Computers in Industry 137 (2022) 103611

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Threat modelling for industrial cyber physical systems in the era of smart manufacturing

Mohammad Jbair*, Bilal Ahmad, Carsten Maple, Robert Harrison

Warwick Manufacturing Group (WMG), University of Warwick, Coventry CV4 7AL, United Kingdom

ARTICLE INFO

Article history:
Received 12 July 2021
Received in revised form 24 December 2021
Accepted 17 January 2022
Available online 2 February 2022

Keywords:
Threat modelling
Industrial cyber physical systems
Digital twins
Smart manufacturing
Automatic code generation

ABSTRACT

Cyber security risks are considered to be one of the foremost challenges that face organisations intending to leverage the benefits of the Smart Manufacturing paradigm. Due to the rising number of cyber-attacks that target critical Industrial Cyber-Physical Systems (ICPS), organisations are required to consider such attacks as severe business risks. Therefore, identifying potential cyber threats and analysing their impacts is crucial to business continuity planning. This paper proposes a structured threat modelling approach for ICPS that enables prediction and analysis of cyber risks to protect industrial assets from potential cyber-attacks. The method involves classifying ICPS assets based on criticality, and then analysing the cyber security vulnerabilities, threats, risks, impacts, and countermeasures. The proposed methodology enables end-to-end threat modelling through the development of a new framework that is integrated with VueOne digital twin tool to model and analyse threats throughout ICPS lifecycle, identifying cyber risks and proposing mitigation controls. Moreover, it uses meta-data extracted from VueOne tool to automatically generate the software code and hardware configurations that can be directly deployed on ICPS assets in order to implement the countermeasures, thereby protecting them from these potential cyber-attacks. The proposed solution has been implemented on a Festo test rig prototype production line.

1. Introduction

The manufacturing industry is steadily shifting to the new paradigm of Smart Manufacturing. The core concept of this paradigm is to utilise ICPS to form and orchestrate smart factories and benefit from the new emerging advancements in Information and Communication Technologies (ICT), Internet of Things (IoT), digital twins (DT) and smart services. However, adoption of these technologies significantly increases threat landscape for ICPS, creating new attack vectors, along with the inherited risks from legacy systems. A recent survey conducted by SANS in 2019 (Filkins and Wylie, 2019) found that there is an increasing trend of reported cyber-attacks targeting industrial systems.

Cyber-attacks can be launched from various sources throughout the industrial network. However, there are a number of common attacks that should be considered for ICPS (Maggi and Pogliani, 2017). These attacks include: (a) Denial of Service (DoS) attacks, which aim to deny availabilities of assets; (b) Man-in-the-Middle attacks, in which an adversary sits between communicating industrial systems to send malicious traffic; (c) Replay attacks, in which an adversary replays false information from legitimate traffic; (d) Ransomware attacks that aim to widespread a malicious code; and (e) Zero day attacks that exploit previously unknown vulnerabilities. The consequences of these attacks can compromise the safety, productivity, profit and reputation of targeted organisations. Therefore, there is an urgent need to address cyber security by identifying cyber threats and potential cyber-attacks using threat modelling at the early design phase of ICPS lifecycle.

Although threat modelling is a key enabler for analysing cyber security risks, it still needs to evolve in order to integrate with methods and tools for engineering ICPS, such as tools for developing and deploying digital twins. These methods and tools provide powerful capabilities and functions to build and simulate ICPS assets in the form of models that can be used for process and product design. However, to large extent, these tools are limited to simulation. There is a need to extend the use of digital models to include a cyber security element. Thus, the novelty of this paper is to propose a structured end-to-end threat modelling technique that evolves modelling and simulation of ICPS to include cyber security. By doing this, threats and cyber-attacks can be modelled at the early design phase of ICPS creation, which in turn will enable identifying the risks levels and the severities, and countermeasures to mitigate these

* Corresponding author.
E-mail address: Mohammad.jbair@warwick.ac.uk (M. Jbair).

https://doi.org/10.1016/j.compind.2022.103611
0166-3615/

risks. In addition, this paper proposes a complete implementation for the mitigation countermeasures in the form of management controls such as security policies and / or technical controls such as software code and hardware configurations that can be applied directly to the ICPS assets to protect them from possible cyber threats.

2. Literature review

We have undertaken a literature review to consider the role of cyber security and threat modelling in the context of Smart Manufacturing and digital twin methods. The focus of the review is on cyber security standards, the state of the art methodological solutions that address modelling of threats in ICPS, and digital twins' methods and tools.

2.1. Threat modelling in ICPS

Threat modelling aims to analyse cyber challenges that organisations face by addressing cyber threats, which affect systems under consideration. The general process involves the analysis of attack vectors, gaining a comprehensive understanding of the underlying architecture, and providing a way to protect from these threats via security controls. Hence, threat modelling can illustrate who will target what and how in order to achieve why (Magar, 2016). To conduct threat modelling for ICPS, it is important to determine the overall approach by demonstrating its characterisation, taxonomies, methodologies and models, then identify threat security control countermeasures.

Threat characterisation determines adversaries' profiles and their behaviour including adversary types, capabilities and motivation to perform an attack. Adversary types can be Insider or Outsider (Lezzi et al., 2018). Insiders are those that have a level of authorised access to ICPS and perform unauthorised actions, with motivations including financial, revenge, or ego. Outsiders may be highly skilled adversaries such as terrorists, nation states, organised criminals and threat actor groups who aim to attack ICPS for reasons including financial or political objectives.

Threat taxonomies are the intelligence collected regarding an adversary's Tactics, Techniques and Behaviour (TTPs). There are several threat taxonomies available for ICPS including the Common Attack Pattern Enumeration and Classification (CAPEC™) by MITRE (MITRE, 2020), which provides a comprehensive classification taxonomy of attack patterns and guidance on how to mitigate adversary's effects to enhance cyber defence. The AVOIDIT Cyber Attack Taxonomy (Simmons et al., 2009), provides information on how to classify all vulnerabilities that can be exploited to perform a cyber-attack. The Reference Incident Classification Taxonomy by ENISA (Status and Forward, 2018), focuses on incident response by enabling incident handlers to deal with their daily cyber incidents in automated and systematic way.

Threat methodologies aim to identify processes to describe principles, tools and practices that guide the analysis of a threat or to understand adversary's behaviour. In context of ICPS, there are many threat methodologies available. The Cyber Kill Chain developed by Lockheed Martin (Hutchins, 2008) defines the steps that an attacker can use to initiate cyber-attacks, namely reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objectives. The ICS Cyber Kill Chain (Chain, 2020) is a customisation of the Cyber Kill Chain methodology to include industrial control systems (ICS) by utilising two stages to analyse cyber-attacks: cyber intrusion preparation and execution, and ICS attack development and execution. The Attack Tree (Saini et al., 2008) is a methodology to represent a series of attacks on a target system by consideration of root nodes and leaf nodes, which are connected logically using AND and OR to model adversaries goals. STRIDE (Khan et al., 2017) is a method that defines six types of security threats and used to analyse vulnerabilities of ICPS: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege.

Threat Models are approaches or frameworks that are used to identify and analyse threats and their capabilities, and propose security control countermeasures. Threat models may be Attacker-Centric, focusing on the attackers' views, goals, motivations, and behaviours. System-Centric models focus on the systems or software being targeted in cyber-attacks. Asset-Centric models consider devices or assets of target systems, which need to be secured, and build cyber-attacks on these assets (Magar, 2016). Several threat models specifically cover ICPS, such as the Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) model by MITRE (MITRE, 2020). This focuses on the adversaries' behaviour by studying several phases of attack lifecycle, then determining and analysing the tactics and techniques used before proposing detection and mitigation mechanisms to prevent harm. MITRE has also released the ICS ATT&CK® model, which is a customised version of ATT&CK® to address OT and ICS. The scope of this model is systems and applications associated with industry including Programmable Logic Controllers (PLC), Safety Instrumented Systems (SIS), Human Machine Interface (HMI), and Industrial IoT devices. Microsoft Threat Modelling (Magar, 2016) is a model that assists in creating cyber threats and determining the effectiveness of security countermeasures, and defines the following five steps: identify security objectives; application survey; decompose the application; identify threats; and identify vulnerabilities.

The methodology presented in this paper considers both threat characterisation types, insider and outsider. It utilises the CAPEC™ threat taxonomy, since it focuses on adversary's TTPs intelligence. The STRIDE methodology is employed since this method is comprehensive and considers the widely accepted confidentiality, integrity, and availability triad. The method encompasses the ICS ATT&CK® model since it specifically addresses ICS, the target domain for this work.

2.2. Cyber security standards in smart manufacturing

Cyber security standards are useful in guiding organisations as they undertake digital transformation providing a baseline for understanding cyber security in ICPS. Over the last decade, several bodies have developed and enhanced standards and best practices that tackle cyber security in the context of Operational Technology (OT), which focuses on industrial applications and control systems. Some of the most relevant are described in this paper.

The ISA/IEC 62443 (ISA, 2021) series of standards addresses security in Industrial Automation Control Systems (IACS). The main objectives of these standards are to address security requirements for OT through the use of four Security-Levels and assessing its security posture through four Maturity-Levels that can help organisations establish OT security programme, identify systems vulnerabilities and reduce cyber risks that targets industrial assets. The NIST 800–82 (Stouffer et al., 2015) standard addresses security in industrial applications by developing an ICS security programme and risk management framework. In addition, it provides guidance and recommendations for designing secure networks and monitoring for OT environments. The ANSSI best practice for ICS security (ANSSI, 2021) provides technical and organisational security controls that define security postures for OT and safeguard their core business functions continuity. The CIS Controls™ guidance for ICS (CIS, 2021) provides comprehensive directions on how to apply defense-in-depth practices to ICS environments by defining a set of security controls, which are categorised to three levels: basic, foundational and organisational. The VDI/VDE 2182 Blatt 1 standard (VDI, 2019), addresses IT security for automated machines and plants to define a procedure for ensuring security of automation systems throughout

Table 1
Methodological solutions for threat modelling in CPS.

Methodological Solution	Threat Modelling method	System addressed	Approach	Year of Publication
Cyber Security Threat Modeling for Supply Chain Organizational Environments	Mixture between Graphical and formal modelling with manual process to model the threats	CPS Supply chain cyber-attacks modelling	The methodology used qualitative approach with STIX design	2019
Developing Abuse Cases Based on Threat Modeling and Attack Patterns	Graphical modelling with manual process to model the threats	Security abuse cases for Health Information System	The methodology focused on STRIDE and CAPEC™	2015
Threat Modeling in Cyber-Physical Systems	Graphical modelling with manual process to model the threats	Security architecture for general CPS		2016
Structured system threat modeling and mitigation analysis for industrial automation systems	Graphical modelling with manual process to model the threats	Energy Networks and control systems	The methodology used quantitative approach	2015
STRIDE-based Threat Modeling for Cyber-Physical Systems	Graphical modelling with manual process to model the threats	Consider system and elements security modelling for CPS	STRIDE method	2017

the entire life cycle covering development, integration, operation, migration, and decommissioning phases.

2.3. Digital twins

Digital twin methods and tools aim to create a representation of ICPS assets in digital form (also referred to as cyber models) to reflect its physical environment. The cyber model involves computations for data analysis and on-board simulations, which allow the analysis of real time data and performance of various simulations for mechanical, electrical, and controlling parts of the ICPS. The role of digital twin in Smart Manufacturing is to forecast and optimise behaviours of ICPS and production systems throughout the entire life cycle (Cimino et al., 2019).

A wide range of digital twin tools are available in the market for designing and creating digital twins for ICPS. These include the NX Mechatronics Concept Design by Siemens (Siemens, 2021), 3DEXPERIENCE by Dassault Systems (Systems, 2021), Visual Components (Components, 2021), WinMOD by Mewes & Partner GmbH (GmbH, 2021) and VueOne by University of Warwick (Harrison et al., 2016). These tools allow the modelling and simulation of ICPS in a 3D environment and enable synchronisation between cyber and physical worlds. As a result, a closed loop system is implemented, and therefore improvements and optimisations for ICPS process can be fulfilled throughout its life cycle.

2.4. Methodological solutions for threat modelling in CPS

A study of the literature has revealed a number of methodological solutions that can be used to conduct threat modelling for CPS in different applications. Table 1 shows an overview of the frameworks, approaches and methodologies that are collected and listed.

This includes a methodology for threat modelling of supply chains in CPS systems (Yeboah-ofori and Islam, 2019). This methodology involves determination of an organisation's objectives, supply chain goals and security requirements. The attack process is then conducted, which aims to identify attacker motivations and TTPs. The next step is to determine probabilities of the attacks and model the threats using the STIX tool (Yeboah-ofori and Islam, 2019), which focuses on observable, indicators, campaign, threat actor, and TTP of each modelled threat. The last step is to provide security control measures to mitigate the attacks identified. These controls consist of directive controls, preventive controls, detective controls, corrective controls and recovery controls. This methodology cannot determine the severity of risks, the risk priorities and does not provide a roadmap for mitigating the cyber-attacks modelled.

The authors in (Yuan et al., 2015) suggest to develop abuse cases for software systems within CPS based on Microsoft threat modelling and CAPEC™ attack patterns. The proposed methodology starts with developing use cases for target systems that describe assets, data flows, and operator behaviour. A Data Flow Diagram (DFD) is created, and modelling of threats - based on the STRIDE method - is conducted. The final step identifies abuse cases based on each element of the DFD and its associated threats. This methodology does not realise risk determinations and countermeasures for the identified abuse cases and modelled threats.

In (Fernandez, 2016) the authors aim to model cyber threats for CPS by using a misuse pattern that describes how attacks could happen on CPS at the architectural level. The methodology defines CPS stakeholders and physical process use cases, such as loading a ship with containers. The process then involves the determination of safety assertions and security constraints for each process. Finally, threats are modelled for each process use case, where good knowledge of CPS physical process will result precise threat enumerations. This methodology cannot determine the risks and mitigations for the threats modelled, and also requires significant experience and knowledge of target CPS systems.

In (Schlegel et al., 2015) the authors propose a methodology that utilises a data model of industrial components from the targeted systems. The components are associated with specific threats, each threat has likelihood factor and impact to describe the severity of the threat in case it is exploited. Finally, mitigations are proposed for the threats modelled. It includes analysis algorithm to find unmitigated threats and proposes a security control measure for them.

The authors in article (Khan et al., 2017) conduct threat modelling for CPS based on STRIDE method. The proposed methodology starts by defining system logical and structural components. Then creates DFD for each identified component to represent component's functionality, where these functionalities include external entity, process, data flow or data store. Third step identifies STRIDE threats for each component. The final step proposes countermeasures for all vulnerabilities discovered. This methodology cannot calculate risk levels and its severities, nor proposing security controls for cyber risks.

To conclude, most of the existing threat modelling approaches provide incomplete solutions for ICPS as they focused on providing a visibility for adversary's TTPs without providing risks severities that are associated with those malicious behaviours. In addition, these methodologies are ad-hoc solutions, which do not integrate with ICPS methods and tools and therefore cannot address threats and risks during ICPS creation. Thus, they have not been put into industrial practices.

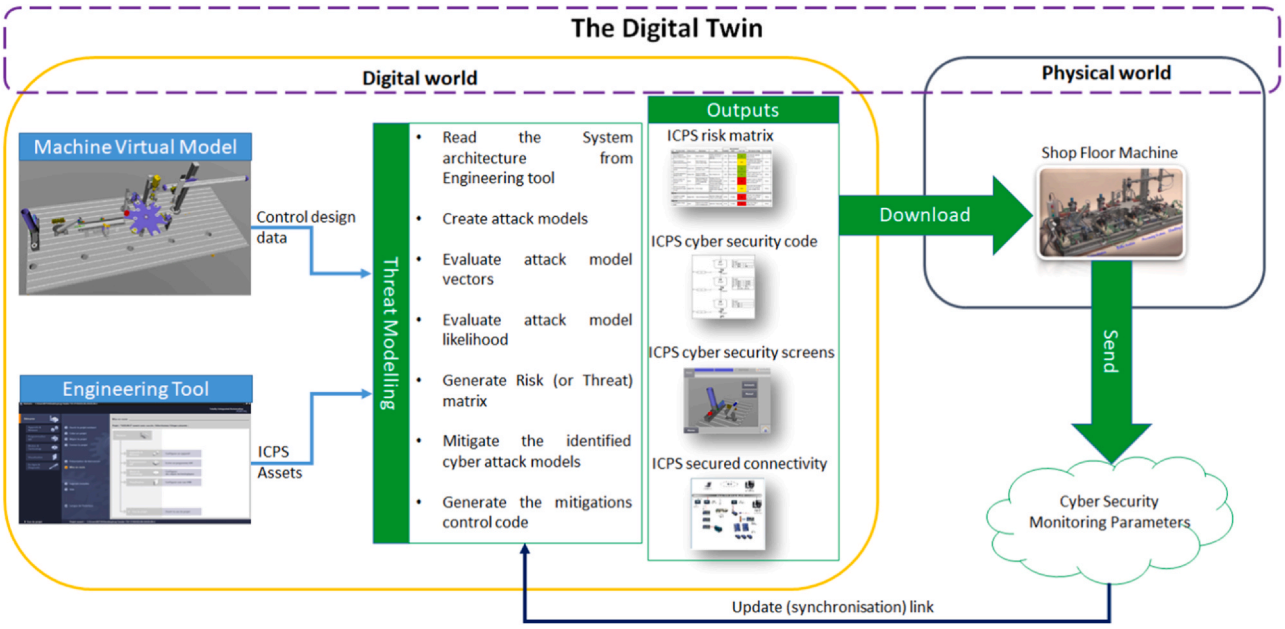

Fig. 1. The Methodology.

3. Methodology

3.1. Objectives

Many methodological solutions have been identified in the literature review section. However, they do not adequately address threat modelling for CPS that is in line with digital twins' methods and Smart Manufacturing framework. This paper aims to create a methodology to model cyber threats for ICPS, so that manufacturing organisations can address potential threats and cyber-attacks to protect their assets at the early stage of ICPS developments lifecycle. It also identifies risks ratings, risks severities, and mitigation countermeasures to enable development of strategic roadmap for business investments in cyber security field. With the aim to provide a detailed analysis for risks and threats landscape that could impact ICPS resulting from cyber security breaches, the following research questions are addressed: What are the potential cyber-attacks that affect security of ICPS assets? How to classify ICPS assets to determine the severity of cyber-attacks on each asset? How to analyse and determine risk levels for ICPS in Smart Manufacturing? How to achieve end-to-end threat modelling framework that utilises design meta-data for ICPS and exploits the benefits of digital twin engineering methods and Smart Manufacturing frameworks?

3.2. Approach

This section outlines the methodology followed in the paper, which aims to create structured threat modelling approach to support organisations to better understand the threats landscape and protect their assets from potential cyber-attacks during early stage of ICPS lifecycle. As illustrated in Fig. 1, ICPS is represented by a digital twin to articulate digital and physical worlds. The methodology focuses on the digital world, where design data are presented. It begins with listing ICPS assets that need to be protected, and model all potential cyber-attacks affecting them. Next stage evaluates attacks modelled by calculating two factors: attack vector and attack likelihood. Third stage generates the risk matrix including risk levels, severities, and risk treatments. The methodology utilises the digital twin and Smart Manufacturing methods and tools to achieve end-to-end threat modelling. Therefore, threat modelling data can be utilised along with the meta-data generated from virtual (cyber) model in order to automatically implement all identified mitigation controls in a form of security policy, software and hardware codes, which can be directly deployed to physical ICPS shop floor machines.

3.2.1. Digital twin as a key enabler for end-to-end threat modelling

In the context of this paper, a digital twin may be defined as a representation of a system of manufacturing applications in both digital and physical worlds; the aim of the digital twin is to connect the two worlds in order to replicate manufacturing systems in real-time to provide smart services such as data analytics, process engineering and optimisation (Cimino et al., 2019). The digital world consists of the manufacturing applications' virtual models that accommodate the manufacturing parameters such as design, engineering, process, and operation & maintenance data. The physical world consists of the physical assets for the manufacturing application. Since the digital twin engineering methods and tools are addressing the entire ICPS lifecycle, they can offer huge value to the proposed end-to-end threat modelling methodology since the threat modelling exercise can be fully integrated within the ICPS lifecycle and be part of its creation process. Therefore, the digital twin methods and tools act as key enablers for threat modelling in smart manufacturing framework.

3.2.2. Data model

In order to conduct threat modelling for ICPS, and thus achieve our objectives, it is essential first to understand the relationship between ICPS assets and potential malicious behaviours that may expose a risk. For this reason, the authors have created the data model parameters illustrated in Fig. 2.

Threat Actor comprises of "Insider" who has a level of privileged access to target ICPS, or "Outsider" who does not have such access yet and aims to launch an attack on ICPS. For both threat actor types, it is required to have certain level of skills, resources and tools to enable them exploiting ICPS assets' vulnerabilities and conducting cyber-attacks.

Cyber-Attack is unauthorised act that aims to compromise assets and its services to perform harmful actions (Task and Transformation, 2012). In the ICPS context, cyber-attack is a malicious action on industrial systems that affects its safety, availability,

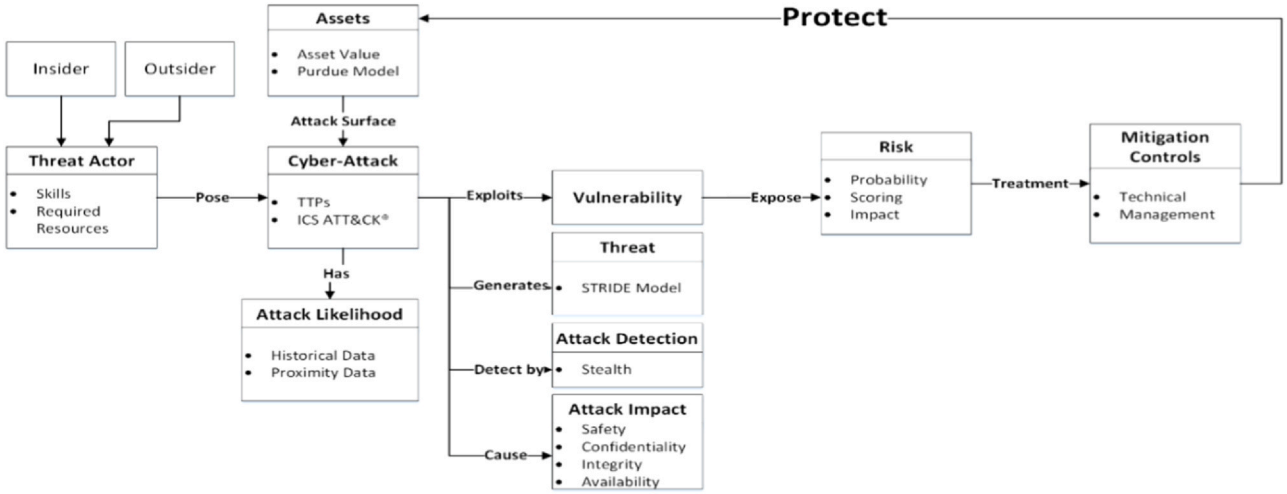

Fig. 2. The Data Model.

integrity and confidentiality. To model cyber-attacks, it is important to understand threat actors' TTPs. Tactics are adversaries' goals for what they want to achieve on the target ICPS. Techniques are individual actions to perform cyber-attacks. Procedures are ways of performing cyber-attack's techniques (Alexander et al., 2020). ICS ATT&CK® is used to understand adversaries' TTPs and model cyber-attacks. It provides a matrix illustrated in (MITRE, 2020) to visualise TTPs, where matrix header reflects tactics and each columns element represents adversary's technique to feed into that tactic goal.

Assets are ICPS components and services that threat actors aim to compromise. Purdue Model (Cimino et al., 2019) is used to characterise ICPS assets. Level-0 contains process assets such as sensors and actuators. level-1 reflects basic control assets such as PLC. Level-2 is the area supervisory control assets such as HMI and workstations. Level-3 contains site manufacturing operations and control asset such as historians and production systems. Level-4 and Level-5 have business and enterprise assets such as business IT assets, email and printing services. Impacts of malicious actions depend on asset levels, lower asset levels directly interact with industrial process and therefore it has higher impact. Hence, asset level is proportional to asset criticality.

Vulnerability is a weakness in ICPS assets and its services that can be exploited by threat actors to conduct malicious actions. Vulnerability scanning techniques in ICS ATT&CK® can discover and identify components vulnerabilities. However, several advisories about known vulnerabilities and security issues are published by entities and organisations such as national security centres, security agencies, or suppliers and vendors. For example, industrial vendor such as Siemens releases advisories in timely manner about vulnerabilities related to their software or hardware assets; MITRE corporation provides dictionary of publically known vulnerabilities known as Common Vulnerabilities and Exposures (CVE™) (MITRE, 2020); NCCIC has a specialised team called ICS-CERT who focuses on security incidents and vulnerabilities within critical infrastructure sectors (NCCIC, 2020).

Attack Impact is the impact on Availability, Safety, Integrity and Confidentiality categories for ICPS when a cyber-attack is conducted. Impact severity for each category depends on ICPS asset level. For example, assets within level-1 have more impact on availability and safety categories compared to integrity and confidentiality, while assets in level-4 and Level-5 have more impact on confidentiality category.

Attack Detection measures cyber-attack detectability and residual evidence left by a threat actor, which lead to understand its attributes. It is important to understand threat actors' TTPs in order to detect their actions. However, once the attack is executed, digital forensics exercise can be conducted to trace attackers' TTPs and understand attack attributes, ICS ATT&CK® lists several mechanisms and tools to detect cyber-attacks and conduct digital forensics.

Attack Likelihood reflects the probability of cyber-attacks modelled based on historical data of similar previous attacks and future expectations and trending for these attacks on ICPS. Maturity of the historical data depends on ICPS sector. For example, Energy sector has encountered many cyber incidents in the past e.g., Black Energy, Industroyer and Havex malware to indicate that likelihood parameter is high in this sector.

Threat is a harmful action facilitated by an exploited vulnerability that results to unwanted impact on ICPS assets. Threat actors aim to discover ICPS threats in order to understand its weaknesses and perform cyber-attacks. STRIDE model (Khan et al., 2017) is used in this methodology to represent security threats for ICPS assets.

Risk is a potential negative impact from malicious acts conducted by a threat actor. Risks vary depending on the damage associated with the target assets. Accordingly, measuring risk levels and its severities can be achieved using qualitative or quantitative methods. Risks are categorised to technical, operational and management. Technical risks linked to ICPS assets, operational risks linked to ICPS systems and management risks linked to organisation's policies and human factors.

Mitigation Controls are countermeasures, articulated and implemented to ensure all identified risks are treated to a risk tolerance or acceptable level. In this paper, two types of mitigate controls are proposed, technical and management. Technical controls are safeguard measures that involve technology element to achieve its objectives, such as implementing identify and access control solution. Management controls are safeguard measures that involve administrative element to achieve its objectives, such as password policy.

Fig. 2 describes methodology's data model parameters and their relationships. A *Threat Actor* with specific skills level and resources can conduct a *Cyber-Attack* by exploiting a *Vulnerability* and *Threat* using a number of TTPs methods to manipulate ICPS *Assets*, where *Attack Impact* depends on asset value. Each of conducted *Cyber-*

Attack can be detected using *Attack Detection* methods. The *Risk* probability exposed by a *Cyber-Attack* calculated using the *Attack Likelihood* and *Attack Impact*; the identified *Risks* then are treated by formulating and implementing a set of *Mitigation Controls* in order to protect the target ICPS *Assets*.

Each data model parameter is evaluated by different levels as explained in Table 2. Very High equivalents to score (5), High equivalents to score (4), Moderate equivalents to score (3), Low equivalents to score (2) and Very Low equivalents to score (1). Every level represents specific criteria. For example, *Threat Actor* skills parameter vary from very knowledgeable - score (5) to no skills knowledge - score (1).

3.2.3. Threat modelling process

The methodology proposes an end-to-end threat modelling, which realising a comprehensive framework that considers entire ICPS lifecycle. Thus, we propose threat modelling process as described below and shown in Fig. 3:

Step-1 "Asset Scoping" identifies ICPS target assets, this step is important because the ultimate objective is to protect these assets from cyber-attacks. Assets scoping can be carried out manually by extracting the target assets from ICPS system architecture and engineering drawings, or automatically by importing the assets from engineering tools. In both cases, assets are categorised based on Purdue Model to represent assets values.

Table 2
The methodology's data model parameters and its related criteria .

Data Model parameter	Criteria Description for each level				
	Very High – 5	High – 4	Moderate – 3	Low – 2	Very Low – 1
Threat Actor					
Skills: what level of skill or knowledge is required by the adversary to conduct the cyber-attack	High skills with knowledge about target ICPS	High skills without knowledge about target ICPS	Some knowledge about target ICPS	Generic technical skills	No skills and no knowledge about target ICPS
Required Resources: tools and software resources required to conduct the cyber-attack	Significant resources about target ICPS are available	Significant resources available but not related to target ICPS	Some resources available related to target ICPS	Minimal resources available, not related to target ICPS	No resources available and required to be developed
Assets					
Asset Value: reflects ICPS asset criticality based on Purdue Model levels	Level-1 assets	Level-2 assets	Level-3 assets	Level-3.5 assets	Level-4&5 assets
Vulnerability					
Vulnerability: How vulnerable is the target asset to be exploited	Published vulnerabilities and known vulnerabilities on ICPS with significant impact	Known vulnerabilities with high impact on ICPS	Customised tools required to identify ICPS vulnerabilities with high impact on ICPS	Customised tools required to identify ICPS vulnerabilities with low impact on ICPS	Customised tools required for vulnerability discovery on patched ICPS
Attack Impact					
Confidentiality: impact measure on loss of ICPS confidentiality from a successful cyber-attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Integrity: impact measure on loss of ICPS integrity from a successful attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Availability: impact measure on loss of ICPS availability from a successful cyber-attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Safety: impact measure on loss of ICPS safety from a successful attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Attack Likelihood					
Likelihood: How frequent a cyber-attack could happen for ICPS based on historical data and future expectations	Happened in past 3 years for target ICPS industry sector or expected to occur in the next 6 month	Happened in past 6 years for target ICPS industry sector or very likely to occur in next 1 year	Happened in the past 10 years for target ICPS sector or likely to occur in next 3 years	Happened in the past 10 years for target ICPS sector or likely to occur in next 6 years	Not happened in the past or likely to occur in next 10 years
Attack Detection					
Stealth: How detectable is the conducted cyber-attack	Not detectable	Detection possible with customised monitoring tools and high forensic skills	Detection possible with customised monitoring	Detection possible with some forensic skills	Detection without any monitoring tools

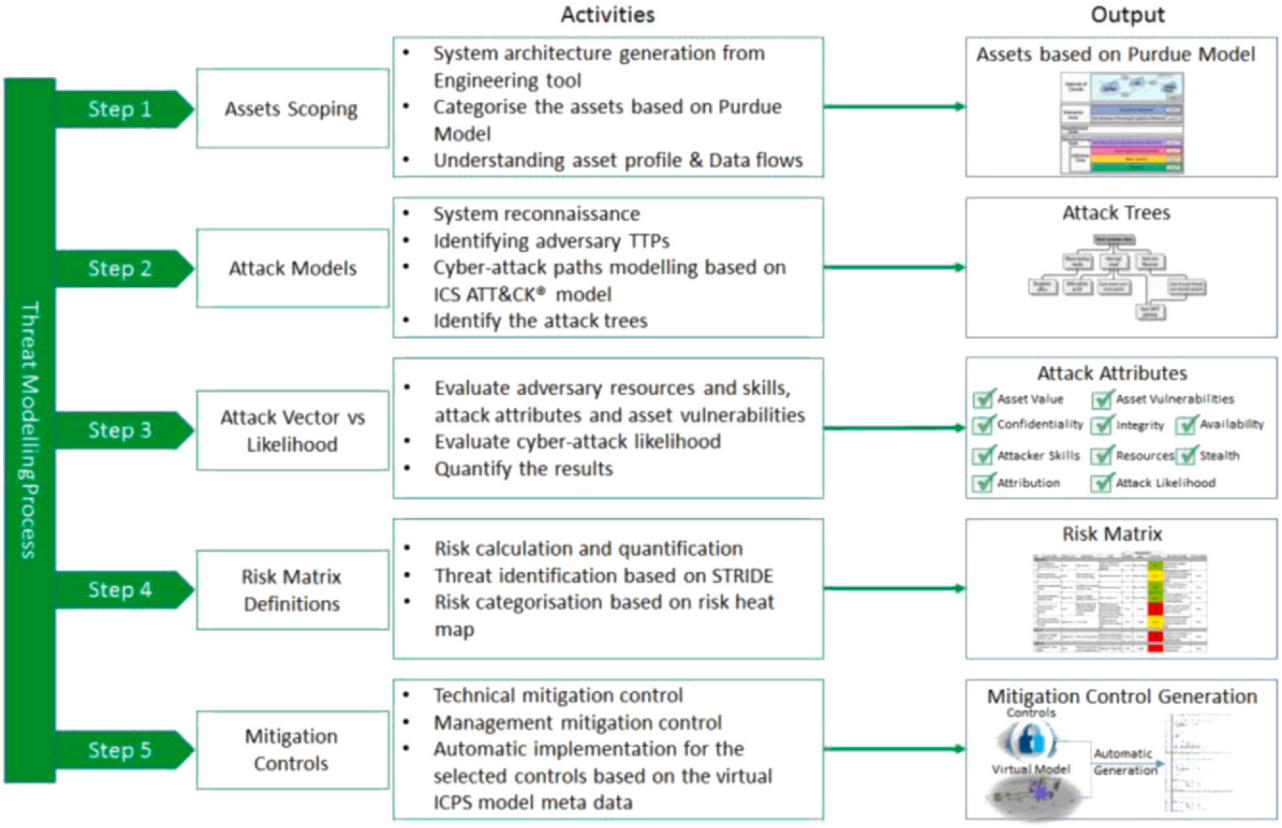

Fig. 3. Proposed Threat Modelling Steps.

Step-2 "Attack Models" aims to build possible attack scenarios for scoped assets by understanding threat actor's TTPs using ICS ATT&CK®. The outcome from this step is a set of attack trees that explain all possible attack scenarios for ICPS assets.

Step-3 "Attack Vector (AV) vs *Attack Likelihood (AL)"* measures the attack vector and attack likelihood for each modelled attack. AV is the window of exposure that a threat actor exploits to initiate a cyber-attack. Based on data model parameters, AV depends on threat actor skills and available resources, vulnerabilities associated with target assets, asset value, attack detection and impact. AL checks whether attacks modelled have been conducted previously on ICPS related industry sector or possibility to have these attacks in the future. The outcome of this step measures the attacks' attributes modelled.

Step-4 "Risk Matrix Definition" aims to produce a matrix that lists all risks for the attacks modelled. Risk matrix demonstrates scoped ICPS assets, attacks modelled, AV and AL values, security threats, risks levels and its severities, and mitigation controls.

Step-5 "Mitigation Controls" is the final step of the threat modelling, where each identified risk will be treated. Two mitigation control types are proposed, technical and management controls. A mitigation controls library is developed for this purpose to propose possible countermeasures that can be implemented to treat risks.

3.2.4. Risk analysis

Understanding associated risks and their severities for ICPS assets is crucial to protect them from cyber-attacks. Therefore, risk analysis is a critical step in threat modelling and evaluation of risk levels is vital for business decisions. Hence, both quantitative and qualitative methods are utilised to measure risks.

Quantitative method is a numeric estimation of risk probabilities using mathematical model techniques that precisely measure the cyber risks for ICPS assets. To quantify risks, we refer to established methods, where *Risk = Consequences X Likelihood*. Referring to methodology data model in Table 2, *Consequences* depend on Threat Actor, Assets, Vulnerability, Attack Impact and Attack Detection, while *Likelihood* depends on Attack Likelihood. For example, highly skilled Threat Actor could create more damage on ICPS compared to non-skilled one, similarly publicly published vulnerability has higher exposure of exploitation compared to unknown vulnerability. Therefore, risk can be defined as function of AV and AL as per the following formula:

$$Ri = AVi * ALi,\ i = 1,\cdots, n$$

where R – risk; AV – attack vector for each modelled attack; AL – attack likelihood; n – number of possible scenarios for cyber-attack.

Risk is proportionally depending on attack vector and likelihood. But, the question is, how to estimate AV and AL? To measure AV, threat actor capabilities need to be determined, understanding of threat exposure to ICPS asset and its vulnerabilities, and most importantly understanding impacts caused from modelled cyber-attacks. By putting these factors into considerations, attack vector is estimated by calculating the geometric mean as following:

$$AV = \sqrt[3]{TA \times TE \times TI}$$

Where TA – threat actor skills and resources; TE – threat exposure for exploitation; TI – threat impact and damage on ICPS assets.

Referring to methodology data model parameters, we can calculate each of attack vector elements as:

$$TA = \sqrt[2]{K \times R}$$

$$TE = \sqrt[3]{As \times Vl \times Ad}$$

$$TI = \sqrt[4]{Ax \times Ix \times C \times S}$$

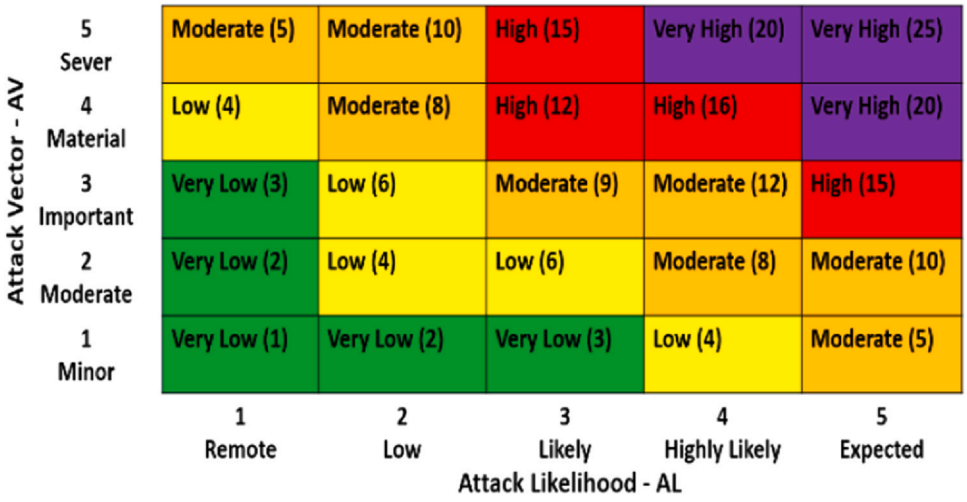

Fig. 4. Risk heat map matrix.

K – threat actor knowledge and skills; *R* – resources required by threat actor to conduct the target attack; *As* – asset value and its criticality; *Vl* – vulnerability rating associated with ICPS asset; *Ad* – attack detection techniques used on modelled attacks; *A* – availability impact; *I* – integrity impact; *C* – confidentiality impact; *S* – safety impact.

Measuring AL, on the other hand, requires determination of the historical data available on similar cyber-attacks for the ICPS sector and predictions or the proximity data for the likelihood on similar attacks. Therefore, Table 2 illustrates the criteria to estimate AL value, where this value varies from very likely attack with score (5) to unlikely with score (1).

Qualitative method is a way to determine risk severities and prioritisations based on a pre-defined probability rating matrix. To measure qualitative risk, we use AV and AL values. Accordingly, risk is estimated based on the risk matrix shown in Fig. 4, where risk severities are Very High, High, Moderate, Low, and Very Low.

3.3. Mitigation controls implementations via the digital twin

The methodology enables modelling of cyber-attacks and provides mitigation controls to identified risks. Moreover, it provides implementations of the mitigation controls by automatically generating all related policies, hardware configurations and software code for the ICSP assets. For example, "firmware version monitoring" control generates code to monitor assets' firmware such as PLC. Similarly, "password enforcement" control automatically creates a user-defined password with read/write access for the assets.

However, how automatic security controls generation can be realised? To generate management or technical controls, it is required to utilise the meta-data extracted from the virtual model within the digital twin, data extracted from the engineering tool, and templates extracted from the policies library.

Fig. 5 explains this process. Virtual model has the meta-data that describes control behaviour and sequence of operations for ICPS components. Engineering tool has software and hardware templates that represent ICPS components. Policies library has templates for security policies and procedures. For instance, a servomotor component has control behaviour description in the virtual model, software function template for control operations and hardware module in the engineering tool. Therefore, if technical control required to be generated for this component, then the Code Generator Engine will map selected mitigation control with the meta-data from the virtual model and the engineering tool. If management control is required, then template from the policies library will be used as basis to generate a policy that is tailored to meet specific asset requirements.

4. Case study

This section demonstrates the feasibility, features and applicability of the proposed threat modelling approach for ICPS through an industrial case study. A Festo Test Rig (FTR) is used, which

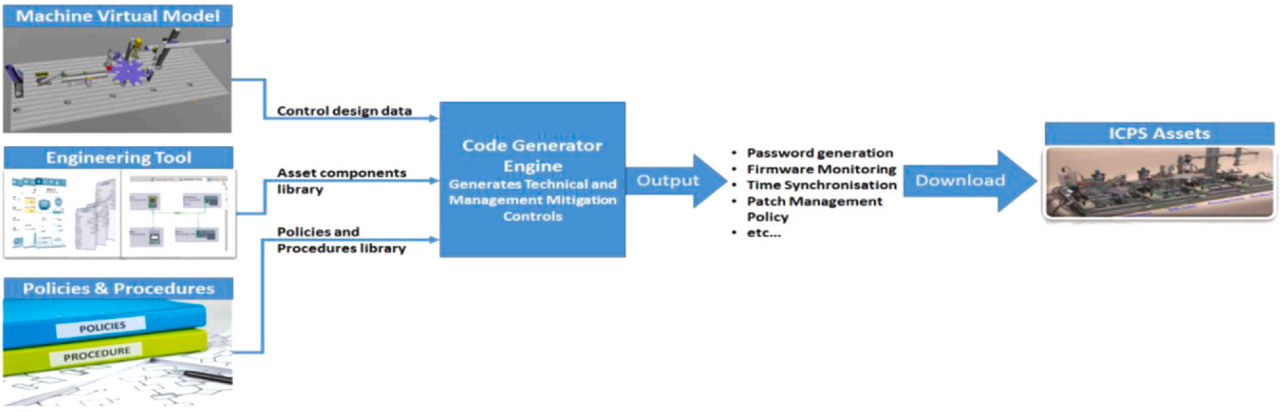

Fig. 5. Automatic code generation process for mitigation controls.

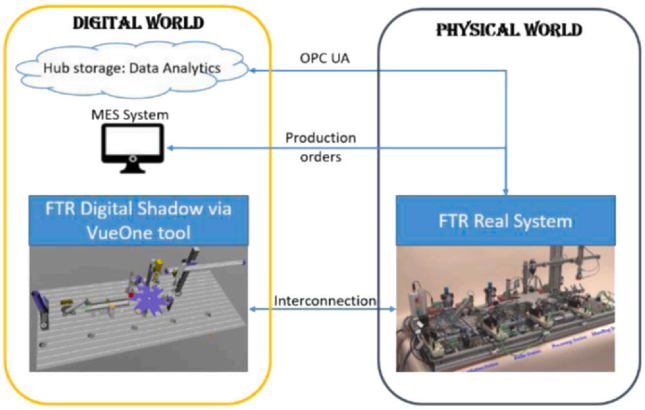

Fig. 6. FTR case study's digital twin.

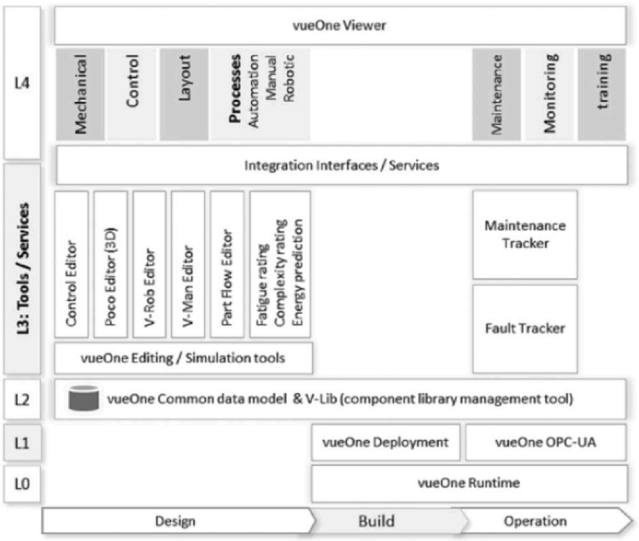

Fig. 7. VueOne engineering environment overview (Harrison et al., 2016).

emulates a small-scale model of a production line, shown in Fig. 6. This rig is used for initial development and acts as a proof- of-concept, demonstrating the validity of the proposed techniques. The FTR is representive of an ICPS on the manufacturing floor that accommodates the following: (1) ICPS systems consisting of multiple (in this case four) stations: (i) Distribution station, (ii) Buffer station, (iii) Processing station, and (iv) Handling station; (2) ICPS connectivity that connects the FTR control components with the higher level of automation via OPCUA (Open Platform Communications United Architecture) communication; and (3) ICPS digital twin, represented by the cyber-physical worlds, the cyber world containing the virtual model rig and the physical world containing the actual hardware components. The Rig produces prototype product (engine) by conveying a workpiece throughout the production line stations to conduct a number of operations such as gripping, transferring, indexing, clamping, drilling, and gauging. The FTR is equipped with a PLC, HMI, local Hub storage to collect data from physical systems via OPCUA communication, and MES (Manufacturing Exaction System) to manage production orders.

The digital twin for the case study has been created using VueOne toolset, which is developed by the Automation Systems Group (ASG) at the University of Warwick (Jbair et al., 2019; Harrison et al., 2016). The toolset is managed by ASG and designed and developed for research purposes. ICPS modelling in VueOne is achieved by considering two main phases: component modelling and system modelling. Component modelling encapsulates the data, which defines the ICPS component geometry using Virtual Reality Modelling Language (VRML) format for 3D model, kinematics, and control behaviour. VueOne supports several ICPS components such as sensors, actuators, human mannequin, robots, factures and more. The system modelling phase aims to create the relationship between the components of the ICPS by assembling them and outlining their sequence of operations thereby defining the interactions between them. VueOne uses a State-Transition-Diagram (STD), which is equivalent to a sequence of operations to describe the control behaviour. This STD is compliant with IEC 61131–3 for process definition. Fig. 7 demonstrates an overview of the VueOne toolset.

4.1. Results

Next subsections demonstrate threat modelling on the FTR case study, which include the FTR industrial sector attack groups analysis, asset scoping, attacks modelling, threats and risks analysis, risk matrix definition, and mitigation controls implementations.

4.1.1. FTR threat actors analysis

This case study represents ICPS in manufacturing sector, precisely in automotive vertical. It is essential to understand threat actors' motivations, skills and their resources before conducting the threat exercise. It is not possible to list all possible threat actors, as there are significant incentives for many individual groups, organisations and states to compromise ICPS. However, we do elaborate some of the major threat actors that are most relevant to the case study's industrial sector and their campaigns and TTPs. We consider the skills level and resource of the three key actors below.

APT32 threat actor group have been active since 2014. The group was focused on Southeast Asian countries, Australia and Germany. The group motivation is information theft and espionage. Their TTPs start with social engineering methods as they used undocumented Microsoft file format with encode Office macros. Upon execution of the macros script, the file downloads several malicious payloads from a remote server to compromise the victim's machine. Consequently, threat actor can conduct techniques such as Network Service Scanning, Network Connection Enumeration, and Valid Account to execute the target cyber-attack. Focused industries for this group are Defense, manufacturing, telecommunications, and high technology. Several software resources are utilised to conduct their cyber-attacks, such as Cobalt Strike, Denis, Goopy, Mimikatz, and OSX_OCEANLOTUS.D (MITRE, 2020).

Mofang threat actor group have been observed since 2012. The group target several countries such as Canada, Germany, India, Myanmar, Singapore, South Korea and USA. Their motivation is information theft and espionage. Their TTPs mainly use phishing email with spearphishing malicious link, upon clicking on this link, user will be prompted to download applications, documents, zip files, or executables, which enable the threat actor to compromise the victim's machine. Once compromised, several techniques can be then employed to launch the cyber-attack such as Network Service Scanning, Brute Force I/O, and Denial of Service. Focused industries for this group are automotive, critical infrastructure, defense, Government and weapon industries. Software resources used to conduct their attacks are ShimRAT, ShimRatReporter and Superman (MITRE, 2020).

Reaper also called APT37 or Ricochet Chollima threat actor group have been active since 2012. The group targeted China, India, Japan, Kuwait, Nepal, Russia, South Korea, and the UK. Their motivation is information theft and espionage. Their TTPs begins by using social engineering methods via spearphishing emails tailored to desired targets, which ask the victim to navigate to a website in order to steal their credentials and compromise the machine. Once the machine is compromised, the threat actor can pivot from it to conduct

further techniques such as Network Service Scanning, System Shutdown/Reboot, and Modify Control Logic. Software resources used to conduct attacks are CORALDECK, Final1stSpy, Freenki Loader, KevDroid, N1stAgent, and Rokrat (MITRE, 2020).

In conclusion, studying several threat actor groups, their tactics and campaigns, helped to understand threat actors' skills level and required resources to conduct the target cyber-attacks. In addition, it provides insights about the possible techniques used to compromise the victims' machine. APT32, Mofang, and APT37 proofed that previous cyber-attacks have been recorded in the case study's industrial sector (manufacturing) and listed possible techniques such as Network Service Scanning and Modify Control Logic that can be potentially used on the case study's assets such as PLC or HMI. They also demonstrated threat actor's skills level and software resources used to conduct the attack, which will be considered as inputs during the case study's threat modelling exercise and risk analysis. Table 3 in Section 4.1.4 shows the skills level and resources required for the case study's modelled attacks.

4.1.2. Assets criticality analysis

FTR consists of several assets that have different criticalities. Level-1 assets include Siemens S7–1500PLC used to control the physical process. Level-2 contains HMI that used to monitor and supervise the physical process. Level-3 contains two assets: MES server used to define production orders and OPCUA server used to collect data from the physical process. Finally, level-5 contains OPCUA Client, which used to collect process data and send it to the local Hub storage. For the threat modelling exercise, scoped assets are S7–1500PLC, HMI and OPCUA server.

4.1.3. Attack trees

To model the attack trees, it is essential first to understand threat actors' TTPs, which can be derived from ICS ATT&CK®. Fig. 8 illustrates the attack trees modelled for scoped assets. Starting with S7–1500PLC, a threat actor can launch PLC firmware attack, PLC code changes, and denial of service attacks. By mapping TTPs from ICS ATT &CK® to PLC firmware attack, an adversary needs to scan ICPS network (technique T841) and enumerates its connections (technique T840) in order to identify associated vulnerabilities and commonly used ports (technique T885) and then exploit certain vulnerability to gain a valid account (technique T859). Once valid account is gained, adversary can perform lateral movement within the network to exploit vulnerabilities associated with PLC system firmware (technique T857) and launch the attack. Similarly, an adversary can list vulnerabilities of ICPS assets using techniques (technique T840, technique T841, technique T869 and technique T861) in order to spoof MAC addresses and intercept network traffic to act as man-in-the-middle (MitM) between PLC and other assets such as HMI. Once this stage is achieved, the adversary can modify PLC control logics (technique T833). Lastly, an adversary can initiate a denial of service attack (technique T814) by enumerating network connections (technique T840) and identifying the IO modules (technique T824), then conduct brute force (technique T806) to target used ports (technique T885) for the PLC.

Regarding HMI asset, an adversary can enumerate network connections (technique T840) in order to identify associated ICPS assets' vulnerabilities and intercept network traffic to act as MitM (technique T859). Then, the adversary can determine HMI points and tags (technique T861) and change program state (technique T875) or send unauthorised command messages (technique T855) to other assets. On the other hand, an adversary can launch a denial of service attack using similar techniques used for PLC.

Third asset is OPCUA server. An adversary can enumerate network connections (technique T840) to identify and exploit related vulnerabilities in order to intercept network traffic and act as MitM (technique T859). Then, the adversary can determine OPC tags (technique T861) and change program state (technique T875) or send unauthorised command messages (technique T855) to other assets. In addition, acting as MitM allows conducting wider attacks, such as replay attack, program changes and set point value tampering.

4.1.4. FTR risk analysis

Two methods to analyse risks are proposed, quantitative and qualitative. The execution for each method on FTR is explained as following:

Quantitative method determines risks by a numerical value to precisely measure their probabilities. The attack trees modelled in Fig. 8 are used as inputs to calculate AV and AL based on the formulas illustrated in Section 3.2.4. However, we need first to measure the data model parameters, which are Asset Values, Threat Actor, Vulnerability, Attack Impact and Attack Detection. Table 3 shows the calculated results for the scoped assets.

Table 3
Quantitative risks results for FTR case study .

Asset Name	Modelled Attack	Threat	Data Model Elements									Attack Vector	Attack Likelihood	Risk Rating	Risk Severity	Mitigation Control
			Asset Value	Required Skills	Resources	Vulnerability	Confidentiality	Integrity	Availability	Safety	Stealth					
S7-1500 PLC	PLC Firmware Attack	Repudiation	5	3	1	3	1	1	5	2	3	3	3	9		TC – Firmware version monitoring
	PLC Code Changes	Tampering	5	4	4	4	2	4	5	4	3	4	4	16		TC – PLC online code changes monitoring
HMI	Denial of Service Attack	Denial of Service	5	2	1	1	1	1	5	2	2	2	2	4		MC – Password policy enforcement
	Set point value tampering	Tampering	4	4	4	4	3	4	3	4	3	4	4	16		TC – HMI online value changes
	Denial of Service Attack	Denial of Service	4	2	1	1	1	1	5	2	2	2	3	6		MC – Password policy enforcement
OPCUA server	Set point value tampering	Tampering	3	3	3	4	3	4	3	4	3	4	4	16		TC – OPC online value changes

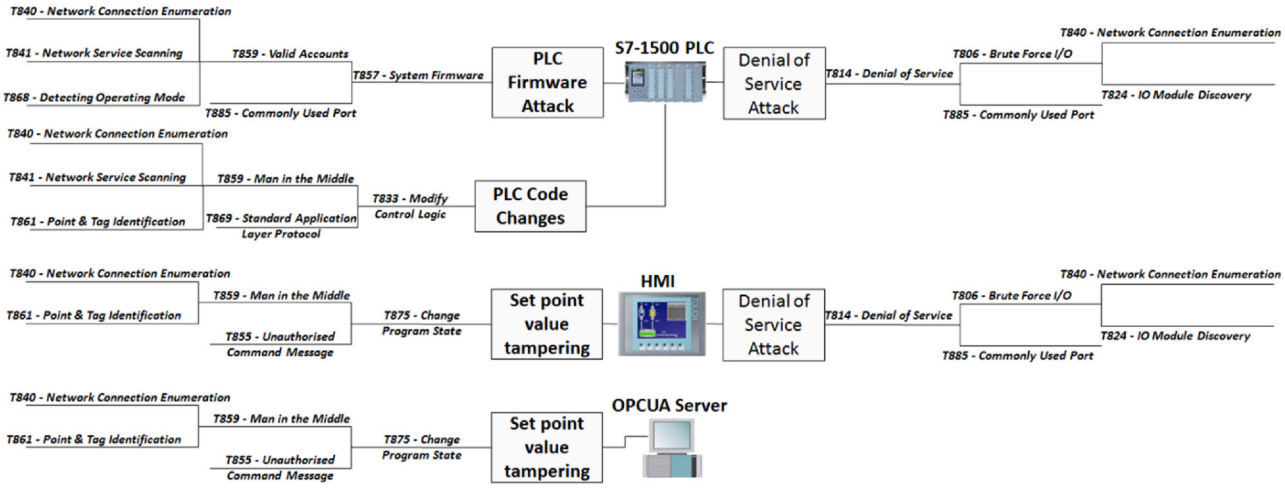

Fig. 8. FTR case study attack trees.

Asset value reflects the criticality of FTR assets and the damage or impact that could happen to those systems in case of a cyber-attack. Therefore, S7–1500PLC is the most critical asset and OPCUA server is the least one. *Threat actor* skills and resources parameters can be estimated by studying threat actor groups tracked for FTR industrial sector. For example, in 2019, both BMW's and Hyundai's assets were hacked by APT32 hackers. The attackers installed a penetration testing toolkit called *Cobalt Strike* on infected hosts, which they used as a backdoor into the compromised network in order to conduct further techniques (ZDNet, 2021). In 2020, APT37 group have used spear phishing attack that targets a government agency in South Korea. The attacker sent email that weaponised with a malicious document uses Hwp files (Hangul Office) with a self-decode macro, which allowed to download a cloud-based Remote Access Trojan (RAT) known as *RokRat* to gain persistent access and conducted further techniques on the network (Malwarebytes, 2021). By looking at the threat actor groups' TTPs and campaigns, it is obvious that threat actors are exposed to a wide range of skills and software tools (resources) allowing them to conduct several methods and techniques. On the other side, *Vulnerabilities* associated with the scoped assets are determined during the reconnaissance phase. However, several publicly know vulnerabilities are published for the FTR scoped assets. For example, CVE-2014–2251, CVE-2014–2249, CVE-2014–2248 and CVE-2014–2246 are vulnerabilities associated with S7–1500PLC Firmware (MITRE, 2020). CVE-2018–12086 and CVE-2020–8867 are vulnerabilities associated with OPCUA server (Foundation, 2020).

Attack impact includes confidentiality, integrity, availability, and safety. Loss of confidentiality for FTR could cause reduction in product (the engine) competitiveness due to loss of know-how, company reputation, and customer trust. Loss of integrity would affect product manufacturing in terms of quality and performance, which lead to sales losses and production waste. Loss of availability leads to have production downtime, and therefore affect delivery times and commercial agreements with customers. Loss of safety could affect humans' life and environmental damage, leading to regulatory compliance violation and financial penalties. *Attack detection* focuses on detectability mechanisms and residual evidence of the attacks trees modelled, which can be determined by understanding adversary's techniques. For example, conducting T840 - Network Connection Enumeration can be detected using network intrusion detection methods, conducting T859 - Valid Accounts to gain privileged access can potentially leave evidence within account policies. *Attack Likelihood* reflects the probability of occurrence for the attacks trees modelled. Based on the historical data collected from several attack groups for FTR sector, there is high probability for the attacks modelled to take place.

Qualitative method reflects risk severities based on five different levels as illustrated in Fig. 4 risk heat map. Based on AV and AL values, Table 3 shows risk severity levels for the scoped ICPS assets. By analysing the FTR risks, the risk matrix can be populated, and risk treatments can be selected from the mitigation controls library. Therefore, FTR risk matrix is populated in Table 3, and the selected security controls are automatically generated based on the meta-data extracted from the FTR digital twin, the engineering tool and the policies library.

4.2. VueOne Threat Modeller and Code Generator Tool (VTM&CG)

To facilitate the implementations of the proposed methodology in this paper, the VueOne Threat Modeller and Code Generator (VTM &CG) tool has been developed. By looking at the VueOne engineering environment in Fig. 7, it is clearly identified that cyber security information is not included for the ICPS, and threat modelling is unavailable during the project development. Therefore, the VTM&CG tool is developed to extend the existing scope of VueOne to include the end-to-end threat modelling and integrate this task as part of ICPS creation to in line with smart manufacturing approaches.

The VTM&CG tool interfaces and integrates with the VueOne Editing / Simulation module that used for modelling the ICPS digital twin, and Siemens TIA Portal engineering tool that used for programming the ICPS assets. This integration enables the VTM&CG tool to deliver threat modelling and mitigation controls automatic generations. The tool has been programmed using Visual Studio C# language. Fig. 9 below demonstrates the novel VTM&CG tool and its integrations with other tools. The VTM&CG tool imports control design meta-data in form of XML file from VueOne digital twin tool, this file contains the modelled FTR assets or components and its sequence of operations. The file contains FTR 3D model that can be used to define operational screens for HMI asset. On the other side, the VTM&CG tool integrates with Siemens TIA Portal tool via TIA Portal Openness, which is application programming interface (API). This integration enables VTM&CG tool to automatically generate control codes (hardware and software) and tailored policies that mitigates the identified risks.

The VTM&CG tool implements the methodology by deploying all steps described in Section 3.2.3. Threat modelling process on the VTM&CG tool starts by importing ICPS network architecture from Siemens tool, where imported assets (scoped assets) are listed on the Purdue Model to indicate asset values. Second step is to model

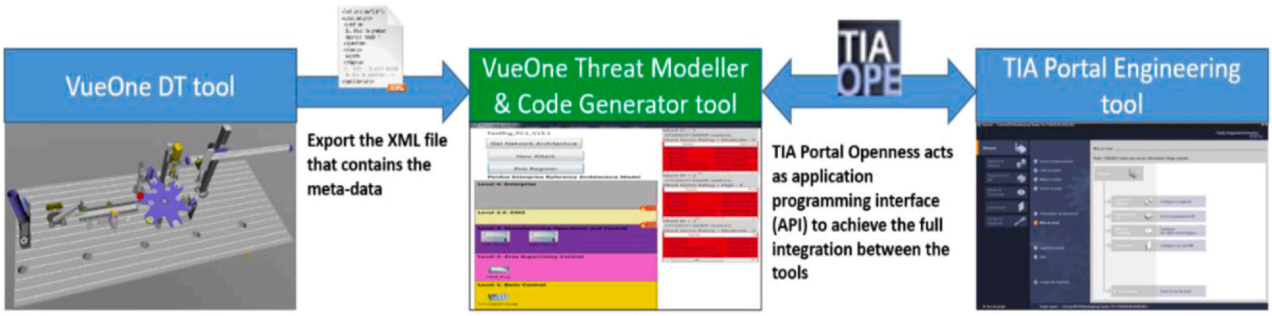

Fig. 9. The VTM&CG tool integrations.

the attack trees using ICS ATT&CK®. Threat actor groups (APTs) benefit from this step as it shows the possible TTPs that an attacker could follow to conduct the cyber-attack. Hence, the modelled attack trees and selected techniques from the ICS ATT&CK® support the analyst to evaluate the data model parameters: Asset Values, Threat Actor, Vulnerability, Attack Impact and Attack Detection. The criteria explained in Table 2 for those parameters are programmed within the tool and the analyst can select the required criteria level from a drop-list menu.

After modelling cyber-attacks and evaluating their data model parameters, the next step is to calculate the AV and AL values from data model parameters, the calculations of AV and AL utilise the formulas illustrated in Section 3.2.4. All the equations are programmed within the tool. Hence, the VTM&CG tool predicts the quantitative and qualitative risk for each modelled cyber-attack. The last step is populating risk matrix that shows all modelled attacks, threats, AV, AL, and risk rating with severities. The same matrix provides the possibility to choose the mitigation controls for each identified risk and generate them automatically to protect the scoped assets from any potential attack.

5. Discussion

The proposed end-to-end threat modelling poses the basis to overcome existing gaps that have been identified in Section 2.4. It also answers the research questions in Section 3.1. The paper's threat modelling exercise has been carried out on a Festo test rig case study with a specific focus on automotive industry. The threat actors in Section 4.1.1 demonstrated actors' motivations and the software resources that can be utilised to conduct a cyber-attack. In addition, it showed threat actor's TTPs, which have been employed during the modelling of the case studies' attacks. Therefore, they helped in modelling the case study's attacks and the analysis of the data model parameters. Although the case study is conducted on an application within manufacturing sector, the proposed methodology is comprehensive and can be used to conduct cyber security analysis in various manufacturing sectors such as transportation, aerospace, machinery, pharmaceutical, and other industries. For example, if this analysis is required for train manufacturing, then same process explained in Section 4.1 can be followed; Threat actors' analysis will be focused on threat groups within the rail sector. Asset criticality will be analysed based on Purdue Model levels. Attacks modelling are carried out utilising the TTPs of ICS ATT&CK®. Risk ratings are calculated based on the quantitative and qualitative methods. Mitigations' countermeasures can be selected from the mitigation library, where the implementation of these mitigations will be generated automatically and can be deployed on the industrial rail assets.

The VTM&CG tool is a good example to practically proof how threat modelling can be integrated with the toolsets provided by Smart Manufacturing and digital twins. Section 4.2 demonstrated how the integration could take place between the newly developed VTM&CG tool, the VueOne digital twin tool and Siemens engineering tool. In fact, this development shows a potential of creating a simulation platform to visualise the cyber-attacks on the ICPS assets and emulate their consequences.

The completeness and adequacy of the proposed end-to-end threat modelling have been examined based on the results from the case study in Section 4 and the reviewed modelling approaches in Section 2.4. The proposed model is in line with smart manufacturing methods as it utilises digital twin tools to fully integrate the modelling exercise within the same digital twin toolset. The model can identify assets criticality based on Purdue Model levels, lower asset levels directly interact with the industrial process and therefore it has higher criticality. The model can predict the cyber risks associated with potential malicious act by a threat actor and determine their severities using quantitative and qualitative methods. The model is able to propose mitigations for the identified cyber risks and execute these mitigations based on an automatic code generation method. Lastly, the proposed model can be scaled to various industrial sectors. Although the proposed model is comprehensive and adequate to be employed within smart manufacturing, but it can be expanded to address areas such as financial losses predictions from the modelled cyber-attacks, simulation of the attack vectors, and insider threat that exposed from the shop floor workers.

The proposed end-to-end threat modelling has been compared with the previous modelling approaches listed in Section 2.4. The work conducted in (Yeboah-ofori and Islam, 2019) has focused on modelling the cyber-attacks using the STIX tool, analysed the risks exposed by them, and propose countermeasures. But it did not link those risks with the assets to show the impact of the modelled cyber-attacks on them. In (Yuan et al., 2015), the work mainly focused on modelling the cyber-attacks, based on the STRIDE method without analysing the risks and proposing mitigations for them. The work conducted in (Fernandez, 2016) aimed to identify the physical processes and assets, then model the cyber-attacks for each process. It lacked identifying the risks for the modelled attacks and mitigating them. In (Schlegel et al., 2015), the work utilised a data model to parametrised several factors for the modelled threats, then analysed the likelihood and the impact to describe the severity for each threat. The work conducted in (Khan et al., 2017) modelled the cyber-attacks based on STRIDE method and analysed the risks for each attack, but did not propose mitigations for them. Most importantly, previous works demonstrated ad-hoc modelling, which do not integrate with ICPS methods and tools and therefore cannot address threats and risks during ICPS creation. Hence, the proposed model bridged those gaps by determining the assets criticality and threat actor's TTPs, then model the cyber-attacks based on ICS ATT&CK® and predicts and analyses the risks with complete proposal for mitigation countermeasures. Furthermore, the proposed model is fully integrated with ICPS methods and tools, which allow to consider threat modelling at very early design stage of ICPS creation.

Table 4
Comparison between the paper methodology and the reviewed methodological solutions.

● Fully comply ◖ Partially comply ○ Not comply

Methodological Solution	In line with Smart Manufacturing	Asset criticality identifications	Quantitative risk identification	Qualitative risk identification	Can be used in critical industries	Cyber-attack modelling	Risk mitigations	Risk matrix generations	Mitigations implementations
The paper methodology	●	●	●	●	●	●	●	●	●
Cyber Security Threat Modeling for Supply Chain Organizational Environments	○	○	●	●	○	●	●	○	○
Developing Abuse Cases Based on Threat Modeling and Attack Patterns	○	○	○	◖	◖	●	○	○	○
Threat Modeling in Cyber-Physical Systems	○	◖	○	○	◖	●	○	○	○
Structured system threat modeling and mitigation analysis for industrial automation systems	○	◖	●	○	●	○	●	●	○
STRIDE-based Threat Modeling for Cyber-Physical Systems	○	◖	○	○	◖	●	○	◖	○

Table 4 has been produced to benchmark the proposed model with the previous work.

6. Conclusions and future work

Nowadays, cyber security is one of the foremost challenges that organisations need to consider when leveraging the benefits of Smart Manufacturing paradigm as the threat landscape is evolving while adopting smart technologies. Hence, to deploy a secure ICPS in smart factories, threats and potential cyber-attacks need to be addressed and risks need to be understood. Therefore, a new approach is required to address these changes and challenges for industrial sectors. Although, the literature review suggests that there are large number of methodological solutions addressing threat modelling for CPS, they are still approaching it traditionally on ad-hoc basis. None of these methodologies has addressed cyber security throughout the entire lifecycle of ICPS and considers the emerging technologies and tools offered by Smart Manufacturing.

Therefore, this paper has presented a five-steps methodology to model cyber threats and assess cyber security for ICPS in smart manufacturing environments. The proposed threat modelling provides a useful guidance for organisations approaching Smart Manufacturing. It is positioning cyber security at the early stage of ICPS developments, identifying assets criticalities, modelling the possible cyber breaches that could affect the target ICPS, analysing the associated risks, and implementing the mitigation controls to protect the target assets from any potential attack. This paper explains the execution of the methodology on an industrial production line, where the results are expected to support researchers, practitioners, and decision makers to understand cyber security for ICPS and provide useful insights to steer all stakeholders for investments in the field of cyber-security.

The paper proposes a structured threat modelling approach that is still in realm of classical threat modelling approach. However, evolved to integrate with cutting-edge Smart Manufacturing methods to provide a complete threat modelling that addressing the entire lifecycle of cyber security including threats identification, cyber-attacks modelling, risks assessment and management.

Based on the paper methodology and the conducted case study, several future work can be foreseen:

- Financial loss predictions and business performance analysis for the cyber-attacks modelled. Precise predications on financial losses and business performance due to cyber incidents is a key when investing in cyber security field. Therefore, a model should be developed to calculate these factors throughout ICPS developments lifecycle.
- Augmented Reality (AR) and Virtual Reality (VR) for ICPS's virtual model in order to virtualise potential scenarios for the modelled attacks and visualise the consequences on data model parameters listed in Table 2.
- Human factor risk analysis. Smart Manufacturing methods and tools are capable of modelling shop floor workers during ICPS development. Hence, cyber risks associated with humans are important to include and analyse at the design stage.

Declaration of Competing Interest

None declared.

Acknowledgements

The authors would like to acknowledge the support of UKRI through the grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research - University of Warwick), EP/N510129/1 (The Alan Turing Institute) and EP/S035362/1 (PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity).

References

Alexander, O., Belisle, M., Steele, J., 2020, MITRE ATT&CK for Industrial Control Systems: Design and Philosophy.
ANSSI, Managing Cybersecurity for Industrial control systems (ICS). ⟨https://www.ssi.gouv.fr/en/guide/managing-cybersecurity-for-industrial-control-systems/⟩ (accessed 12 January 2021).
Chain, C.K., 2020. The Industrial Control System Cyber Kill Chain. SANS Inst..
Cimino, C., Negri, E., Fumagalli, L., 2019. Review of digital twin applications in manufacturing. Comput. Ind. 113.

CIS, Implementation Guide for Industrial Control Systems (ICS). cisecurity.org (accessed 12 January 2021).
V. Components, Visual Components. ⟨https://www.visualcomponents.com/⟩ (accessed 15 January 2021).
Fernandez, E.B., 2016, Threat modeling in cyber-physical systems.
Filkins, B., Wylie, D., 2019. SANS 2019 State of OT / ICS Cybersecurity Survey. SANS.
O. Foundation, OPCUA Vulnerabilities. ⟨https://opcfoundation.org/security-bulletins/⟩ (accessed 23 December 2020).
M.& P. GmbH, WinMOD. ⟨http://www.winmod.de/en/⟩ (accessed 13 January 2021).
Harrison, B.R., Vera, D., Ahmad, B. Ieee, M., 2016, Engineering Methods and Tools for Cyber – Physical Automation Systems.
Harrison, R., Vera, D., Ahmad, B., 2016, Engineering Methods and Tools for Cyber-Physical Automation Systems, 104.
Hutchins, E.M., 2008, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, (2008) 1–14.
ISA, International Society of Automation. ⟨https://www.isa.org/⟩ (accessed 12 January 2021).
Jbair, M., Ahmad, B., Ahmad, M.H., Vera, D., Harrison, R., Ridler, T., 2019, Automatic PLC Code Generation Based on Virtual Engineering Model.
Khan, R., Mclaughlin, K., Laverty, D., Sezer, S., 2017. STRIDE-Based Threat Model. Cyber-Phys. Syst.
Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Comput. Ind. 103.
Magar, A., 2016, State-of-the-Art in Cyber Threat Models and Methodologies.
Maggi, F., Pogliani, M., 2017. Attacks on Smart Manufacturing Systems. IIoT World.
Malwarebytes, APT37 used VBA self decode technique to inject RokRat. ⟨https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/⟩ (accessed 15 November 2021).
MITRE, Common Vulnerabilities and Exposures (CVE®). ⟨https://cve.mitre.org/⟩ (accessed 9 December 2020).
MITRE, MITRE ATT&CK®. ⟨https://attack.mitre.org/⟩ (accessed 30 November 2020).
MITRE, CVE Details. ⟨https://www.cvedetails.com/⟩ (accessed 23 December 2020).
MITRE, Common Attack Pattern Enumeration and Classification (CAPEC). ⟨https://capec.mitre.org/⟩ (accessed 30 November 2020).
MITRE, MITRE ICS ATT&CK Knowledge Base. ⟨https://collaborate.mitre.org/attackics/index.php/Main_Page⟩ (accessed 9 December 2020).
NCCIC, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ⟨https://us-cert.cisa.gov/ics⟩ (accessed 9 December 2020).
Saini, V.K., Duan, Q., Paruchuri, V., 2008, Threat Modeling Using Attack Tree.
Schlegel, R., Obermeier, S., Schneider, J., 2015, Structured System Threat Modeling and Mitigation Analysis for Industrial Automation Systems.
Siemens, NX MCD. ⟨https://www.plm.automation.siemens.com/global/en/products/mechanical-design/mechatronic-concept-design.html⟩ (accessed 13 January 2021).
Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q., 2009. AVOIDIT: A Cyber Attack Taxon.
Status, T.F., Forward, W., 2018. Ref. Incid. Classif. Taxon.
Stouffer, K., Stouffer, K., Abrams, M., 2015. Guide to Industrial Control Systems (ICS) Security. NIST..
D. Systems, 3DEXPERIENCE. ⟨https://www.3ds.com/products-services/delmia/⟩ (accessed 13 January 2021).
Task, J., Transformation, F., 2012. Guide for Conducting Risk Assessments. NIST,.
VDI, The Association of German Engineers. ⟨https://www.vdi.eu/⟩ (accessed 19 February 2019).
Yeboah-ofori, A., Islam, S., 2019, Cyber Security Threat Modeling for Supply Chain Organizational Environments.
Yuan, X., Nuakoh, E.B., Williams, I., Yu, H., 2015. Dev. Abus. Cases Based Threat Model. Attack Patterns 10.
ZDNet, BMW and Hyundai hacked by APT32. ⟨https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/⟩ (accessed 15 November 2021).