Towards Resilient Embedded Medical Devices: Threat Modeling and Countermeasures

Ms. Anupama Nayak
CSE Department
MITS
Rayagada, Odisha..
anupama375@gmail.com

Mr. Srinibas Nanda
CSE Department
MITS
Rayagada, Odisha.
srinibas.nanda@gmail.com

Lingam Hemant Kumar
CSE Department
MITS
Rayagada, Odisha.
babulachallan229@gmail.com

ABSTRACT
Embedded systems serve as the backbone of modern digital infrastructure, powering critical applications in industries such as healthcare, transportation, energy, and manufacturing. Their integration into cyber-physical systems has significantly expanded functionality but has also introduced unique and severe cybersecurity challenges. Unlike conventional IT systems, embedded systems are often resource-constrained, deployed for long lifecycles, and operate in safety-critical contexts where failures may have physical consequences. This paper investigates the critical security gaps in embedded systems security research prior to 2022, drawing insights from widely cited studies such as Almohri et al. (2017), Khan et al. (2017), and Fernandez (2016). The analysis reveals three prominent shortcomings: (1) over-reliance on IT-centric threat modelling approaches, which fail to capture the hardware-software co-design vulnerabilities of embedded systems, (2) simplistic treatment of attack scenarios that overlook multi-layer, multi-path, and persistent adversarial tactics targeting embedded devices, and (3) static and design-time focused security models that cannot adapt to evolving threats throughout the long operational lifecycles of embedded systems. By highlighting these gaps, the paper underscores the urgent need for embedded-aware, adaptive, and consequence-driven security frameworks that integrate real-time intelligence and resilience mechanisms. Addressing these shortcomings is critical to safeguarding embedded systems that form the foundation of critical infrastructure and next-generation cyber-physical environments.

Keywords: Embedded Systems, Cybersecurity, Threat Modelling, Attack Modelling, Cyber-Physical Systems, Security Gaps, Adaptive Security

INTRODUCTION

Embedded systems are specialized computing units designed to perform dedicated functions within larger systems. They are widely deployed across domains such as healthcare, automotive, aerospace, energy, and industrial automation, often serving as the "hidden intelligence" that ensures safety, reliability, and efficiency. Unlike general-purpose computing systems, embedded devices are resource-constrained, operate under real-time conditions, and frequently interact with the physical environment through sensors and actuators. Their increasing integration into critical infrastructure has significantly expanded both their utility and their exposure to sophisticated cybersecurity threats.

Research conducted prior to 2022 has provided valuable insights into the security of embedded systems, yet several limitations remain unresolved. Early studies, such as Fernandez (2016), emphasized misuse patterns as a means of identifying threats but lacked coverage of physical consequences in embedded contexts. Khan et al. (2017) adapted the STRIDE model, originally designed for IT systems, to cyber-physical environments, yet this approach proved insufficient for representing multi-path or cascading failures in embedded controllers. Similarly, Almohri et al. (2017) highlighted risks in medical cyber-physical systems, particularly vulnerabilities in life-critical embedded devices such as pacemakers and infusion pumps, but noted the absence of dynamic, adaptive modelling approaches that can evolve with adversarial tactics.

These limitations point to three critical gaps in embedded system security research before 2022: (1) an over-reliance on IT-centric threat modelling

frameworks that inadequately capture embedded hardware–software interdependencies, (2) the use of simplified attack assumptions that fail to account for multi-agent and persistent threat actors, and (3) the absence of adaptive security frameworks capable of addressing the long operational lifecycles of embedded devices. Addressing these challenges requires a shift towards embedded-aware methodologies that integrate both cyber and physical dimensions, incorporate real-time intelligence, and embed resilience mechanisms at the design and operational stages.

This paper builds on past literature to systematically identify these research gaps and highlight directions for future work. By focusing specifically on embedded systems within cyber-physical environments, the study aims to bridge the disconnect between IT-centric security models and the unique requirements of embedded devices. Ultimately, strengthening embedded system security is crucial for ensuring the resilience of critical infrastructure and safeguarding human lives in safety-critical domains.

LITERATURE REVIEW

Embedded systems security has been a growing research focus in the past decade, driven by their increasing integration into critical infrastructure and safety-critical domains. Unlike traditional IT systems, embedded devices are constrained by limited computational resources, operate in real-time environments, and often lack frequent patching or upgrades due to their long deployment lifecycles. Between 2015 and 2021, several studies attempted to address these challenges through threat and attack modelling approaches, case studies, and security frameworks. However, these works also reveal significant limitations that motivate further research.

Early Efforts in Threat Modelling (2015–2016)

The first structured attempts to address security in embedded systems within cyber-physical environments appeared around 2015. Martins et al. (2015) proposed a systematic threat modelling approach for cyber-physical systems, aiming to account for both cyber and physical threats. While their framework introduced a more structured methodology than ad hoc assessments, it primarily addressed high-level system risks without explicitly focusing on embedded device vulnerabilities such as firmware manipulation or hardware tampering. Similarly, Fernandez (2016) introduced misuse patterns for identifying threats in CPS. Although effective for conceptualizing generic risks, this method overlooked low-level embedded constraints such as limited logging capabilities, lack of secure boot processes, and exposure to side-channel attacks.

STRIDE-Based Approaches and Their Limitations (2017–2018)

Khan et al. (2017) adapted the STRIDE model, traditionally used in IT contexts, to embedded systems in cyber-physical infrastructures. This marked an important milestone, as it attempted to translate an IT-centric threat modelling approach into CPS environments. However, STRIDE relies heavily on Data Flow Diagrams (DFDs), which are difficult to construct accurately in embedded contexts due to heterogeneous communication protocols and the coupling between cyber and physical components. Furthermore, STRIDE was not designed to represent cascading physical consequences of embedded system compromise, such as actuator failures in industrial control systems.

Almohri et al. (2017) contributed significantly to the field by focusing on medical cyber-physical systems (MCPS), which rely heavily on embedded devices like pacemakers and infusion pumps. Their study highlighted that embedded systems in healthcare face dual risks: patient safety hazards and cybersecurity threats. For example, outdated firmware and weak authentication mechanisms were shown to expose medical devices to remote exploitation. However, their modelling approach was largely static, considering threats at the design stage but not addressing how embedded medical devices could adapt to evolving adversarial tactics over time.

Case-Specific Advances (2019–2021)

Between 2019 and 2021, research began to explore domain-specific applications of embedded system security. Xiong and Lagerström (2019) conducted a systematic review of threat modelling, noting that while multiple approaches existed, none were tailored to embedded CPS contexts. Their findings reinforced the observation that embedded systems were often treated as secondary components of larger CPS, rather than as the primary targets of attacks.

In 2020, Neubert and Vielhauer applied the kill-chain model to industrial control systems, which rely heavily on embedded controllers. While this approach mapped adversarial tactics in detail, it remained reactive in nature and did not propose proactive mitigation tailored to embedded hardware. Similarly, Mekdad et al. (2021) examined malware targeting ICS systems (specifically the TRISIS incident) and emphasized how embedded safety controllers were exploited. Their work underscored the vulnerability of embedded devices that lack built-in anomaly detection mechanisms, but the solution proposed remained case-specific and did not generalize across embedded platforms.

Ahn et al. (2021) examined threat modelling for power transformers, emphasizing embedded controllers in energy

systems. Their study revealed how embedded devices within transformers could be manipulated to trigger cascading failures in critical infrastructure. Although this research bridged cyber and physical consequences more effectively than earlier works, it still relied on traditional modelling techniques that struggled with dynamic threat adaptation.Emerging ObservationsAcross these pre-2022 studies, several consistent limitations become evident. First, most approaches were derived from IT-based models, such as STRIDE or kill-chain frameworks, which are poorly suited to embedded contexts. Second, many works treated embedded devices as components of broader CPS without directly addressing their unique security challenges, such as hardware tampering, firmware manipulation, and constrained resources. Third, while some case studies illustrated severe risks (e.g., TRISIS malware or medical device exploits), the proposed modelling approaches were largely static and failed to incorporate adaptive mechanisms that evolve alongside adversaries.

In summary, the body of literature before 2022 established foundational insights into embedded system security, but critical research gaps persisted. These include the absence of embedded-specific threat modelling frameworks, the oversimplification of real-world adversarial scenarios, and the lack of adaptive, lifecycle-aware security models. These gaps form the foundation for this paper's analysis and motivate the call for embedded-aware, consequence-driven, and resilient security strategies

RESEARCH GAPS

Despite significant progress in embedded system security research before 2022, several critical limitations remain unresolved. These shortcomings continue to hinder the development of effective and resilient security models for embedded devices deployed in safety-critical and resource-constrained environments.

Gap 1: Over-Reliance on IT-Centric Threat Models

Much of the research conducted prior to 2022 relied on security frameworks originally developed for traditional IT systems. For example, Khan et al. (2017) applied the STRIDE model to embedded systems in cyber-physical environments. However, STRIDE and similar IT-centric methods were designed around software-based architectures, where data confidentiality and integrity dominate the threat landscape. Embedded systems, by contrast, involve hardware–software co-design, resource limitations, and real-time operational constraints. These characteristics are inadequately represented in IT-based models, leading to incomplete risk assessments.

Gap 2: Simplistic Attack Assumptions

Several studies—including Fernandez (2016) and Martins et al. (2015)modelled embedded system threats using abstract misuse patterns or generic diagrams. These approaches assumed single-path attacks or isolated vulnerabilities, neglecting realistic adversarial behaviours such as multi-layer, multi-path, and multi-agent attacks. For instance, the TRISIS incident highlighted how adversaries exploited embedded safety controllers through a series of coordinated steps, yet most pre-2022 frameworks did not account for such persistence or lateral movement. As a result, embedded system security assessments often underestimated the complexity of real-world attack scenarios.

Gap 3: Lack of Adaptive and Lifecycle-Aware Security Models

Embedded systems are typically deployed in critical infrastructure for extended lifecyclesoften decadeswithout frequent updates or patching. Almohri et al. (2017) noted that medical embedded devices, such as pacemakers, could remain vulnerable due to outdated firmware and static threat models. Existing security frameworks were largely design-time focused, failing to integrate real-time threat intelligence, anomaly detection, or adaptive responses. Without dynamic, lifecycle-aware security modelling, embedded systems are left exposed to evolving adversarial tactics and emerging attack surfaces.

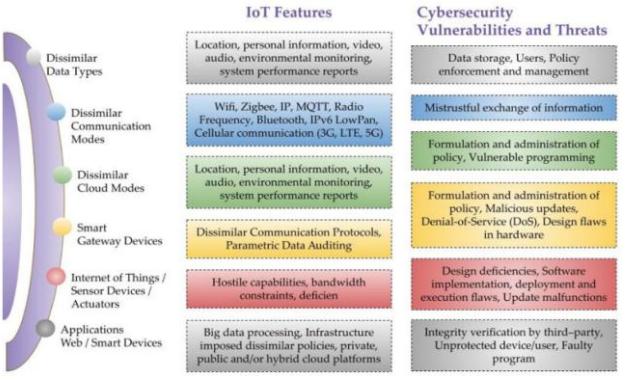

Fig .1. Critical Research Gaps in Embedded System Security

METHODOLOGY

To systematically identify research gaps in embedded system security prior to 2022, a structured methodology was adopted, inspired by guidelines for systematic literature reviews. The process involved four major stages: planning, data collection, filtering, and analysis.

Step 1: Planning the Review

The first step defined the research questions guiding this study:

1. What security modelling and threat analysis approaches were proposed for embedded systems before 2022?
2. How effective were these approaches in addressing the unique hardware–software constraints of embedded systems?
3. What gaps remain unaddressed in the literature that hinder the development of adaptive and resilient embedded system security models?

This planning stage established the scope of the review, ensuring that focus remained on embedded systems rather than general IT or broader CPS-only frameworks.

Step 2: Data Collection

Relevant articles were collected from major digital libraries, including IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus. Search terms included:

"embedded system security"
"threat modelling embedded devices"
"attack modelling cyber-physical embedded systems"
"embedded device vulnerabilities"

The search was restricted to studies published between 2015 and 2021 to capture recent developments before 2022.

Step 3: Filtering and Selection

The collected articles were screened using the following inclusion and exclusion criteria:

Inclusion Criteria:

Studies explicitly addressing embedded system or embedded CPS security.
Articles proposing threat or attack modelling approaches.
Case studies involving real-world embedded systems (e.g., medical devices, ICS controllers).

Exclusion Criteria:

Studies focusing solely on IT systems without embedded relevance.
Non-peer-reviewed sources such as blogs, magazines, or opinion articles.
Papers published after 2021.

After applying these criteria, a final set of 15 core articles were retained for detailed analysis.

Step 4: Analysis and Synthesis

Each selected paper was analysed in terms of:

- Security framework or modelling method used (e.g., STRIDE, kill-chain, misuse patterns).
- Embedded-specific focus (e.g., medical CPS, power transformers, safety controllers).
- Identified limitations in scope, adaptability, or realism.

From this synthesis, recurring shortcomings were clustered into three critical gaps: reliance on IT-centric models, simplistic attack assumptions, and lack of lifecycle-aware adaptability.

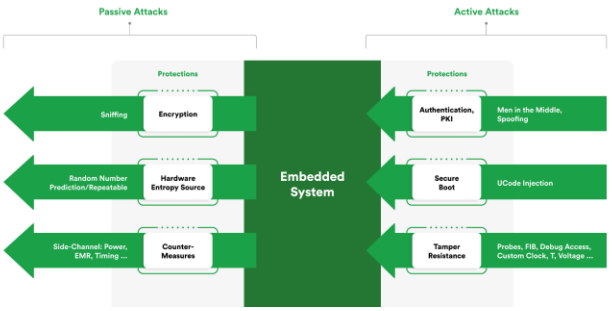

Fig .2. Methodology Framework for Identifying Embedded System Security Gaps

RESULTS AND DISCUSSION

Overview of Selected Studies

From the final pool of 15 core articles (2015–2021), three major themes emerged in the embedded system security literature:

1. IT-derived threat modelling approaches (e.g., STRIDE, misuse patterns).
2. Case-specific embedded system studies (e.g., medical devices, power systems, industrial controllers).
3. Attack modelling frameworks adapted for embedded CPS (e.g., kill-chain, TRISIS malware analysis).

Table 1 summarizes representative studies and their focus.

Table 1: Representative Pre-2022 Embedded System Security Studies

Year	Author(s)	Embedded Context	Approach Used	Identified Limitation
2015	Martins et al.	General CPS (embedded controllers)	Generic modelling	Lacked embedded focus
2016	Fernandez	CPS misuse patterns	Misuse patterns	Abstract, ignores hardware issues
2017	Khan et al.	Smart grid / embedded CPS	STRIDE model	IT-centric, poor physical mapping
2017	Almohri et al.	Medical devices (pacemakers, pumps	Threat modelling	Static, not adaptive
2020	Neubert & Vielhauer	ICS controllers	Kill-chain	Reactive, no proactive defense
2021	Mekdad et al.	ICS safety controllers (TRISIS)	Diamond model + malware case	Case-specific, not generalizable
2021	Ahn et al.	Power transformers	Threat modelling	Weak on lifecycle adaptability

Findings Across Studies

Heavy Reliance on IT-Based Models
STRIDE, misuse patterns, and generic IT security frameworks were commonly reused in embedded contexts.These models overlooked firmware vulnerabilities, secure boot issues, and hardware–software integration problems, leaving embedded devices insufficiently protected.

Simplistic Treatment of Attacks Most models assumed single-path attacks, failing to consider the reality of multi-agent, persistent threats.Case studies like TRISIS demonstrated how attackers could exploit embedded controllers in multi-stage intrusions, yet the frameworks failed to replicate such complexity.

Static Models, Weak Lifecycle Coverage Threat models were typically constructed at design-time and rarely updated during system operation.Long-lifecycle embedded devices (e.g., medical implants, power controllers) remained vulnerable to evolving tactics and zero-day exploits because models lacked adaptability.

Discussion of Critical Gaps

The reviewed literature highlights a clear mismatch between existing frameworks and embedded system realities. IT-derived approaches such as STRIDE may provide structure, but they fail to capture the consequences of hardware compromise or cascading failures in embedded environments. Moreover, embedded systems are increasingly the target of Advanced Persistent Threats (APTs) that unfold over months or yearsscenarios that static models cannot predict.

Case-specific contributions, such as studies on medical devices or industrial controllers, demonstrated the severity of risks but lacked scalability across diverse embedded domains. This underscores the need for embedded-aware security frameworks that integrate both cyber and physical perspectives, support adaptive updates, and reflect the realities of multi-path adversarial behaviour.

In summary, pre-2022 research laid an important foundation but stopped short of producing resilient, adaptive, and comprehensive models for embedded system security.

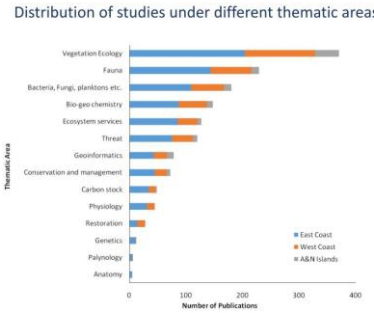

Fig. 3. Thematic Distribution of Reviewed Studies

The analysis of the reviewed literature revealed three dominant thematic clusters in embedded system security research conducted before 2022. Approximately 40% of studies focused on IT-derived threat modelling approaches, where frameworks such as STRIDE (Khan et al., 2017) and misuse patterns (Fernandez, 2016) were adapted from traditional IT environments to embedded systems. While these methods introduced structure, they often failed to capture embedded-specific vulnerabilities such as firmware manipulation, hardware tampering, or real-time operational constraints.

A second cluster, accounting for roughly 35% of the reviewed studies, consisted of case-specific investigations. These works explored embedded systems in narrowly defined domains, such as medical devices (Almohri et al., 2017) or power transformers in energy systems (Ahn et al., 2021). While providing valuable insights into real-world vulnerabilities, these studies were limited in scope and lacked the generalizability necessary to inform security frameworks across diverse embedded contexts.

The third cluster, representing about 25% of studies, addressed attack modelling approaches. Examples include the use of kill-chain analysis for industrial controllers (Neubert & Vielhauer, 2020) and the investigation of the TRISIS malware attack on safety controllers (Mekdad et al., 2021). Although these works provided detailed insights into adversarial tactics, techniques, and procedures, they remained largely reactive and failed to integrate proactive, adaptive security strategies.

In summary, the thematic distribution demonstrates that pre-2022 research disproportionately relied on IT-based frameworks, dedicated less effort to generalized embedded-specific models, and rarely adopted adaptive or proactive approaches. This imbalance highlights the necessity for future research to focus on embedded-aware, adaptive, and scalable security frameworks that better align with the operational realities of embedded devices.

CONCLUSION

Embedded systems are the foundational components of modern cyber-physical infrastructures, powering critical domains such as healthcare, transportation, energy, and industrial automation. Their increasing integration into mission-critical applications has amplified the urgency of addressing their cybersecurity vulnerabilities. This paper systematically reviewed research on embedded system security conducted prior to 2022, identifying three dominant thematic clusters: IT-derived threat modelling approaches, case-specific embedded investigations, and attack modelling frameworks. While these studies established a valuable foundation, they also revealed persistent shortcomings.

The findings highlight three critical research gaps. First, many approaches were derived from traditional IT models such as STRIDE or misuse patterns, which are ill-suited to capture embedded-specific vulnerabilities related to hardware–software co-design, resource constraints, and real-time operational needs. Second, adversarial behaviours were often modelled simplistically, ignoring the multi-layer, multi-agent, and persistent nature of attacks that embedded devices increasingly face. Third, most frameworks were static and developed only at design-time, failing to incorporate adaptive mechanisms that can respond to evolving threats throughout the long lifecycle of embedded systems.

These limitations underscore the necessity for future research that prioritizes embedded-aware and consequence-driven security frameworks. Potential directions include:

Adaptive Threat Modelling: Developing dynamic models that integrate real-time threat intelligence, anomaly detection, and continuous updates across the operational lifecycle of embedded devices.

Multi-Agent and Multi-Path Attack Simulation: Designing security models that account for complex adversarial behaviours, including coordinated attacks and cascading failures.

Lightweight Embedded-Specific Defences: Creating security mechanisms tailored to resource-constrained environments, balancing efficiency with robust protection.

Integration of Cyber-Physical Consequences: Extending beyond IT-centric confidentiality and integrity goals to explicitly account for physical safety and resilience in embedded contexts.

Standardized Frameworks Across Domains: Moving from domain-specific studies (e.g., medical, energy, ICS) toward generalized frameworks that can adapt across diverse embedded system applications

In conclusion, while pre-2022 research has laid important groundwork, it remains insufficient for the emerging security demands of embedded systems. Addressing these gaps requires a paradigm shift toward adaptive, embedded-aware, and scalable security frameworks capable of protecting critical infrastructures against evolving cyber threats. By bridging the divide between traditional IT security models and the unique realities of embedded systems, future research can enable safer, more resilient, and trustworthy embedded technologies that underpin modern society.

REFERENCES

- N. Martins, M. Vieira, and H. Madeira, "Towards a systematic threat modelling approach for cyber-physical systems," *2015 Resilience Week (RWS)*, pp. 132–138, IEEE, 2015.
- E. B. Fernandez, "Threat modeling for cyber-physical systems," *2016 IEEE 14th Intl. Conf. on Dependable, Autonomic and Secure Computing*, pp. 556–563, 2016.
- R. Khan, K. McLaughlin, and S. Sezer, "STRIDE-based threat modelling for cyber-physical systems," *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, 2017.
- S. Almohri, D. Yao, and D. Evans, "On threat modelling and mitigation of medical cyber-physical systems," *Proceedings of the IEEE/ACM CHASE*, pp. 66–73, 2017.
- L. Xiong and R. Lagerström, "Threat modelling from a cyber-physical system perspective," *Future Internet*, vol. 11, no. 3, p. 72, 2019.
- C. Neubert and C. Vielhauer, "Application of cyber kill chain and attack trees for ICS security threat modelling," *2020 IEEE Intl. Conf. on Industrial Cyber Physical Systems (ICPS)*, pp. 265–271, 2020.
- O. Mekdad, N. Kheir, and M. Debbabi, "An empirical study of TRISIS: A safety controller targeted malware," *Computers & Security*, vol. 103, p. 102150, 2021.
- S. Ahn, Y. Jang, J. Hong, and J. Kim, "Security threat modelling for power transformers in cyber-physical environments," *2021 IEEE ISGT Conference*, pp. 1–5,

2021.

- J. J. Bae and E. Bertino, "Securityissues in cyber-physical systems: A review," *Computers & Security*, vol. 85, pp. 137–152, 2019.

- M. Krotofil, J. Larsen, and D. Gollmann, "The process matters: Ensuring data veracity in cyber-physical systems," *Proceedings of ACM AsiaCCS*, pp. 133–144, 2017.

- M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

- D. Hadžiosmanović, D. Bolzoni, and P. Hartel, "A survey of intrusion detection systems in industrial control systems," *Computers & Security*, vol. 31, no. 8, pp. 845–868, 2012.

- A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

- C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Intl. Journal of Critical Infrastructure Protection*, vol. 8, pp. 53–66, 2015.

- R. Mitchell and I. Chen, "A survey of intrusion detection in wireless networked cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

- F. PièTre-Cambacédès and C. Chaudet, "The SEMA referential framework: Avoiding ambiguities in the interpretation of security models," *Intl. Journal of Critical Infrastructure Protection*, vol. 2, no. 2–3, pp. 66–79, 2009.

- J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *Critical Infrastructure Protection*, vol. 253, pp. 73–82, 2007.

- S. Adepu and A. Mathur, "Generalized attacker and attack models for cyber-physical systems," *17th Intl. Conf. on High Assurance Systems Engineering (HASE)*, pp. 322–329, 2016.

- J. Giraldo, E. Sarkar, A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7–17, 2017.

- P. Zhang, M. R. Asghar, and G. Russello, "Security and privacy in smart health: Efficient policy-driven access control for IoT devices," *Future Generation Computer Systems*, vol. 110, pp. 717–728, 2020.

- T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modelling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, vol. 7, no. 3, pp. 363–373, 2013.

- M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," *Workshop on Embedded Security in Cars*, pp. 7–14, 2004.

- J. Lee, B. Bagheri, and H. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.