A novel approach: continuous cascade model for assessing security and resilience in IIoT

Emanuel Krzysztoń
Faculty of Computer Science, Kazimierz Wielki University, Chodkiewicza 30 Street, 85-064 Bydgoszcz, Poland
emanuel.krzyszton@ukw.edu.pl

Izabela Rojek
Faculty of Computer Science, Kazimierz Wielki University, Chodkiewicza 30 Street, 85-064 Bydgoszcz, Poland
izabela.rojek@ukw.edu.pl

Dariusz Mikołajewski
Faculty of Computer Science, Kazimierz Wielki University, Chodkiewicza 30 Street, 85-064 Bydgoszcz, Poland
dariusz.mikolajewski@ukw.edu.pl

Jan Cybulski
Faculty of Computer Science, Kazimierz Wielki University, Chodkiewicza 30 Street, 85-064 Bydgoszcz, Poland
jan.cybulski@ukw.edu.pl

Abstract

The paper presents a novel methodology for a continuous cascade model that defines the current state of security and resilience of an Industrial Internet of Things (IIoT) system. The approach integrates system objective definition, critical process and asset identification, and hybrid threat modelling (STRIDE/LINDDUN). Identified threats are correlated with attack techniques using the MITRE ATT&CK for Industrial Control System framework (ICS), while Common Vulnerability Scoring System (CVSS) is employed for vulnerability assessment. Risk quantification adheres to ISO/IEC 27005 guidelines. The paper concludes by discussing the methodology's strengths and limitations, alongside avenues for future research.

Keywords: IIoT; Security; Threat modeling; Vulnerabilities; Risk.

1. Introduction

The current state of organizational security safeguards necessitates streamlining and enhancing existing solutions to effectively counter diverse threats. Industrial systems at the convergence of IT (Information Technology) and OT (Operational Technology), particularly emerging IIoT technologies due to their application, complexity, proliferation, and heterogeneity, require focused attention [13].

IIoT is a comprehensive ecosystem encompassing everything with connectivity, from sensors to extensive infrastructure management systems [3,8,12]. IIoT Consortium presented a three-tier model of IIoT technology architecture [4]. The proposed model was created to ensure and enhance flexibility, scalability and security. Despite the standards that have been introduced, there is a lack of methodologies and methods that consider the specificity of the characteristic threats to IIoT systems [9,13].

Table 1 shows the findings of a thorough analysis of the literature review, indicating the approach taken, the research gaps identified and the directions for further research in ensuring the security and resilience of IIoT systems.

Table 1. Findings of the literature review analysis (own elaboration).

Source	Adopted Approach	Research Gap	Future Research Directions
Zhukabayeva, T. et. al. [13]	system-centric attacker-centric	A literature gap exists regarding IIoT attacks, intrusion methods, and threats.	Creating innovative threat identification techniques.
Ozkan, C. et. al. [10]	attacker-centric asset-centric	Currently, there is no consistent methodology for comprehensively identifying threats in ICS systems.	Analysis based on real-world cases and scenarios with automatic threat mapping.
Khalil, S.M. et. al. [8]	asset-centric attacker-centric system-centric	It is necessary to develop a comprehensive, empirically based risk & threat modelling framework for ICS and to explore new techniques.	Creating robust structures, ensuring consistency with other security processes, and research based on real-world data.
Saurabh, K. et. al. [11]	asset-centric attacker-centric software-centric	A notable gap exists in the standardised identification, evaluation, and prioritisation of IIoT threats.	Real-world testing with dynamic factors and development of systems to support automation.
Zahid, S. et. al. [12]	system-centric asset-centric attacker-centric	IIoT environments lack a consistent, flexible, and objective method for risk identification, assessment, and prioritisation.	Continuing research on risk assessment methods.

With reference to the research gap shown in Table 1, publications confirm the need to develop new methodologies. These methodologies should be tailored to the specifics of OT/IIoT from the perspective of security and resilience. Considering this context, this paper adopted the following research questions (RQ):

RQ 1: How do varied methodological approaches influence the comprehensive assessment of IIoT system security and reliability?

RQ 2: What methods and techniques from other disciplines and areas can be adapted to IIoT systems?

RQ 3: How can the heterogeneity and inherent complexity of IIoT environments be effectively reflected in risk analysis methodologies?

The paper focuses on analysing the main challenges in this area and presenting a novel proposal. The main contribution of this paper includes (ARQ):

ARQ 1: This article presents a novel methodological approach that integrates system, process, asset, attacker, and software considerations into a coherent quantitative risk assessment framework. This provides a hierarchical and cohesive perspective, linking strategic business objectives with technical details and real-world threats.

ARQ 2: For IIoT systems, an adaptation of the business impact analysis (BIA) approach has been put forward to determine critical processes and the importance of assets, along with the implementation of practices and guidelines to guarantee information security in accordance with the ISO/IEC 27005 standard.

ARQ 3: In IIoT contexts, the criticality of impact on physical processes, functional safety, and operational continuity is paramount. This research introduces variable asset importance ($Weight_{sig}(Z_{k,j})$) and α coefficients, whose selection criteria are meticulously defined to directly reflect the unique attributes and architecture of IIoT system.

This work introduces a mathematically formalised methodology assessment in IIoT risk analyses through a continuous, cascading process.

2. Methodology

Illustrated in Figure 1 methodology facilitates understanding system processes (K), identifying critical ones by prioritizing physical and operational consequences. This is achived through a streamlined Business Impact Analysis (according to ISO 22317 [5]). It then involves defining measurable criteria for evaluating the impact. Subsequently pinpointing key (e.g., personnel, physical assets, infrastructure, services) essential for these processes ($z_{k,j}$). To each essential asset is assigned a significance weight $Weight_{sig}(Z_{k,j}) \in [0,1]$ where value is determined through expert elicitation and functional analysis based on adopted criteria. Upon identifying these assets ($z_{k,j}$), potential threats ($T_{k,j}$) are identified using a hybrid STRIDE [8] (security-focused) and LINDDUN [9] (privacy-focused) approach and then mapped to attack techniques within the MITRE ATT&CK for Industrial Control Systems (ICS) [1,7] framework ($t_{k,j,r}$). This step specifically addresses the uniqueness of IIoT threats by aligning with real-world ICS attack techniques. Subsequently, a vulnerability assessment employing the CVSS metric [2] ($V_{k,j,r}$) is conducted to assess the technical severity of the underlying vulnerability. CVSS provides a numerical score from 0 to 10 based on exploitability and impact. These scores are derived through expert judgment based on the technical characteristics of the vulnerability and attack vector. Potential impact of the materialized threat ($U_{k,j,r}$) on the IIoT system's objectives is quantified on a scale of $[0,1]$ assessment directly correlates with the criticality criteria defined for the system aligned with ISO/IEC 27005 guidelines [4], aiming to determine the likelihood and potential impact of identified assets and threats on IIoT system security and resilience.

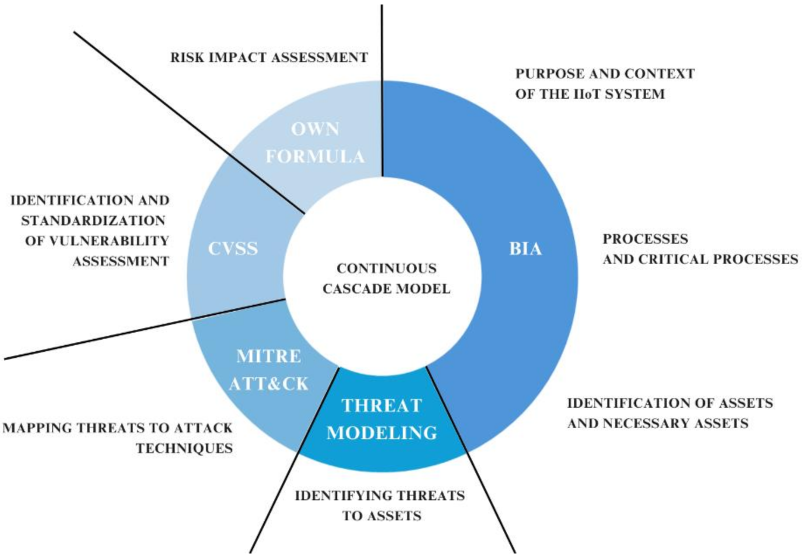
RISK IMPACT ASSESSMENT
PURPOSE AND CONTEXT OF THE IIoT SYSTEM
OWN FORMULA
IDENTIFICATION AND STANDARDIZATION OF VULNERABILITY ASSESSMENT
CVSS
CONTINUOUS CASCADE MODEL
BIA
PROCESSES AND CRITICAL PROCESSES
MITRE ATT&CK
THREAT MODELING
IDENTIFICATION OF ASSETS AND NECESSARY ASSETS
MAPPING THREATS TO ATTACK TECHNIQUES
IDENTIFYING THREATS TO ASSETS

Fig. 1. Model schema for ensuring the security and resilience of the IIoT system (own elaboration).

3. Mathematical representation of the adopted methodology

The methodology has been expressed using a hierarchical approach, aggregating risk from individual threats to overall system risk.

3.1. Risk of an individual threat to an asset (1)

The risk for a given threat ($t_{k,j,r}$) affecting an important asset ($Z_{k,j}$) in critical process (K) calculated as the product of the normalized vulnerability score ($\frac{V_{k,j,r}}{10}$) and its potential impact ($U_{k,j,r}$) to a scale from 0 to 1 allows for consistent comparison with the impact assessment. This formula quantifies the direct risk of a single threat's materialization.

$$R_{k,j,r} = \frac{V_{k,j,r}}{10} \times U_{k,j,r} \tag{1}$$

3.2. Risk of an significant asset (2)

The risk for an significant asset ($z_{k,j}$) within critical process (K) is calculated as a weighted average of the risks of all identified threats ($T_{k,j}$) affecting that asset. The asset's importance weight ($Weight_{sig}(Z_{k,j})$) reflects its criticality to the functioning of its associated process. The average threat risk is the sum of individual threat risks divided by their count, incorporating a function δ ($|T_{k,j}|$), which prevents division by zero in the case of no threats (in which case the asset risk is 0).

$$R_{k,j} = Weight_{sig}(Z_{k,j}) \times \left(\frac{\sum t_{k,j,r} \in T_{k,j}\{R_{k,j,r}\}}{|T_{k,j}| + \delta\left(|T_{k,j}|\right)} \right) \tag{2}$$

3.3. Overall IIoT system risk (3)

The last formula to calculate risks of significant assets in order to obtain an overall system risk assessment. This holistic measure combines the average risk across all assets and critical processes with the maximum identified asset risk, weighted by a coefficient α. Functions $\delta(|I_k|)$, $\delta\ (|K|)$ prevent division by zero in the case of a lack of significant assets in the critical process or a lack of critical processes. The second part of formula (3) identifies the highest risk among all significant assets in all critical processes. The weight of this maximum risk is determined by (1−α). The total system risk is therefore a weighted sum of the average risk and the maximum risk. The weight α in this sum allows for adjusting whether greater emphasis is placed on the overall risk level or on individual, most significant asset.

$$R_{system} = \alpha \times \left(\frac{\sum k \in K\ (\frac{\sum z_{k,j} \in I_k\{R_{k,j}\}}{|I_k| + \delta(|I_k|)}}{|K| + \ \delta\ (|K|)} \right) + (1 - \ \alpha) \times (max_{k \in K}(max_{Z_{k,j} \in I_k}\{R_{k,j}\})) \tag{3}$$

4. Discussion

4.1. Case study for assessing a novel approach

Methodology was tested in an agri-food organisation. Data was collected through interviews with decision-makers and analysis of the documentation, equipment, and software of the IIoT system. This allowed for an understanding of the system's architecture and dependencies. Subsequently, based on defined evaluation criteria, 11 critical processes and 34 significant assets were identified. A total of 442 threats to these assets were identified, with 238 of them mapped to attack techniques for ICS systems, which increased the objectivity of the threat assessment and the significance of the assets ($Weight_{sig}(Z_{k,j})$). Following this, the vulnerabilities of the assets were assessed after normalising the values. Finally, a parameter (α) incorporating all dependencies was determined. The final security assessment of the IIoT system was 0.639. This dimensionless result reflects the overall security status of the IIoT system, indicating a moderately high level of risk according to the adopted range.

4.2. Limitations of the study

Despite the adoption of standards, IIoT risk assessments exhibit inherent subjectivity, stemming from reliance on expert judgment. This leads to inconsistent and incomparable outcomes. While the model incorporates asset importance ($Weight_{sig}(Z_{k,j})$) and a weighting factor (α) to account for complex IIoT interactions, its linear expression of risk oversimplifies these dynamics. Furthermore, the model presents a static risk profile, failing to account for the evolving nature of threats and system configurations, thereby necessitating continuous updates. Crucially, the absence of probabilistic dependency considerations precludes the direct depiction of risk escalation following individual component failures.

4.3. Future research directions

To overcome the identified limitations and further improve the methodology, upcoming studies should consider:

- Automating data acquisition and standardising assessment criteria.
- Developing dynamic, real-time assessment capabilities for IIoT security.
- Mapping complex risk propagation and exploring advanced, non-linear risk models.
- Analyzing the asset importance ($Weight_{sig}(Z_{k,j})$) and α coefficients impact to create standardized contextual selection guidelines.
- Establishing transparent efficacy metrics and applying the methodology across diverse industries.

5. Summary

This study contributed on a novel continuous cascade model methodology for assessing IIoT system security and resilience. The methodology mathematically formalises risk aggregation from individual threats to overall system risk, incorporating IIoT architecture complexity factors. Despite its strengths, challenges such as subjective assessment, static risk profiles, and a lack of probabilistic dependency consideration remain, indicating avenues for future research.

Appendix A (definitions of variables)

T - a collection of all possible threats in the IIoT system.
V - a collection of all possible vulnerabilities in the IIoT system
I - a collection of all possible impacts in the IIoT system.
K - a collection of all critical processes in the IIoT system.
I_k - a collection of significant assets in a critical process $k \in K$.
$z_{k,j}$ - the j-th significant asset in the critical process, where k , where $z_{k,j} \in I_k$.
$T_{k,j}$ - a collection of threats identified for the significant asset $z_{k,j}$.
$t_{k,j,r}$ - r -th threat identified for the significant asset $z_{k,j}$, where $t_{k,j,r} \in T_{k,j}$.
$V_{k,j,r}$ - vulnerability assessment for the threat $t_{k,j,r}$ (on the CVSS scale from 0 to 10).
$U_{k,j,r}$ - assessment of the potential impact of the threat $t_{k,j,r}$ (scale from 0 to 1).
$Weight_{sig}(Z_{k,j})$ - importance weight of the asset $z_{k,j}$ for the critical process k, where $Weight_{sig}(Z_{k,j}) \in [0,1]$.
α - weight coefficient assigned to the average risk of the system, where $\alpha \in [0,1]$.
$\delta(n)$ - the function returns 1, if $n = 0$, or 0 otherwise.

References

1. CISA. Best Practices for MITRE ATT&CK® Mapping (2023) https://www.cisa.gov/sites/default/files/2023/01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf. Accessed April 2, 2025.
2. Common Vulnerability Scoring System version 4.0: Specification Document. (2023), https://www.first.org/cvss/v4-0/specification-document. Accessed April 2, 2025.
3. Czeczot, G., Rojek, I., Mikołajewski, D., Sangho, B.: AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes. Electronics. 12(18), 3800 (2023).
4. Industry IoT Consortium (IIC) (2022), The Industrial Internet Reference Architecture, Version 1.10. https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf. Accessed April 2, 2025.
5. ISO/IEC: Information security, cybersecurity and privacy protection —Information security management systems —Requirements. ISO/IEC 27005:2022 (2022).
6. ISO/TS: Security and resilience — Business continuity management systems — Guidelines for business impact analysis ISO/IEC 22317:2021 (2021).
7. Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L.T.H., Lim, H.W., Sikdar, B., MITRE ATT&CK Applications in Cybersecurity and The Way Forward. https://arxiv.org/abs/2502.10825 (2025).
8. Khalil, S.M., Bahsi, H., Korõtko, T.: Threat Modeling of Industrial Control Systems: A Systematic Literature Review. Comput. Secur. 136, 103543 (2024).
9. Krzysztoń, E.: AI system in the context of: threat modeling, its risk management and regulatory requirements. Stud. Mater. Inf. Stosow. 16(3), 24-33 (2024).
10. Ozkan, C., Singelee, D.: Evidence-Based Threat Modeling for ICS. arXiv preprint, arXiv:2411.19759 (2024).
11. Saurabh, K., Gajjala, D., Kaipa, K., et al.: TMAP: A Threat Modeling and Attack Path Analysis Framework for Industrial IoT Systems (A Case Study of IoM and IoP). Arab J Sci Eng. 49, 13163–13183 (2024).
12. Zahid, S., Mazhar, M.S., Abbas, S.G., Hanif, Z., Hina, S., Shah, G.A.: Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. 3 Internet of Things. 22, 100766 (2023).
13. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., Alnazzawi, N.: Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. Sensors. 25, 213 (2025).