 4.0 [3, 4]. The implementation of distributed ledger technology (DLT) such as blockchain is also proposed for trust management in MaaS systems [10].

Industry standards such as ISO 27001:2022 [12] exist for the security management of IT systems. Due to the convergence of IT and OT in MaaS, the knowledge in such standards should be further expanded

upon by exploring the gaps that existing attack taxonomies do not cover [2] and to classify threats and likely attack targets such as sensors or CAD software [3].

Threat modelling appears as a key step [11] with other fields such as enterprise architecture providing examples of how to use modelling languages such as ArchiMate [14, 15] for this purpose. Using standards such as ISO 27005:2022 [16], it is possible to then assess the risks caused by these threats and implement risk treatment activities such as mitigation. IT security controls are described in the ISO 27002:2022 [17] standard and security taxonomies like MITRE ATT&CK [18] which provide techniques for the mitigation of cybersecurity attacks. Solutions to implement a specific control can also be stored as security patterns [19].

Analysis of related research reveals that, while there is extensive industry knowledge available on security management, how to model threats and assess risks, and how to specify security controls and patterns, there currently does not exist a method for successfully implementing all of these steps in the MaaS context where different manufacturing systems, devices and technologies need to securely distribute data between themselves. This identifies an existing gap for securely managing MaaS platforms and an area for potential research.

## 3. Research problem

This section of the paper defines the proposed research problem for MaaS security management using an IDEF0 function and lists the proposed research questions by the author to help resolve the problem.

### 3.1. Problem definition

The proposed research problem is how to specify a function that would take the MaaS context (marketplace data, IoT telemetry data and manufacturer capacity), use the knowledge available in a MaaS security ontology and risk assessment, dynamically readjust risk scores based on current data, and, as a result, provide the full list of actions (automated and/or manually executed) that are necessary to bring the MaaS platform to an optimal state that balances the security requirements and the capacity of connected manufacturers. This research problem is illustrated using an IDEF0 top level (A-0) diagram (see Figure 1).

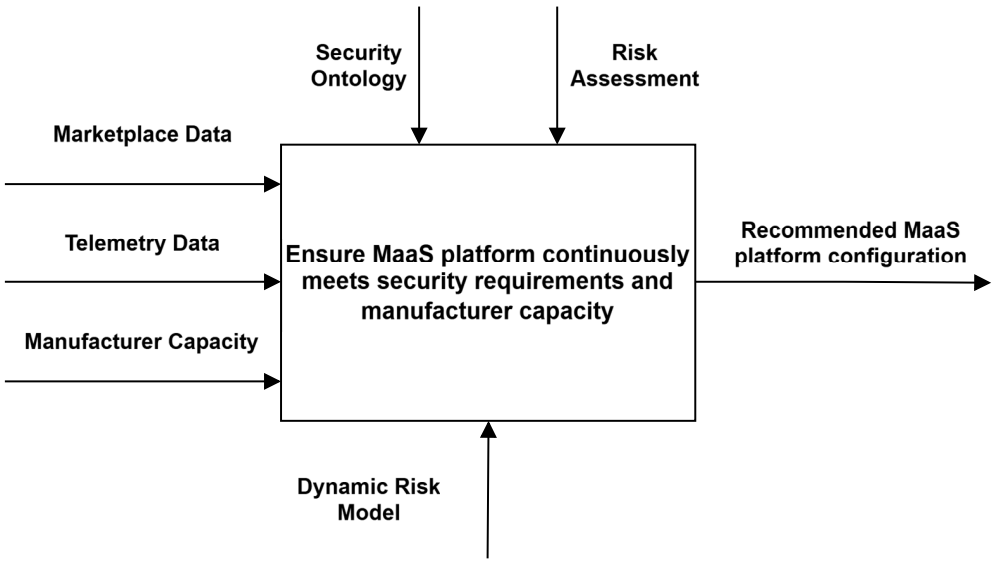


**Figure 1:** IDEF0 A-0 diagram of a function for MaaS security management.

The author argues that, while the individual implementation of such a function may vary between different MaaS ecosystems, the required steps and procedures to achieve that can be reused. As such, it

is worthwhile to design a method for MaaS security management that could be reused and iterated on by MaaS platform operators. A method with clearly defined steps would also allow to more easily automate tasks (e.g., the configuration of new components) that have a straightforward solution.

### 3.2. Research questions

The author outlines seven research questions in order to research and tackle the defined research problem. The structure of the questions is based on the standardized template for DSR research questions as proposed by Thuan et al. in their 2019 paper [20]:

**RQ1** What are the main requirements for designing a new method for MaaS platform security management?
**RQ2** Which essential resources (systems, data, hardware etc.) define the method?
**RQ3** What existing knowledge (methods, management processes) is currently used for MaaS security management?
**RQ4** How can we elaborate a new security management method for MaaS platforms to be compliant with user requirements and existing IT and OT industry standards?
**RQ5** How can we evaluate the usefulness of the new MaaS security management method?
**RQ6** How can we use the new MaaS security management method?
**RQ7** What new knowledge about the security management of MaaS platforms does this method contribute?

This format of research questions has been selected by the author as it allows to more easily provide definitive answers to each question and link them to the presented research results. A matrix can be created at the end of the research to showcase which questions are addressed by each of the included publications.

## 4. Methodology and expected results

The design of the new security management method follows the DSR methodology [21]. This research method has been selected due to the need for producing a specific artifact that will then be used by both technical and non-technical MaaS domain experts.

The author implements the *DSR research grid* as proposed by vom Brocke & Maedche in 2019 to better capture projects implementing the DSR method [22]. This grid (see Figure 2) describes the creation of the new method according to six key dimensions that are relevant for DSR led research.

Key points to highlight in the DSR grid are that there are many concepts related to MaaS that need to be explored and covered during research, the high amount of input knowledge that is required to complete the research, and the fact that the method needs to be evaluated and analysed for the MEDUSA use-case. It also highlights how it is important for the author to clearly define the MaaS concept itself due to usage of different terms in related studies.

The main result of the described research is the creation of a new artifact: a method for the security management of MaaS platforms. This method must be accessible to both technical and management experts by listing the security management phases that need to be carried out to implement this method and by providing specific actions (with examples) that need to be taken during each of these phases. As described previously, this method must provide the user with a solution on how to move their MaaS platform to a state that meets the previously specified security requirements, risk appetite, and capacity of individual manufacturers.

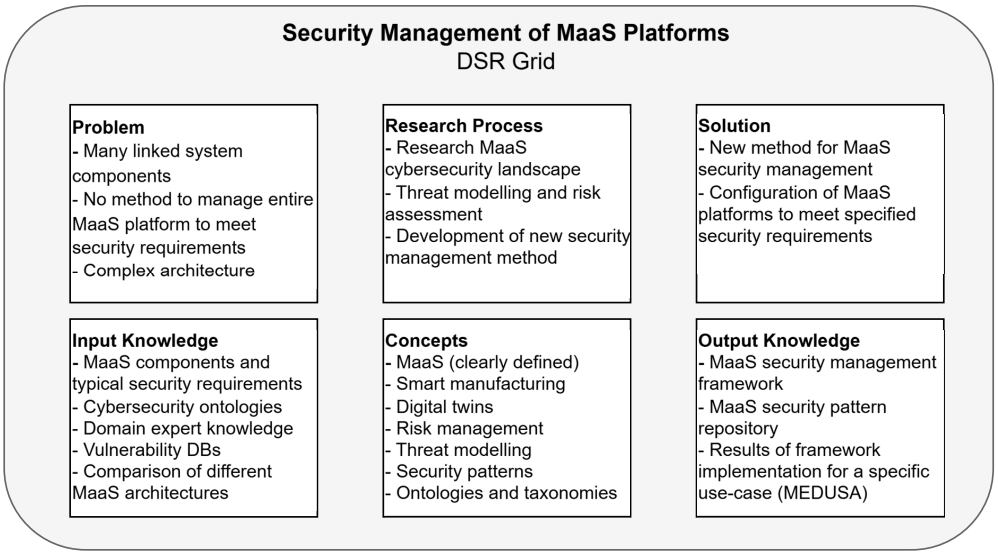


**Figure 2:** DSR grid for designing a new MaaS security management method.

The author's proposed plan for the doctoral research confirms to the seven DSR research guidelines [21] in order to ensure that it follows the core ideas behind design science (see Table 1 for further clarification). The argumentation provided in this table is based on the current stage of the research.

**Table 1**
Research Compliance with DSR Guidelines

| DSR Guideline | Reason for compliance |
|---|---|
| Guideline 1: Design as an Artifact | The end result of the research is a method that can be used repeatedly for MaaS security management. |
| Guideline 2: Problem Relevance | MaaS is a modern approach for manufacturing that is relevant for the European Union's transition to a competitive circular economy [23]. There is currently no single industry-accepted approach for MaaS security management. |
| Guideline 3: Design Evaluation | The method is planned to be evaluated and its utility, quality and efficacy demonstrated via defined evaluation methods and showcased via an example implementation. |
| Guideline 4: Research Contributions | Research results are be presented in scientific conferences and journals for peer-review. The designed artifacts are open for further iteration and elaboration by future researchers. |
| Guideline 5: Research Rigour | The methods for constructing and evaluating the method are described in-detail as part of the final doctoral research. |
| Guideline 6: Design as a Search Process | Research follows state-of-the-art research in both MaaS and IT/OT security management. The method is designed to comply with user requirements and common industry standards such as ISO 27005:2022 [16]. |
| Guideline 7: Communication of Research | The designed method is targeted for both technical and management oriented domain experts. The higher-level processes described by the method are further elaborated with technical details that allow for instantiation. |

## 5. Research progress

This section summarizes the research results that have already been published by the author and outlines the plan for future research that is still needed to tackle the research problem and provide

answers to the research questions. The result of the described research is a new method for MaaS security management which includes the following key phases:

1. Identification and **prioritization of critical MaaS assets**
2. **Threat modelling** to map key threats targeting MaaS assets
3. **Creation of a risk registry** based on the threat modelling results
4. **Selection of risk treatment strategies** and security controls for the identified MaaS risks
5. Building of a **security pattern repository** to store and retrieve solutions for implementing security controls
6. **Dynamic risk modelling and reassessment** to keep the risk registry up-to-date and measure the effectiveness of current security controls

The implementation of this method would allow MaaS operators without in-depth security management knowledge to ensure that their solution remains secure against changes in system context and the discovery of new vulnerabilities and attack techniques.

## 5.1. Published results

An illustrative example of a threat model and risk assessment for the MaaS platform MEDUSA has been presented in a paper at the ICISSP 2026 conference [24] that showcases how the ArchiMate language can be used to model the trust boundaries between different MaaS architecture layers (see Figure 3). The research is based on the work by Steven Bradley [14] which uses ArchiMate for enterprise threat modelling with SABSA [25]. The author has adapted the work for a different use-case where risk management is implemented using an asset-based approach with the ISO 27005:2022 standard [16]. The model has been validated by domain experts in the MEDUSA project consortium.

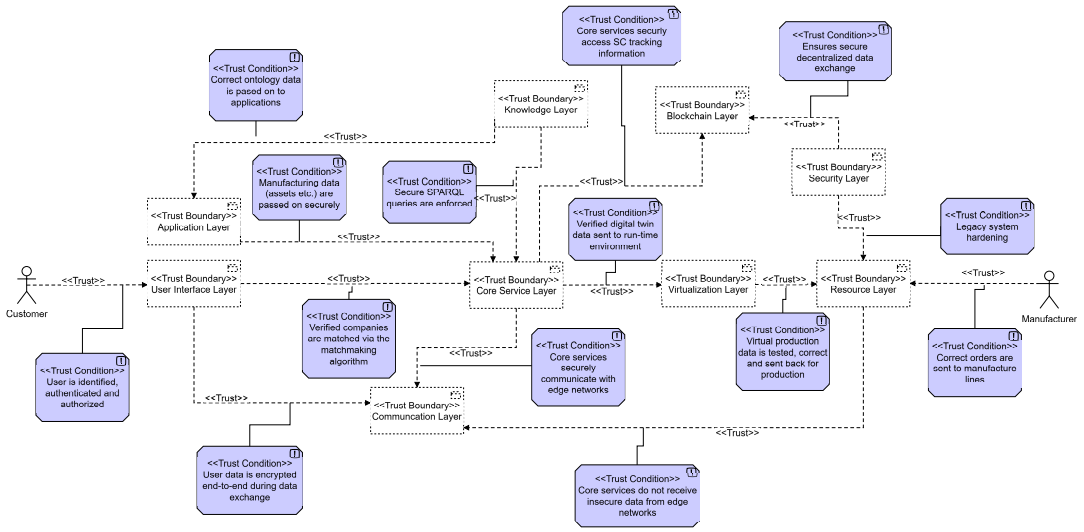


**Figure 3:** Overall threat model of the MEDUSA MaaS platform.

Each of the layers is populated with the different assets (MaaS components) which are linked to each other as specified in the MEDUSA architecture. After that, identified vulnerabilities, threats and risks have been added to the model with corresponding security objectives and security controls (see Figure 4 for an example where a risk regarding production asset tampering in the digital twin has been mitigated). Relevant ISO 27001:2022 Annex A security controls [12] and MITRE ATT&CK mitigation techniques [18] are also linked to the specified control objective. This is based on an approach provided by Band et al. in 2015 [15] which is now also part of the ArchiMate specification itself [26].

These results provide the first answers to the previously raised research questions. They highlight how the method must include threat modelling and risk assessment of the MaaS platform as a key step (RQ1, RQ2). The paper also showcases how traditional solution-driven threat modelling methods are not

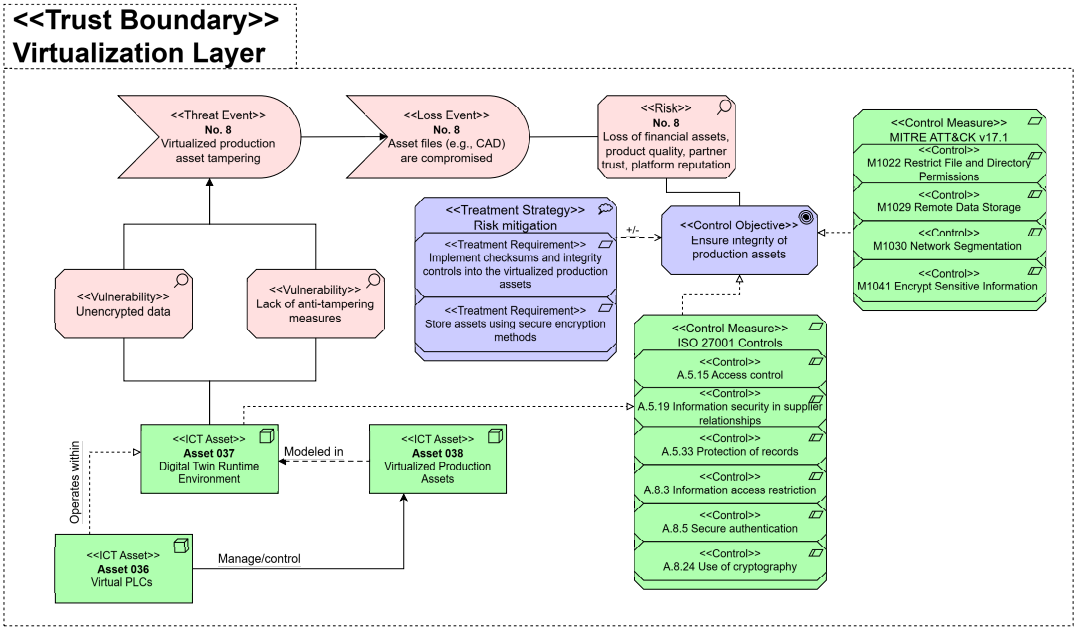


**Figure 4:** Modelling MaaS threats and planning risk mitigation using ArchiMate.

sufficient during the early MaaS design stage (RQ3) due to the multitude of different components that are not yet fully defined. It also provides an example how to identify and model (RQ6) the relationships between MaaS platform components using the ArchiMate language.

## 5.2. Future research

The author currently plans to still address three main areas of research: (1) a more complete and systematic review of the current cybersecurity landscape of MaaS, (2) the dynamic monitoring of risks in a live MaaS platform and (3) the storing and retrieval of solutions from a security pattern repository.

The MaaS cybersecurity landscape is planned to be analysed as part of an in-depth literature review that aims to identify what threats are particular to MaaS platforms and how their related risks are currently mitigated. The literature review would identify the key threats that MaaS platforms are currently facing, grouping them into three main categories: business continuity (threats which endanger the continuous operation of the manufacturers and marketplaces), third-party management (threats that exist due to the cooperation between various organizations in the MaaS platform), and IT/OT interoperability (threats linked to connecting manufacturing systems to IoT devices).

The dynamic MaaS risk model is aimed at ensuring that the initial risk assessment carried out during the design phase of creating a new MaaS platform is able to adapt to changes in context (either by changes in the architecture of the solution or by the discovery of new cybersecurity risks) as expected by the ISO 27005:2022 standard which describes risk management as an iterative process [16]. Such a model would then monitor live data from sources such as SIEM or IDS logs, data from marketplaces and manufacturer IoT devices, and newly discovered vulnerabilities (CVEs).

Upon the detection of data anomalies, the model (see Figure 5) would recalculate risk scores and, if needed, register new MaaS assets. Once the model detects an event has exceeded a specified risk score threshold, it is classified as an incident which triggers countermeasures that are retrieved from known security patterns and an investigation is started. Risks that are currently rated highly but are not detected for prolonged time periods may be reclassified as lower risks by the model. Similarly, a risk that triggered an important cybersecurity event will be rescored higher.

The security pattern repository will be designed to store the knowledge linked to the mitigation of previously identified MaaS threats. Storing this knowledge in the form of patterns allows to easily categorize it by linked threats, context (in this case, the MaaS architecture) and provide a solution [19].

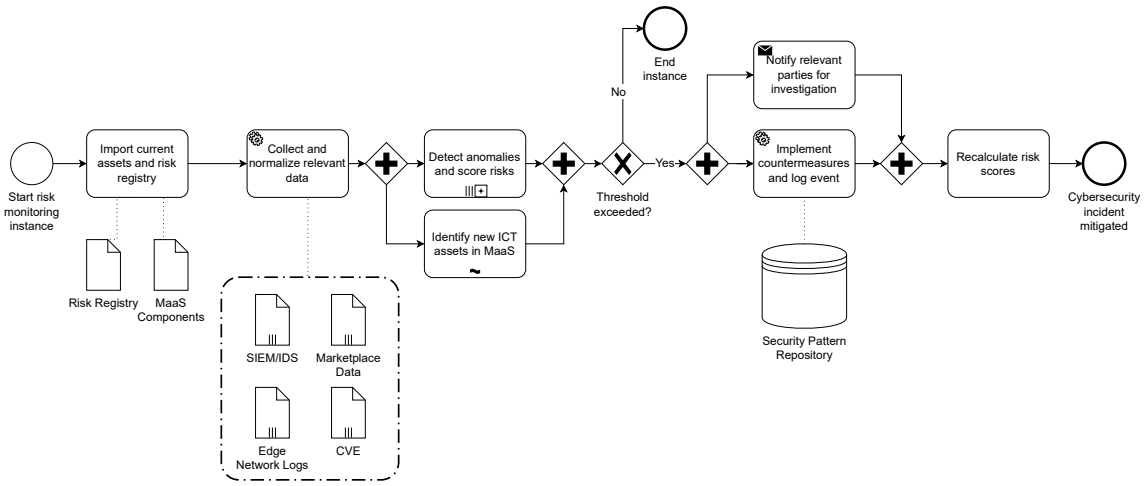


**Figure 5:** BPMN 2.0 diagram of the MaaS dynamic risk monitoring process.

This repository can also link with a broader MaaS security ontology which would allow to directly connect described patterns to security controls that protect against specific cybersecurity threats and mitigate risks [27]. An example of such a MaaS security pattern is showcased in Table 2 where threats to data exchange security are countered by the enabling of encrypted data exchange using the MQTT protocol. The generalized solution can then be supplemented by a specific reference implementation for known systems and hardware.

**Table 2**
MaaS Security Pattern Example

| Property | Value |
|---|---|
| Name | Encrypted MQTT data exchange |
| Categories | Middleware |
| Context | Security of data exchanged using the MQTT protocol requires encryption (TLS or similar) to ensure confidentiality for IoT devices. |
| Solution | 1. Create CA certificate.<br>2. Load certificate unto device.<br>3. Configure MQTT client on device.<br>4. Test MQTT broker connection.<br>5. Harden production configuration. |

## 6. Conclusions

This paper showcases how there is a gap between the existing knowledge for security management of IT and OT systems and direct methods for implementation, especially in models such as MaaS where IT and OT converge with their own respective security threats and vulnerabilities. The proposed research plan and currently published results highlight how there is a lot of potential in the design of such a method. Access to real-time data permits to react to changes in the context of a MaaS platform, as showcased with the dynamic risk model that can adjust risks and identify security incidents while the platform is live. A dedicated repository of MaaS security patterns can also be further refined and extended as more information is shared between the different organizations connected to a specific MaaS platform.

The MaaS threat model that has already been created using ArchiMate, demonstrates the importance of looking at other fields such as enterprise architecture for best practices that could be included as part of the designed MaaS security management method. This is also further underlined by how MaaS is

not yet a fully established term in literature so there is potential for finding relevant knowledge when adopting a broader view on which studies to identify and screen for the research.

At this current stage of research, the author has identified the following key challenges that still need to be addressed to successfully complete the doctoral research. First, the term MaaS is not as ubiquitously used as the author had expected and it is possible that important state-of-the-art knowledge has not yet been retrieved due to it being published using another term. It is recommended to do an extended keyword analysis of already retrieved studies to further refine search queries.

Second, clear methods to be used for the evaluation and validation of the usefulness of the new MaaS security management method have not yet been selected. Evaluation and validation examples should be analysed within existing security management research due to the high importance placed on this by DSR. If such validation methods are not available, then one needs to be defined as part of this research.

Finally, while the threat modelling method using ArchiMate has been validated by the domain experts involved in the development of MEDUSA, the entire MaaS security management method described in this paper would benefit from further interviews and validation from domain experts about the usefulness of the overall approach. It should also be evaluated against other IT threat modelling methods.

## Acknowledgments

I would like to thank the supervisors of my doctoral research prof. Jānis Grabis and assoc. prof. Rūta Pirta for their guidance and support in the planning of my research and the review of this paper.

MEDUSA is created as part of the project *Manufacturing as a service framework exploiting decentralized secure data exchange promoting sustainability and circularity* and has received funding from the European Union's HORIZON-CL4-TWIN-TRANSITION-01 programme under grant agreement no. 101178045.

## Declaration on Generative AI

The author has not employed any Generative AI tools in the writing of this paper.

## References

[1] M. H. Rahman, M. Shafae, Cyber-Physical Security Vulnerabilities Identification and Classification in Smart Manufacturing – A Defense-in-Depth Driven Framework and Taxonomy, Journal of Computing and Information Science in Engineering 25 (2025). doi:10.48550/arXiv.2501.09023.

[2] M. H. Rahman, T. Wuest, M. Shafae, Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies, Journal of Manufacturing Systems 68 (2023) 196–208. doi:10.1016/J.JMSY.2023.03.009.

[3] P. Mahesh, A. Tiwari, C. Jin, P. R. Kumar, A. L. Reddy, S. T. Bukkapatanam, N. Gupta, R. Karri, A Survey of Cybersecurity of Digital Manufacturing, 2021. doi:10.1109/JPROC.2020.3032074.

[4] D. Peters, T. S. Heinze, Security challenges for cloud manufacturing: A case study in the space domain, in: CEUR Workshop Proceedings, volume 2339, 2019, pp. 58–61. URL: https://ceur-ws.org/Vol-2339/.

[5] S. Altaha, M. M. H. Rahman, A Mini Literature Review on Integrating Cybersecurity for Business Continuity, in: 5th International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2023, 2023, pp. 353–359. doi:10.1109/ICAIIC57133.2023.10067127.

[6] T. N. Rane, System and Risk Analysis of Cloud-Manufacturing System, International Journal of Computer Science & Engineering Survey 13 (2022) 13–27. doi:10.5121/ijcses.2022.13302.

[7] A. Ma, A. Nassehi, C. Snider, An analysis of premium payments as a mechanism for securing preferential service in cloud manufacturing, Procedia CIRP 81 (2019) 168–173. doi:10.1016/J.PROCIR.2019.03.030.

[8] B. Cinar, Supply Chain Cybersecurity: Risks, Challenges, and Strategies for a Globalized World, Journal of Engineering Research and Reports 25 (2023) 196–210. doi:10.9734/jerr/2023/v25i9993.

[9] M. Mourad, A. Nassehi, D. Schaefer, Interoperability as a Key Enabler for Manufacturing in the Cloud, in: Procedia CIRP, volume 52, Elsevier B.V., 2016, pp. 30–34. doi:10.1016/j.procir.2016.07.051.

[10] M. A. Umer, L. B. Gouveia, E. G. Belay, Provenance blockchain for ensuring IT security in cloud manufacturing, Frontiers in Blockchain Volume 6 - 2023 (2023). doi:10.3389/fbloc.2023.1273314.

[11] M. Jbair, B. Ahmad, C. Maple, R. Harrison, Threat modelling for industrial cyber physical systems in the era of smart manufacturing, Computers in Industry 137 (2022). doi:10.1016/j.compind.2022.103611.

[12] ISO/IEC, ISO/IEC 27001:2022 standard, 2022. URL: https://www.iso.org/standard/27001.

[13] C. Alcaraz, J. Lopez, Digital Twin: A Comprehensive Survey of Security Threats, IEEE Communications Surveys & Tutorials 24 (2022) 1475–1503. doi:10.1109/COMST.2022.3171465.

[14] S. Bradley, TSI T100 – Modelling SABSA with ArchiMate, Technical Report, The SABSA Institute, 2026. URL: https://sabsa.org/white-paper-requests/.

[15] I. Band, W. Engelsman, C. Feltus, S. G. Paredes, J. Hietala, H. Jonkers, S. Massart, Modeling Enterprise Risk Management and Security with the ArchiMate® Language, Technical Report, The Open Group, 2015. URL: https://pure.unamur.be/ws/files/12366722/Modeling_Enterprise_Risk_Management_and_Secutity_with_the_ArchiMate_Language.pdf.

[16] ISO/IEC, ISO/IEC 27005:2022 standard, 2022. URL: https://www.iso.org/standard/80585.html.

[17] ISO/IEC, ISO/IEC 27002:2022 standard, 2022. URL: https://www.iso.org/standard/75652.html.

[18] MITRE, MITRE ATT&CK, 2025. URL: https://attack.mitre.org/.

[19] A. V. Uzunov, E. B. Fernandez, An extensible pattern-based library and taxonomy of security threats for distributed systems, Computer Standards & Interfaces 36 (2014) 734–747. doi:10.1016/j.csi.2013.12.008.

[20] N. H. Thuan, A. Drechsler, P. Antunes, Construction of Design Science Research Questions, Communications of the Association for Information Systems 44 (2019) pp–pp. doi:10.17705/1CAIS.04420.

[21] A. R. Hevner, S. T. March, J. Park, S. Ram, Design Science in Information Systems Research, Management Information Systems Quarterly 28 (2004) 75–106. doi:10.2307/25148625.

[22] J. v. Brocke, A. Maedche, The DSR Grid: Six Core Dimensions for Effective Capturing of DSR Projects, Electronic Markets (2019). doi:10.1007/s12525-019-00358-7.

[23] EU Directorate-General for Research and Innovation, 'Made in Europe' - Research and innovation - European Commission, 2020. URL: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/made-europe_en.

[24] K. Ābelnīca, G. Leopizzi, R. Pirta, J. Grabis, B. Krauze, Designing Secure Manufacturing-as-a-Service Platforms: Threat Modeling and Cybersecurity Risk Assessment, in: Proceedings of the 12th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, INSTICC, SciTePress, 2026, pp. 213–220. doi:10.5220/0014357000004061.

[25] The SABSA Institute, SABSA executive summary, 2025. URL: https://sabsa.org/sabsa-executive-summary/.

[26] The Open Group, ArchiMate® 3.2 Specification, The Open Group Series, Van Haren Publishing, 2022. URL: https://publications.opengroup.org/standards/archimate/c226.

[27] J. Grabis, R. Pirta, K. Ābelnīca, G. Leopizzi, Towards Ontology for Security Management Knowledge Sharing in Manufacturing-as-a-Service, Proceedings of the 20th International Conference on Research Challenges in Information Science (RCIS), 2026. (in-press).