Human Factors in Cybersecurity, Vol. 127, 2024, 198–207
https://doi.org/10.54941/ahfe1004779

The Human Factor Impact on a Supply Chain Tracking Service Through a Risk Assessment Methodology

Dimitris Koutras[1], Kitty Kioskli[2,3], and Panayiotis Kotzanikolaou[1]

[1]Department of Informatics University of Piraeus, 80 Karaoli & Dimitriou st., Piraeus, Greece

[2]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Colchester CO4 3SQ, United Kingdom

[3]Trustilio B.V., Vijzelstraat 68, Amsterdam 1017 HL, The Netherlands

ABSTRACT

This paper presents a novel risk assessment methodology for supply chain tracking systems, uniquely focusing on integrating human error with technological and security risks. Our approach examines the interaction between human factors and technological elements such as IoT and cloud services, highlighting their impact on security and operational efficiency. The methodology extends beyond technical aspects to include the strategic business requirements of SC tracking. Through a proof-of-concept case study, we demonstrate the methodology's applicability across diverse SC contexts. This work emphasizes the crucial role of human factors in enhancing the reliability, security, and effectiveness of SC tracking systems.

Keywords: Asset categorization, Risk assessment, Human factor, SC tracking systems

INTRODUCTION

In the rapidly evolving landscape of Supply Chain (SC) management, the importance of tracking services in overseeing the lifecycle from production to sale. These services rely on sophisticated systems that monitor vital condition information such as temperature, humidity, light and position of the transferred products. However, beyond the technical and mechanical aspects, human factors play a critical role in the operational integrity of these systems (Chen, 2020).

In an environment where standardization efforts in SC risk assessment methodologies are ongoing, our work identifies the necessity for more specialized techniques, particularly those addressing security risks related to tracking and monitoring systems. Given the distributed nature and internet connectivity of these systems, they are inherently susceptible to numerous security challenges, predominantly involving their technological equipment.

Employing well-known risk assessment standards and threat modeling guides, our methodology scrutinizes targeted IT components used in SC tracking systems, their technical characteristics, and realistic threat agents in the SC ecosystem. We aim to evaluate whether security attacks originating from SC-specific threat agents result in tangible security risks against targeted hardware and software components within SC networks (Reiman, 2021).

Numerous risk assessment methodologies related to SC security have been documented in the literature. In (Koutras, 2023), an initial version of the methodology presented in this paper is defined. In the preliminary version, our initial approach did not incorporate human factors within the risk assessment process, focusing more on a formal and structured analysis based on predefined categories. In addition the methodology lacked asset granularity; assets were examined in groups or categories rather than individually, which meant that the assessment didn't account for the nuances of each specific asset. This made the initial methodology more straightforward and understandable but less tailored to the unique characteristics and vulnerabilities of individual assets.

Other studies (Schauer, 2019; Papastergiou, 2018) present an innovative evidence-based risk assessment methodology for analyzing and evaluating risks within the maritime SC domain. Their methodology is based on the use of publicly available information, well-established mathematical principles, and industry best practices. Its primary objective is the automated detection and assessment of vulnerabilities and potential threats associated with the cyber assets involved. A similar approach is presented in (Polemi, 2015), where the authors propose a SC risk assessment methodology aligned with ISO 28001 standards, specifically designed for the comprehensive assessment of SC-related risks, including cascading threat scenarios.

In Pollini (2022) introduces a holistic Human Factors approach, integrating individual, organizational, and technological aspects to assess Human Factors vulnerabilities and their impact on cybersecurity risks in healthcare organizations. It employs a methodology, combining qualitative and quantitative research methods, to evaluate the cybersecurity maturity levels of these organizations. The article (Neumann, 2021) addresses the underrepresentation of human factors in Industry 4.0 research, identifying a significant gap through focused content analysis of existing literature. It proposes a conceptual framework that integrates key concepts from human factors engineering, tailored specifically for the context of Industry 4.0. Another study (Sgarbossa, 2020) utilize their experience to outline the vision, challenges, and opportunities in integrating human factors and ergonomics in industrial and logistic system design and management.

Motivation-Contribution

Despite ongoing attempts to standardize SC risk assessment methodologies, there is a growing need for more specialized approaches, particularly those that tackle security risks associated with tracking and monitoring systems. Given that these systems are widely distributed and connected to the internet, they are prone to a range of security challenges, primarily stemming from their technological components, but also from security challenges related with the human factor. Therefore, it becomes essential to adopt a focused risk assessment methodology that not only addresses these technological aspects but also places a central emphasis on human factors. This shift towards a human-centric approach recognizes the pivotal role of human elements in influencing the security and efficiency of SC tracking systems, ensuring a more holistic and effective risk evaluation.

Our focus is concentrated on the security risks associated with SC traceability services, particularly focusing on tracking systems responsible for monitoring critical conditions like temperature and humidity during the transit of assets. We introduce a specialized risk assessment methodology designed to specifically evaluate the security risks in SC tracking systems. This methodology incorporates established risk assessment standards and threat modelling techniques (NIST, 2012), (Casey, 2007). It takes into consideration the specific IT components (assets) utilized in SC tracking systems, their technical features, and realistic threat agents pertinent to the SC environment. Our primary objective is to determine if security breaches initiated by SC-specific threat agents can lead to substantial security threats against the designated hardware and software IT components within SC networks. To showcase the practicality and efficacy of our proposed method, we provide a proof of concept demonstration, grounded in a real-case scenario. This approach is now enhanced by placing a strong emphasis on human factors, recognizing their crucial impact on the security and functionality of SC tracking systems, and ensuring a more comprehensive and effective risk assessment.

THE RISK ASSESSMENT METHODOLOGY ARCHITECTURE

The methodology, as depicted in Figure 1, offers a comprehensive framework tailored to assess security risks in SC tracking systems, incorporating human factors into its core. It aligns with the NIST 800–30 risk assessment guide (NIST, 2012) and integrates the threat modeling principles of Intel's TAL model (Casey, 2007), while also considering the latest ENISA threat landscape (Enisa, 2021). This approach not only categorizes common asset types in SC traceability, such as edge devices and data processing systems, but also emphasizes the role of human interaction with these assets. By acknowledging the human element, the methodology adapts to different SCs, recognizing the variability in human behavior and its impact on security risks. This inclusion of human factors, alongside the technical aspects, ensures a more holistic and realistic assessment of the security challenges in SC tracking systems.

Stakeholder Analysis

In the development of our SC security assessment methodology, we have identified a structured approach encompassing several crucial steps to comprehensively evaluate the security posture of companies participating in the SC system. The first pivotal step involves a meticulous analysis of the security policies employed by these companies. This initial examination allows us to gain insight into the existing security frameworks, protocols, and measures that each organization has in place. By scrutinizing these policies, we can identify potential vulnerabilities and gaps in their security practices.

After the policy analysis, the second step entails the formulation of precise technical requirements. These requirements encompass various aspects crucial to SC security, such as:

- Determining the minimum lifetime of tracking devices,
- Specifying the level of tracking granularity (whether per box, package, or product),
- Defining the data recorded during storage,
- Ensuring end-to-end sensor discrimination capabilities,
- Outlining the tracking data recorded during transportation, and
- Considering other pertinent technical specifications.

Each of these technical requirements is meticulously crafted to align with industry standards and best practices, ensuring that they contribute to the overall security enhancement of the SC system. Furthermore, this step involves a granular assessment of the assets within the SC, affording us the opportunity to assess each asset individually, identify potential vulnerabilities, and tailor security measures accordingly. By adopting this comprehensive approach, our methodology seeks to address the multifaceted nature of SC security and facilitate a robust security framework that safeguards critical assets throughout the SC process.

Methodology Main Process

In the next step of our methodology, we leverage the valuable information extracted from the previous phases, as illustrated in Figure 1.

First Step

This critical step consists of two integral parts, with the first part focusing on threat assessment. In this context, our approach encompasses a comprehensive listing of threats and threat agents, aimed at creating a robust security threat assessment framework for each asset within the SC.

To initiate this process, we employ a threat agent categorization methodology based on the features outlined in the INTEL TAL standard (Casey, 2007). This approach allows us to construct a targeted threat agent map, encompassing all potential threat agents that could be involved and possess varying degrees of influence on the security of different types of SCs. By incorporating this map into our methodology, we enhance our SC threat model, enabling a more refined understanding of the security landscape.

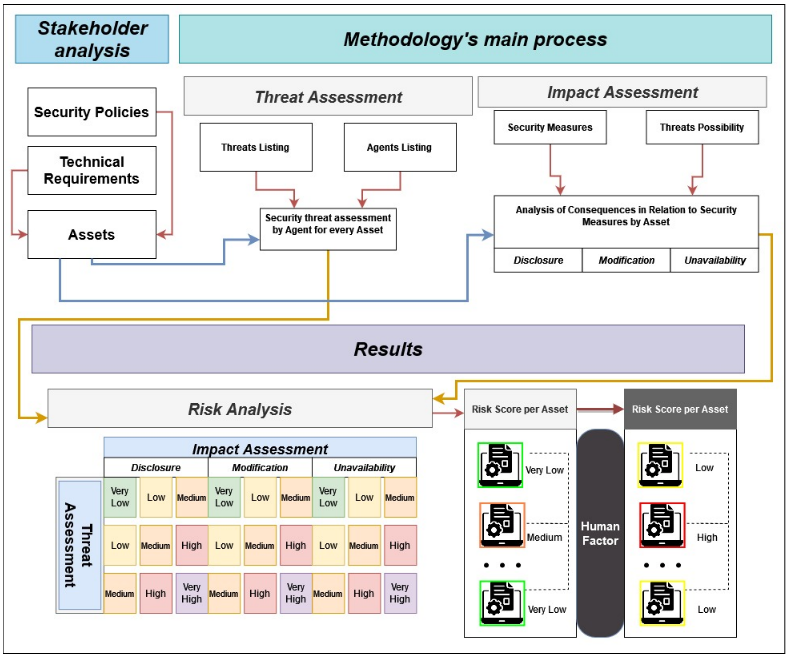
To further refine our threat assessment, we utilize a three-level classification system (Low-Medium-High) to determine the likelihood of occurrence for each threat agent within a specific threat concerning an asset. This classification aids in quantifying the potential impact of threat agents on SC security. Some notable agents within our examination may include:

- Employee (Irresponsible, Untrained, or Reckless),
- Competitor,
- Data Miner,
- Disgruntled Employee,
- Scammer,

- Cyber-Criminal,
- Others.

The next critical aspect of this step involves threat categorization. Each identified threat agent may potentially trigger one or more threats specific to the corresponding system assets. Some notable threats within our examination include:

- Data Modification,
- Data Leakage,
- Unauthorized Access,
- Destruction,
- Malfunction,
- Side-channel Attacks,
- Others.



Impact Assessment	Disclosure			Modification			Unavailability		
Threat Assessment	Very Low	Low	Medium	Very Low	Low	Medium	Very Low	Low	Medium
	Low	Medium	High	Low	Medium	High	Low	Medium	High
	Medium	High	Very High	Medium	High	Very High	Medium	High	Very High

Figure 1: Methodology.

Second Step

In the next step of this phase of our methodology, we shift our focus to impact assessment. This pivotal step is based on the synthesis of security measures and the possibility of threats, resulting in a comprehensive analysis of the potential consequences concerning the security measures for each individual asset. Our assessment primarily revolves around the aspects of disclosure, modification, and unavailability.

To initiate this process, we begin with a threat's possibility per asset. At this juncture, each threat undergoes a meticulous examination, specifically regarding each system asset. We evaluate the applicability of each threat to each asset under consideration, taking into account the capabilities of threat agents, i.e., examining whether a threat agent is capable enough to activate the respective threat. For each asset deemed susceptible to a particular threat, we assess the likelihood of that threat occurring. This assessment employs a three-level qualitative scale for threat likelihood, categorized as follows:

Low Threat Level: This category characterizes threats that, while deemed potentially actionable, carry a relatively low estimated probability of occurrence, typically less than a 10% probability of occurrence per year.

Medium Threat Level: Threats in this category have an increased estimated probability of occurrence, typically falling between a 10% and 30% probability of occurrence per year.

High Threat Level: This category pertains to threats with a high estimated probability of occurrence, typically exceeding a 30% probability of occurrence per year.

Following the Threats Inventory per SC step, we proceed to the Security Requirements Inventory per SC. In this phase, we combine the information obtained from the Threats Inventory per SC with the data from the security requirements assessment. This integration results in a comprehensive table that correlates each threat identified in the Threats Inventory with one or more of the twenty-two security requirements. The outcome is a detailed report summarizing the specific security requirements applicable to each individual asset.

The subsequent step involves the creation of a Security measures Inventory per SC. For each asset represented in the table, we meticulously evaluate the potential consequences associated with the violation of the three fundamental security properties, namely disclosure, modification, and unavailability of data pertaining to the asset in question. This assessment is carried out in accordance with established risk assessment standards, drawing from guidelines based on ISO/IEC 27005:2008 and NIST SP 800–30. By systematically analyzing these measures, our methodology provides a comprehensive understanding of the potential security risks specific to each SC, aiding in the development of targeted risk mitigation strategies.

Results

The final phase concerns the production of risk estimation results. Specifically, it generates a comprehensive table that meticulously outlines the assessed risk associated with each category of assets concerning the potential threats related to each individual asset within every SC. This risk estimation is conducted with due consideration of the three fundamental security principles: Disclosure, Modification, and Unavailability.

To effectively convey the assessed risk, we employ a refined scale consisting of five distinct values (0, 1, 2, 3, 4). This scale is derived from the classical low, medium, high risk assessment framework and is structured as a two-parameter matrix. It allows for a more granular evaluation of risk levels, ensuring a comprehensive and precise representation of potential security risks within the SC system.

The culmination of the risk estimation process involves the introduction of a human factor filter. This filter is applied to every asset where a specific threat agent is deemed applicable for threat implementation. In instances where such applicability exists, the risk scores are elevated by one level. Consequently, this filter serves to elevate risks from a low to a medium level, enhancing the accuracy of risk assessment and reflecting the potential impact of human factors on security outcomes.

Incorporating this human factor filter into our risk estimation process enhances the methodology's capacity to capture and account for the dynamic interplay between threat agents and assets, ultimately resulting in a more refined and comprehensive evaluation of security risks within the SC.

IMPLEMENTATION ON A REAL CASE SCENARIO AND RESULTS

Figure 2 provides an overview of the architecture of the real case system concerning SC management, focusing on data and system security. In general, the architecture integrates various security technologies such as blockchain, Internet of Things (IoT), and encryption. The system aims to ensure the secure and efficient transfer of data and accurate tracking of products as they move through the SC.

Following the entire process, we incorporate an additional step involving *human factor assessment*. After this final assessment, we present the final score. This allows us to compare the scores generated by our system both before and after considering the influence of human factors. In terms of visual representation in the tables, the presence of blue boxes signifies instances impacted by human factors. Conversely, if there is no blue box in a specific column, it means that the human factor does not influence the threat associated with the asset in question. This approach ensures a thorough evaluation that considers the interplay between automated risk assessment and the nuanced impact of human factors, offering valuable insights into security risks within the SC context.

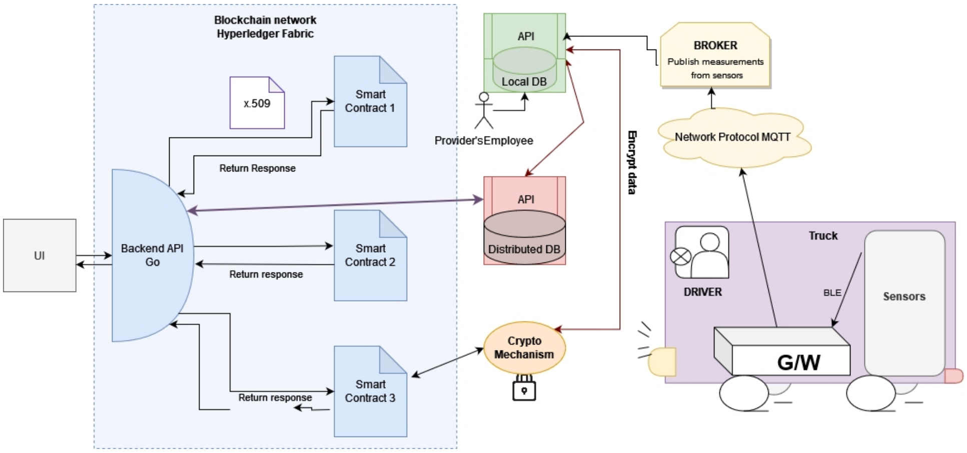


Figure 2: Real case scenario.

In this case, we present not all the results but a part of them. In this scenario, the examined threat agent is a careless worker (truck driver) who initiates the security threats. This part concerns the gateway. The gateway consists of two assets:

- The V2M-Juno r2 (EG1)
- The Raspberry Pi 3 (EG_2).

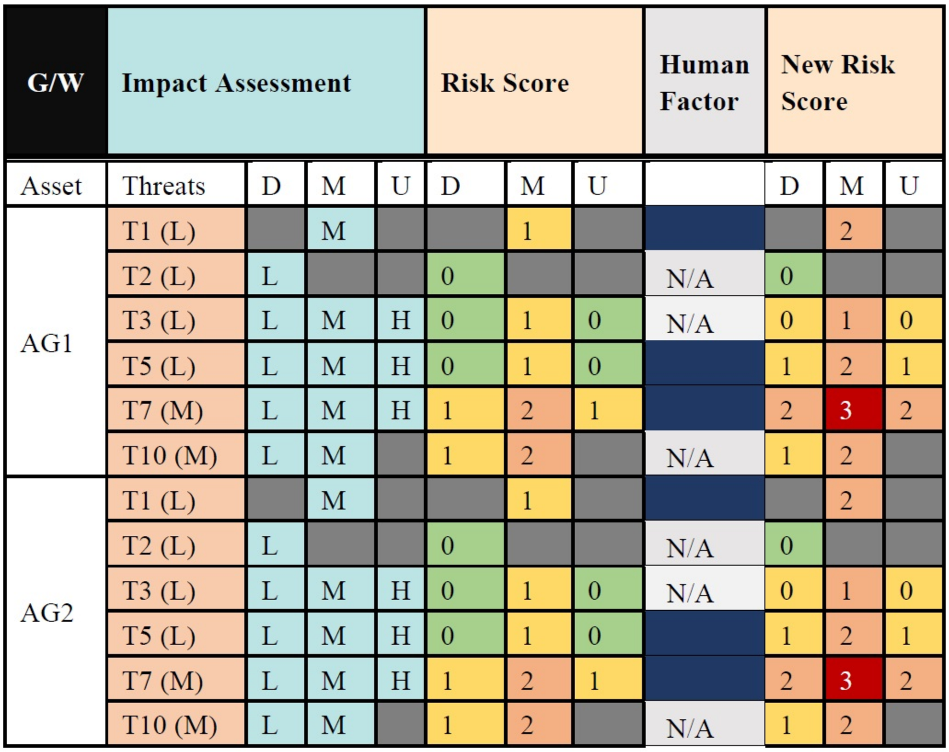
The threats considered are the following:

- T1: Data Modification
- T2: Data Leakage
- T3: Unauthorized Access
- T5: Destruction
- T7: Malfunction
- T10: Side-channel Attack.

Regarding the Asset Gateway - Data Collection Sensors for Product Transport Vehicles, in order to assess the efficiency of the mechanisms, we have introduced an additional step in the risk analysis methodology. We will examine the sum of values in the table before and after the implementation of security measures. According to our calibration, a lower number indicates a safer system.

The initial system scored 20, while the system after the measures scored 34. Therefore, the Asset Gateway system is 1.7 times more vulnerable in case of a human mistake.

Table 1. Risk estimation score – result matrix.



G/W	Impact Assessment				Risk Score			Human Factor	New Risk Score		
Asset	Threats	D	M	U	D	M	U		D	M	U
AG1	T1 (L)		M			1		■		2	
	T2 (L)	L			0			N/A	0		
	T3 (L)	L	M	H	0	1	0	N/A	0	1	0
	T5 (L)	L	M	H	0	1	0	■	1	2	1
	T7 (M)	L	M	H	1	2	1	■	2	3	2
	T10 (M)	L	M		1	2		N/A	1	2	
AG2	T1 (L)		M			1		■		2	
	T2 (L)	L			0			N/A	0		
	T3 (L)	L	M	H	0	1	0	N/A	0	1	0
	T5 (L)	L	M	H	0	1	0	■	1	2	1
	T7 (M)	L	M	H	1	2	1	■	2	3	2
	T10 (M)	L	M		1	2		N/A	1	2	

CONCLUSION

Conducting risk assessments in SC tracking platforms is an increasingly complex and critical task for operational managers, particularly in the context of unexpected, high-impact "black swan" events that carry significant economic implications in the interconnected realm of global SC networks. The methodology we propose addresses this complexity by meticulously refining the operational requirements unique to different types of SCs, thereby pinpointing specific security risks inherent in SC tracking systems.

A key aspect of our approach is the integration of human factors and asset granularity into the risk assessment process. This integration is vital as it acknowledges the nuanced roles that individual human actions and specific asset characteristics play in the security landscape of SC tracking. By modifying existing threat and risk assessment methodologies, our approach not only identifies distinct threats and risks for various types of SCs but also offers a more detailed and human-centric analysis.

This granular focus on both human factors and individual assets ensures a more accurate, tailored, and effective risk assessment, which is crucial for future research and operational strategies in diverse SC scenarios. As evidenced in our case study, this approach can reveal significant variations in operational requirements across different SCs, underscoring the importance of a detailed, human-focused, and asset-specific risk assessment framework in enhancing the security and efficiency of SC tracking systems.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: 'Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594. The 'Human-centered Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042. The 'advaNced cybErsecurity awaReness ecOsystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411. And 'Fostering Artificial Intelligence Trust for Humans towards the optimization of trustworthiness through large-scale pilots in critical domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

REFERENCES

Casey, T. (2007). Threat Agent Library Helps Identify Information Security Risks. *Intel White Paper*, (September), 12. Available at: https://communities.intel.co.jp/servlet/JiveServlet/previewBody/1151-102-1-1111/ThreatAgentLibrary 07-2202w.pdf.

Chen, S., Brahma, S., Mackay, J., Cao, C. & Aliakbarian, B. (2020). The role of smart packaging system in food SC. Journal of Food Science, 85(3), 517–525. Available at: https://ift.onlinelibrary.wiley.com/doi/abs/10.1111/1750-3841.15046.

ENISA. (2021). Landscape for SC Attacks. *ENISA*, (July).

Koutras, D., Malamas, V., Kotzanikolaou, P. & Dasaklis, T. (2023, January). A Risk Assessment Methodology for SC Tracking Services. In *2023 International Conference on Cyber Management and Engineering (CyMaEn)* (pp. 555–559). IEEE.

Neumann, W. P. *et al.* (2021) 'Industry 4.0 and the human factor – A systems framework and analysis methodology for successful development', *International Journal of Production Economics*, 233, p. 107992. doi: 10.1016/j.ijpe.2020.107992.

NIST. (2012). NIST Special Publication 800–30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Guide for Conducting Risk Assessments*, (September), 95.

Papastergiou, S. & Polemi, N. (2018). MITIGATE: A Dynamic SC Cyber Risk Assessment Methodology. In *Lecture Notes in Networks and Systems*, 18, 1–9.

Polemi, N. & Kotzanikolaou, P. (2015). Medusa: A SC risk assessment methodology. In *Communications in Computer and Information Science*, 530, 79–90.

Pollini, A., Callari, T. C., Tedeschi, A. et al. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24, 371–390. Available at: https://doi.org/10.1007/s10111-021-00683-y.

Reiman, A. *et al.* (2021) 'Human factors and ergonomics in manufacturing in the industry 4.0 context – A scoping review', *Technology in Society*, 65, p. 101572. doi: 10.1016/j.techsoc.2021.101572.

Schauer, S., Polemi, N. & Mouratidis, H. (2019). MITIGATE: a dynamic SC cyber risk assessment methodology. *Journal of Transportation Security*, 12(1-2), 1–35.

Sgarbossa, F. *et al.* (2020) 'Human factors in production and logistics systems of the future', *Annual Reviews in Control*, 49, pp. 295–305. doi: 10.1016/j.arcontrol.2020.04.007.