



Digital twins in cyber effects modelling of IoT/CPS points of low resilience

Gregory Epiphaniou^{a,*}, Mohammad Hammoudeh^b, Hu Yuan^a, Carsten Maple^a, Uchenna Ani^c

^a Secure Cyber Systems Research Group (SCSRG), University of Warwick, Warwick Manufacturing Group (WMG), Coventry, United Kingdom

^b Information and Computer Science Department King Fahd University of Petroleum & Minerals, Saudi Arabia

^c School of Computing and Mathematics Keele University, Keele, United Kingdom

ARTICLE INFO

Keywords:

CPS
IoT
Cyber resilience
Digital twins
Cyber M&S

ABSTRACT

The exponential increase of data volume and velocity have necessitated a tighter linkage of physical and cyber components in modern Cyber–physical systems (CPS) to achieve faster response times and autonomous component reconfiguration. To attain this degree of efficiency, the integration of virtual and physical components reinforced by artificial intelligence also promises to improve the resilience of these systems against organised and often skillful adversaries. The ability to visualise, validate, and illustrate the benefits of this integration, while taking into account improvements in cyber modelling and simulation tools and procedures, is critical to that adoption. Using Cyber Modelling and Simulation (M&S) this study evaluates the scale and complexity required to achieve an acceptable level of cyber resilience testing in an IoT-enabled critical national infrastructure (CNI). This research focuses on the benefits and challenges of integrating cyber modelling and simulation (M&S) with digital twins and threat source characterisation methodologies towards a cost-effective security and resilience assessment. Using our dedicated DT environment, we show how adversaries can utilise cyber–physical systems as a point of entry to a broader network in a scenario where they are trying to attack a port.

1. Introduction

Modern cyber infrastructures include a wide range of Cyber–Physical Systems (CPS) that are highly diverse in terms of their operations and components with applications found in critical national infrastructure (CNI), healthcare, defence and transportation systems [1]. The interactions between CPS create new threat ecosystems that their characterisation is a challenging task, mainly due to the inability of existing threat models to adequately capture all interdependencies regarding adversarial behaviours and actions in such environments. In addition, the clear explication on vulnerabilities' relationships can create further processing and computational complexity underpinned by the interactions between Physical-to-Cyber (P-C) and Cyber-to-Cyber (C-C) components.

Existing efforts relate to the design and implementation of secure software engineering (SSE) procedures to protect high-value critical missions CPS and, most importantly, establish distinct threat modelling and risk assessment processes early in the software development lifecycle(s) [2]. In that respect, simulation exercises that model real events in threat response and cyber risk assessment attract significant attention. Analytic models establish processes to model the susceptibility of cyber risk and threat in a given

* Corresponding author.

E-mail addresses: gregory.epiphaniou@warwick.ac.uk (G. Epiphaniou), M.Hammoudeh@kfupm.edu.sa (M. Hammoudeh), h.yuan.4@warwick.ac.uk (H. Yuan), cm@warwick.ac.uk (C. Maple), u.d.ani@keele.ac.uk (U. Ani).

<https://doi.org/10.1016/j.simpat.2023.102744>

Received 2 March 2022; Received in revised form 16 February 2023; Accepted 27 February 2023

Available online 15 March 2023

1569-190X/© 2023 The Author(s).

Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Published by Elsevier B.V. This is an open access article under the CC BY license

infrastructure and simulate residual risks and thresholds. The use of modelling and simulation (M&S) processes is a relative new tool in the arsenal of proactive and reactive cyber defence.

These processes can facilitate the early detection of threats and more proactive approaches in mitigating them in CPS and their sub-systems. However, there is currently no model or approach preferred for CPS threat landscape modelling, as both the requirements and threat actors can span across a broad spectrum of interactions between the physical, electronic and cyber domains [3]. That creates challenges around the way that cyber effects and observables are modelled in a simulation environment and the way that cyber attack impact is represented in synthetic environments that utilise different cyber models.

We observe an increase in existing and emerging research efforts that utilise Cyber M&S tools to measure the resistance of CPS/IoT against such adversarial actions [4,5]. In CPS, both targeted and multi-staged attacks can manifest different physical, natural and electronic effects for the same attack propagation scenarios. This makes it extremely difficult to understand the impact of physical and control processes and, thus, deploy safeguards optimally. Simulation tools can be used to calculate the impact of implementing particular controls in an environment and provide a quicker response to the associated cost of defence relevant to these attacks. Due to the complexity and diversity of existing CPS ecosystems, it is hard to trace and examine attacks, as threats and vulnerabilities are harder to detect and assess, especially those that impact availability [6]. In that respect, Digital twins as virtual representations of actual systems and processes, may be used to monitor, visualise, and anticipate the states of CPS/IoT under different attack scenarios. Other security-enhancing use cases of digital twins that may be achieved in systems engineering or during plant operation include security testing and intrusion detection [7].

The purpose of this research is twofold: (a) to examine the effectiveness of DT when integrated with AI-enabled threat source characterisation methodologies for testing and deploying controls in various applications and (b) identify existing gaps when integrating standard security description references for attack analysis (e.g. Cyber standards) with simulation standards. We derive pre-defined attack scenarios using a UK port as a use case executed in a DT environment. We devised a four-step strategy to attain these objectives: (1) Scope definition: Define the scope of the research effort that focuses on cyber modelling and simulation analysis tied to DT technology and cutting-edge AI-threat hunting in the CNI domain. (2) Desk-based study: Conduct a comprehensive literature gap analysis by grouping research in DT for security analysis and incident management, Cyber M&S standards and AI-enabled threat source identification and resilience strategies. (3) Determine operating and testing scenarios in DT and record the efficiency of attack simulation and control analysis for IoT sensors. Lastly, (4) design a plan for development and deployment using a Proof of Concept (PoC) demonstration that allowed us to monitor and record the fidelity of simulations when adversarial actions are modelled and the integration challenges of cyber standards for attack analysis and existing simulation standards. In our use case, a DT was used to estimate potential damages to port assets, operation collision or shut down and information security. The DT also executes attacks demonstrated against certain resilience metrics, which may facilitate designing the security and safety mechanisms of CPSs. Finally, we estimate that the DT could also detect weak spots in the architecture, unnecessary functionality of devices or even unprotected services that would allow an adversary to gain a foothold in the target system.

Our primary contributions and activities on this paper include:

1. Identify the requirements and cyber system description to incorporate DT and AI threat source profiling in M&S.
2. Integrate DT and AI threat source profiling for M&S and derive courses of action (CoA) to simulate resilience metrics in a testbed.
3. Investigate the challenges when integrating cyber standards and simulation standards for security evaluation in IoT/CPS CNI using and actual DT implementation.
4. For the CNI attack simulation, we defined the AI-threat characterisation and important security considerations. We created technical and operational scenarios for a DT for the Southampton port and evaluated the Port's resistance to cyberattacks.

On the basis of these activities, a proof-of-concept of comprehensive cyber resilience testing utilising DT at the Port of Southampton is developed that combines simulation standards and security descriptors to reflect the effects of cyberattacks and resilience measures while recording challenges and issues faced in this process.

The remainder of this paper is structured as follows: Section 2 presents how is DT using virtual digital equivalents to present physical products for cybersecurity. The cyber modelling and simulation standards and methods with regards to their ability to capture cyber observables for security testing are studied in Section 3. Meanwhile, Section 4 discusses cyber resilience testing by using DT while our DT testbed used for mapping the Port of Southampton and adversarial attack scenarios is presented in Section 5. The simulation results are in Section 6, and challenges, open issues and future directions are discussed in Section 7. Finally, Section 8 concludes this paper.

2. Digital twins in cybersecurity

The concept of the Digital Twin (DT), which is using virtual digital equivalents to present physical products, was introduced in 2003 by Michael Grieves for Product Life-cycle Management (PLM) [8]. The DT is a real-time digital counterpart of the physical object or process. Generally, the DT modelling of a physical product contains three parts: (1) what are the physical products components and parameters in the real environment, (2) the mapping of physical products to virtual products in the virtual/digital environment, and (3) the connections of data and information that ties the virtual and real products together. DT can be used to ensure the sustainability and enhancement of existing processes in Critical National Infrastructure (CNI) which is achieved through advanced data analytic and essential resources to inform better decision-making [9].

Table 1
Classification based on the level of data integration [10].

Level of integration	Dataflow	
	Physical→ Digital	Digital→ Physical
Digital model	Manual	Manual
Digital shadow	Automatic	Manual
Digital twin	Automatic	Automatic

Normally, a DT solution is characterised by (i) its intended areas of application, (ii) the used technologies, and (iii) the data integration level [10]. Kritzinger proposed a classification of the DT, that how the data exchange between the virtual replica and its physical counterpart [10]. Table 1 presents the terms digital model, digital shadow, and digital twin, defined based on the data flow to and from the virtual products. The trend demonstrates that DT can rapidly and effectively visualise CPS and its performance and may be implemented in a variety of ways throughout the lifespan of the systems. There are three categories for use cases of DT [11]: (i) monitoring (e.g., health assessment), (ii) mirroring the operation of systems (e.g., lifecycle management), and (iii) decision support (e.g., modelling, visualisation, simulation and optimisation).

DT can be combined with a cyber range to analyse how the system to be engineered behaves under attack [12]. The DT also can run attacks demonstrated against the resilience metrics, which may facilitate the design of the security and safety mechanisms of CPSs. In particular, the DT can be used in four distinct cybersecurity aspects of resilience:

Security identity: A knowledge-based intrusion detection system can be implemented with DT presented by Eckhart and Ekelhart [13]. This intrusion detection technology relies on specific misuse patterns that the system would exhibit upon a compromise [14]. In this study, the DT defined two rules: safety and security rules. The safety rule specifies a threshold for a programmable logic controller (PLC) (maximum velocity of a motor that the PLC controls). In contrast, the security rule defines a consistency check between a PLC tag and a human-machine interface (HMI) tag. During the operation of the CPS, the DT are checked continuously for any rule violations.

Security detection: Virtual products that are representing the system devices should copy functions of corresponding devices with a certain level of detail. For example, with an IoT DT simulator may use the similar communications interface and I/O modules for the hardware layer, while the software layer may be replicated by executing the control logic. If hardware and software configurations of real devices have been manipulated, the DT should exhibit noticeable differences in its characteristics, which could indicate malicious actions.

Security response: DT has the ability which allows penetration testers to implement security tests virtually, such as on digital twins instead of natural systems. In this way, it can be ensured that the implementation of these tests does not negatively affect the operation of live systems. Thus, this approach can be used to fix vulnerabilities of the CPS early in its lifecycle. The DT also can be applied to protect privacy, such as the driver privacy of the intelligent car [15]. In particular, this work explores how automated privacy assessments can be carried out based on a virtual replica of a smart car that continuously receives data (e.g., from on board sensors) in the real-time.

System recovery testing: DT can be coupled with a cyber range for testing the recovery ability [12]. The resilience of CPS can be achieved by a four-step process (i) risk assessment, (ii) resilience engineering, (iii) resilience operation, and (iv) resilience enhancement [16]. These four steps aim to minimise the probability of incidents occurring, their impacts, and the time required to recover from them, albeit at different phases of the lifecycle. Thus, users can determine potential impacts.

3. Cyber modelling and simulation landscape

3.1. Standard cybersecurity description references

Typical cybersecurity description references are studied in this section, including various vulnerabilities’ databases, common attack patterns, and security incident repositories. Based on those reference standards’ features, a list of recommendations is provided on their respective impact in assessing security testing scenarios in IoT simulated environments that leverage a DT. The emphasis is placed on the different M&S standards applicable in DT for the design and execution of computer-assisted exercises that assess the resilience of assets against cyber-attacks. The summary of cyber threats description is in Table 2.

3.1.1. Common vulnerabilities and exposures (CVE)

CVE can be used to model multi-stage cyberattack scenarios where privilege escalation, exfiltration and malware propagation attacks are to be modelled. Certain CVE information can be used in modelling attacks against data and information integrity (spoofing, forgery, etc.). Although this entails that further processing is necessary to identify these vulnerabilities relevant to IoT devices, CVE can develop and test automated processes that assess IoT devices and support the modelling of those in emulated (often with simulation) environments.

Table 2
Summary of cybersecurity description references.

Ref.	Type	Organisation	Recommendation	Data Search
CVE	Vulnerabilities Database	MITRE Corporation	<p>CVE can be used to model multi-stage cyberattacks scenarios where privilege escalation, exfiltration and malware propagation attacks are to be modelled.</p> <p>CVE can develop and test automated processes that assess IoT devices and support modelling those in emulated (often with simulation) environments.</p>	CVE ID
NVD	Vulnerabilities Database	ITL, NVD	<p>NVD vulnerabilities database is a repository of standards-based vulnerability management data. It enables the automation of vulnerability management, security measurement, and compliance.</p> <p>The security measurements aspects also support system design knowledge (e.g. IoT sensor reactions to events)</p>	CVE ID or OVAL query
CVSS	Vulnerabilities Scoring	FIRST. Org, Inc.	<p>A key component of CVSS is that any ambiguity regarding vulnerabilities is removed, making it clearer to characterise them in terms of exploitability and impact.</p> <p>A gap between actual versus theoretical risk exists that might alter (erroneously) any mitigation prioritisation efforts.</p>	NVD CVSS Calculators
CWE	Weaknesses Database	MITRE Corporation	<p>CWE contains hardware weaknesses, which can inform better modelling of different attack types in the simulation environment where different weaknesses are exploited in combination or in sequence to achieve a specific negative (adversarial or unintended) outcome affecting resilience.</p> <p>However, CWE does not support advanced reasoning tasks on software weaknesses, such as predicting missing relations and expected consequences. Such reasoning tasks become critical to managing and analysing large numbers of common software weaknesses and their relationships.</p>	CWE List
CPE	Naming Scheme	NIST	<p>CPE Product Dictionary provides an agreed-upon list of official CPE names. So all vulnerability and configuration information items have an important distinction that affects, which helps IT and security management.</p> <p>However, naming IT platforms is subject to vulnerability and configuration guidance, one of the requirements is the application environment. It is not easy to define because of the multipurpose usage of the software. Such as, the IoT and computer networks share the same software platform.</p>	URI
CAPEC	Common Attack Patterns	MITRE Corporation	<p>The CAPEC can analyse attack patterns from the expected data leakage, resource depletion, and spoofing categories to include broader emerging classes such as physical, social, and supply chain attacks.</p> <p>However, the attack patterns are specified from the attacker's viewpoint. Therefore, unintentional and unexpected behaviours of attackers are impossible to analyse.</p>	CAPEC List
RISI	Security Incident Database	MITRE Corporation	<p>CSIS can be used to analyse cyber risk in the industry sector. It is a set of brief descriptions not specific to control systems, and with minimal detail, it helps the industry assess its security level.</p> <p>However, only a few organisations have initiated a higher engagement level to identify and eliminate the most significant vulnerabilities.</p>	ISID

3.1.2. National vulnerability database (NVD)

NVD vulnerabilities database is a repository of standards-based vulnerability management data. It enables automation of vulnerability management, security measurement, and compliance. The NVD can also provide a common language for discussing, finding and dealing with software security vulnerabilities. The ability of NVD to provide a contextual understanding of threats and their assessment can support further validation of threats before injecting them into a simulated environment. The security measurements aspects also support system design knowledge (e.g. IoT sensor reactions to events). In conjunction with different descriptors such as CAPEC, it can better represent threats in a simulated environment [17].

3.1.3. Common vulnerability scoring system (CVSS)

CVSS can be used to model how a vulnerability can be assessed and the anticipated impacts of their exploitation. It attempts to reduce the complicated multi-variable problem of security vulnerability. A key component of CVSS is that any ambiguity regarding vulnerabilities is removed, making it clearer to characterise them in terms of exploitability and impact. This can support M&S of attack progress, and malware propagation scenarios as CVSS provides the flexibility to model pre and post conditions of the vulnerabilities exploitation. This is a desirable feature in technical scenarios tested in simulated environments.

The usefulness of CVSS to the Internet of Things is still a matter for debate. Many researchers feel that the scoring inadequately represents the many challenges presented by some of these new devices. The scoring process is relatively static, and it is based on the theoretical risk a vulnerability might impose. That risk is often assessed once and does not consider the changing threat landscape conditions within which the vulnerability might be exploited. Thus, a gap between actual versus theoretical risk exists that might alter (erroneously) any mitigation prioritisation efforts. In a cyber M&S environment, this might have an adverse effect as wrong mitigation prioritisation might give the false perception of severity in measurements related to resilience.

3.1.4. Common weakness enumeration (CWE)

Common Weakness Enumeration (CWE) is a community-developed list of standard software and hardware weakness types with security ramifications. The weaknesses include flaws, faults, bugs, vulnerabilities, or other software or hardware implementation errors, code, design, or architecture that, if left unaddressed, could result in systems, networks, or hardware being vulnerable to attack.

3.1.5. Common platform enumeration (CPE)

CPE Product Dictionary provides an agreed-upon list of official CPE names. Hence, all vulnerability and configuration information items have an important distinction that affects IT and security management. However, for naming IT platforms subject to vulnerability and configuration guidance, one of the requirements is the application environment.

3.1.6. Common attack pattern enumeration and classification (CAPEC)

The Common Attack Pattern Enumeration and Classification (CAPE) provides a publicly available catalogue of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities [18]. The CAPEC can analyse attack patterns from the expected data leakage, resource depletion and spoofing categories to include broader emerging classes such as physical, social engineering and supply chain attacks. CAPEC can be combined with automated tools to generate attack scenarios and security events agnostic to the underlined network status in terms of vulnerabilities. That makes the model flexible in interpreting different categories of adversarial actions and parameter estimates that correspond to attack features in IoT or CPS in general. However, the attack patterns are specified from the attacker's viewpoint. Therefore, unintentional and unexpected behaviours of attackers are impossible to analyse and cause issues with modelling the environment in simulations.

3.1.7. Security incident database (RISI)

CSIS can be used to analyse cyber risk in the industry sector. It is a set of brief descriptions, not specific to control systems, and with minimal detail, it helps the industry assess its security level. However, only a few organisations have initiated a higher engagement level to identify and eliminate the most significant vulnerabilities.

3.2. Cyber modelling and simulation standards

Traditional M&S models were originally designed to address military C2 and training needs with limited exposure and access to the scale and velocity of cyber threats experienced today. They are also designed to incorporate traditional mission-centric scenarios with limited capability to represent the impact of threats on cyber assets' security and resilience. Recent developments in cyber standards for M&S include those that categorise incidents using threat information exchange (See TAXII and CyBOX), situational awareness of threat-related scenarios, and visualisations of threat and attack analysis. The aim is to better understand the diverse and constantly changing threat landscape and standardise how cyber incidents are understood and communicated. The Summary of cyber modelling and simulation standards is in [Table 3](#).

3.2.1. Cyber range interoperability standard (CRIS)

CRIS can connect cyber models to logical scenarios for security testing and training exercises. It contains a set of assets and capabilities located at one or more sites. It can accommodate tailored scenarios related to cyber resilience steps (e.g. identify, prevent, detect, respond and recover) but at the expense of increased complexity. In terms of IoT/CPS the benefit is that it incorporates multiple cyber models connected to each scenario allowing for greater flexibility in terms of the attacks introduced and represented by a threat. Throughout our investigation, we note a challenge to appropriately integrating cyber standards with simulation standards. For example, the traffic generator model used in a Cyber Range can influence the cyber event's fidelity in the synthetic environment. There still seems to be a gap in integrating cyber standards with simulations standards in an effective way to provide a holistic representation of scenarios, particularly those that include IoT and CPS. More work is also needed in understanding how different cyber models are connected in logical ranges and how this affects the accuracy of attack simulations. However, there are several shortcomings in operational testing, Integration Conferences, Network Maps and Instructions, Remote Access Management, and Automation and Pre-configuration Templates [19].

Table 3
Summary of cyber modelling and simulation standards.

Standards	Organisation	Type	Recommendation	Publish date
CRIS	US Department of Defense	Cyber Range Interoperability Standards	<p>CRIS can connect cyber models to logical scenarios for security testing and training exercises. It contains a set of assets and capabilities located at one or more sites.</p> <p>However, there are several shortcomings in operational testing, Integration Conferences, Network Maps and Instructions, Remote Access Management, and Automation and Pre-configuration Templates [19].</p>	Nov 2015
DIS: IEEE 1278 Series	IEEE	Distributed Interactive Simulation	<p>Series of 1278 is a group of standards about the data message in different computer network layers. It has various applications such as Entity Information/Interaction, Warfare, Logistics, Simulation Management, Distributed Emission Regeneration, Radio Communications, Entity Management, Minefield, Synthetic Environment, Simulation Management with Reliability, Information Operations, Live Entity Information/Interaction and Non-Real-Time protocol.</p> <p>However, for the CPS, the cyber threats and issues mix with different domains rather than the computer networks.</p>	August 2012
HL-A: IEEE 1516	IEEE	Regulation of HLA	<p>HLA can interact with other computer simulations regardless of the computing platforms for the CPS simulation and provides an abstraction of logical time that allows for time synchronisation between simulators with different time semantics.</p> <p>Also, the FOM can include attack attributes related to specific scenarios for the simulation interactions within and across a DT platform, similar to our testbed. Examples could consist of the representation of an attack's impact on C4C/C4O simulations.</p>	August 2010
RFC 5070	Network Working Group	Data Representation	<p>RFC 5070 is a format for representing computer security information commonly exchanged between CSIRTs. It provides an XML representation for conveying incident information across administrative domains between parties with operational responsibility of remediation or a watch-and-warning over a defined constituency.</p> <p>However, the new GDPR announced plenty of data sharing and transformation restrictions.</p>	Dec 2007
NATO: NISP, STANAG 4631, STANAG 5067	NATO	Programme Management	Standards or profiles are enforced for NATO joint-funded systems in planning, implementing and testing. However, the standard's application is only used for testing and programme /project planning.	2012-2020
DODD 8500.1	US Department of Defense	Information Assurance	<p>The DoDD 8500.1 is a directive of operating regulation of information security within the defence department.</p> <p>However, It is not a reasonable fit for civil purposes. It needs an update as well after nearly 20 years later.</p>	November 2003
THE DHS-7	Department of Homeland Security	Cybersecurity Guidance of ICS	DHS-7 is fundamental guidance for the cyber defence of industrial control systems. However, it is not directly applicable to cybersecurity modelling and simulation.	January 2015

3.2.2. DIS:IEEE 1278 series

Distributed Interactive Simulation (DIS) is an IEEE standard for conducting real-time platform-level wargaming across multiple host computers. Simulation state information is encoded in formatted messages, known as protocol data units (PDUs) and exchanged between hosts using existing transport layer protocols, including multicast. Series of 1278 is a group of standards about the data message in different computer networks layers. It has a wide range of application such as Entity Information/Interaction, Warfare, Logistics, Simulation Management, Distributed Emission Regeneration, Radio Communications, Entity Management, Minefield, Synthetic Environment, Simulation Management with Reliability, Information Operations, Live Entity Information/Interaction, and Non-Real-Time protocol. However, for a CPS, the cyber threats and issues mix with different domains rather than the computer networks.

3.2.3. HL-A: IEEE 1516

High-Level Architecture (HLA) is the capstone document for a family of related HLA standards. The architecture's main function is to provide a platform for reusing and flexibly interoperating simulation systems. It allows developers to incorporate system parameters and exchange those with other simulation systems and assets. This can be used using the Federation Object Model (FOM) that specifies how information is exchanged in runtime [20]. Also, the FOM can include attack attributes related to specific scenarios for the simulation interactions within and across a DT platform, much similar to our testbed. Examples could consist of the representation of an attack's impact on C4C/C4O simulations.

3.2.4. RFC 5070

The Incident Object Description Exchange Format (IODEF) [21] defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This document describes the information model for the IODEF and provides an associated data model specified with XML Schema. RFC 5070 is a format for representing computer security information commonly exchanged between CSIRTs. It provides an XML representation for conveying incident information across administrative domains between parties with operational responsibility of remediation or a watch-and-warning over a defined constituency.

3.2.5. NATO: NISP, STANAG 4631, STANAG 5067

NISP gives guidelines to capability planners, programme managers and test managers for NATO joint funded systems in the short or mid-term timeframes [22]. The NISP prescribes the necessary technical standards and profiles to achieve Communications. The DoD 8500.1 is a directive of operating regulation of information security within the defence department. Most of the programmes for CNI fell under this standard within DoD. The references to operational resilience of mission-critical functions and network operations through a dedicated supporting acquisition programme presents indicators on the application of cyber M&S tools mainly on [23] (a) planning for mission continuation (b) exercising under realistic cyber conditions (c) periodically evaluate the ability to operate under loss of data or connectivity and (d) rapidly and dynamically allocate resources to sustain mission operations.

3.2.6. THE DHS-7

DHS-7 is fundamental guidance for the cyber defence of industrial control systems (ICS). It follows seven strategies as part its approach enumerated as follows: (1) Implement application whitelisting (2) Ensure proper configuration/patch management (3) Reduce your attack surface area (4) Build a defendable environment (5) Manage authentication (6) Implement secure remote access (7) Monitor and respond. DHS-7 is fundamental guidance for the cyber defence of industrial control systems but is not directly applicable to cybersecurity modelling and simulation.

Finally, in terms of best practice(s) for the establishment of simulation environments, the Simulation Interoperability Standards Organisation (SISO) proposes the Distributed Simulation Engineering and Execution Process (DSEEP). This simulation standard deploys an iterative spiral model for the representation of cyber effects in more traditional scenarios. DSEEP is a generalised process for developing distributed simulation applications with an open community that maintains it. This process can support infrastructure interdependency analysis that requires the simulation of multiple domains (for the CNI case).

4. Cyber M&S for resilience testing

Cyber resilience is essential to a hyper connected system and refers to the ability of that system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with adversaries [24]. Hacking and failures of such systems have an impact on critical services with potentially significant consequences. Therefore, improving their resilience is a crucial challenge. We use the term resilience strictly as the capacity of a system to recover from disruptions.

The resilience definition was used to define metrics in the four domains: (a) physical, (b) information, (c) cognitive, and (d) social [25]. Furthermore, this resilience framework was applied to develop resilience metrics for cyber systems [26]. The R4 framework comprises robustness (the ability of systems to function under degraded performance), redundancy (identification of substitute elements that satisfy functional requirements in the event of significant performance degradation), resourcefulness (initiate solutions by identifying resources based on prioritisation of problems), and rapidity (ability to restore functionality in a timely fashion).

A framework of cyber resiliency engineering was presented by MITRE, which identifies the goals, threat model and structural layers of cyber resiliency [27]. In addition, the National Institute of Standards and Technology (NIST) offered a cyber resilience framework to improve the cybersecurity and resilience of critical infrastructures [28]. This framework presented five functions at the highest levels: identity (understanding and managing the risk to systems, assets, data, and capabilities), protect (implementing the appropriate tools to ensure critical infrastructure services delivery), detect (identifying cybersecurity events occurrence), respond (taking action regarding cybersecurity events), and recover (restoring capabilities or services impaired due to a cybersecurity event).

Some researchers analysed the resilience of the CPS. Such as the work provides detailed guidelines for ICS security [29]. Furthermore, Collier outlines the general theory of performance metrics and highlights examples from the cybersecurity domain and ICS [30]. Finally, the necessary measures to be taken to make ICS and critical infrastructures resilient was defined in [31].

A state estimation algorithm resilient to sparse data injection attacks on the CPS was presented by Yong [32]. Koutsoukos presented a simulation and integrated modelling platform of cyber resilience in transportation systems [33]. However, the resilience metrics to measure the quality quantitatively were not clearly defined. Another issue of these frameworks is that they apply to the

cyber–physical system (CPS) is not suitable. First, because CPS necessitates a short recovery time and quick response, it differs from typical ITS [34]. Furthermore, ITS is more accessible to apply the anti-malware software and automatically download and apply security patches compared with the CPS. On the other hand, the CPS systems are designed for functional purposes rather than security aims, and the devices in CPS are limited memory and processing capacity [34].

4.1. Cyber resilience assessment using digital twins

Cyber resilience assessment defines the form and the speed of system recovery and adaptation after a cyber attack or an incident based on natural events. Various methods refer to resilience assessments [35]. The two types of assessment methods used for cyber resilience are metrics-based and model-based. Metric based approaches use system individual components or functions to assess the overall system performance of resilience. In contrast, model-based approaches use system configuration modelling and scenario analysis to predict system performance.

Collier et al. presented the cyber metrics as the performance measures of the cyber system [30]. At present, the lack of universally applicable resilience measurement and the inability to formalise the value system related to the current problems are the obstacles to the broad implementation of metrics-based methods.

The model-based approach is a way that tries to represent the real world and define resilience by using mathematical or physical concepts. The modelling usually requires knowledge of system functions, mission, patterns, thresholds, system memory and adaptation [36]. A combination of the two mentioned methods for cyber resilience assessment was presented in a tiered framework [37].

The limitation of these approaches is that they lack a precise representation of adversarial behaviours, especially in targeted or multi-stage cyber attacks that use physical components as the attack agents. More traditional approaches such as STRIDE and DREAD have also been deployed with an active debate on the efficacy in CPS due to their emphasis on security analysis of Internet-based applications. The lack of a systematic approach that automates security analysis in CPS has also been flagged as a gap in the existing knowledge base [38]. The authors emphasised the necessity to develop techniques that consider the emerging threat landscapes as a function of hardware and software interactions rather than considering threats in isolation. The inherent ambiguity in modern cyber infrastructures renders the modelling of incomplete observations a fundamental step in the threat source characterisation processes.

That creates additional challenges in visualising critical infrastructure interdependencies in a simulation environment to maintain asset and threat characteristics across different datasets.

An IoT-based cyber–physical DT is implemented with the microgrid control system to ensure its proper resiliency [39,40]. Similarly, a DT and reinforcement learning (RL)-based production control method was studied for micro intelligent factory resilience [41]. However, sophisticated adversaries can learn the defence strategies and use clandestine attack strategies to avoid detection. The authors used DT to enhance the security level of CPS. They designed a Chi-square detector in a Digital Twin (DT), an online digital model of the physical system [42].

DT used in supporting the resilience of intelligent factories was addressed by Becue et al. [43]. The authors introduced a novel approach that integrates human behaviour and capacities for security testing with Digital Twins. It shows how Digital Twin can enable resilient Factories of the Future.

The DT for cyber resilience has been widely implemented, and the authors provided a study of cyber resilience in healthcare DT [44]. In addition, they presented a novel scheme for recognising potentially vulnerable functions to support healthcare digital twins. Finally, a novel end-to-end scheme was proposed for cyber resilience, which can recognise potentially vulnerable functions. For supply chain control, a DT based framework was studied for supply chain recoverability for operation resilience [45]. Work in [46] discuss further the integration challenges when DT couples with Federated Learning technologies are used for managing resources in smart cities. Authors show that in IIoT, the decision-making of the DT is data-driven and based on the vast amounts of data that are dispersed among several industrial devices. In IIoT, data islands exist in real-time, and there are also privacy concerns; consequently, it is extremely difficult to combine data that is dispersed across several devices.

5. DT testbed and adversarial scenarios

Our DT addresses industry-focused cybersecurity challenges in IoT-enabled CNI and emulates critical components of wind/solar farms, smart cities/homes with electrical distribution and vehicle charging technologies, as in Fig. 1. Our AI-enabled DT emulates infrastructure at scale and enable experimentation to optimise resilience against cyber and other attacks. It integrates with a new generation of Schneider Electric infrastructure products that are IoT enabled and secured by Blueskytec's technology-enhanced by AI/ML technology and AI cyber defence tools (see Fig. 2). We run experiments on a DT that connects a physical testbed to thousands of virtual devices to provide a massive-scale demonstrator required to effectively model and test AI security models by learning from virtual and physical data. The ability to visualise physical assets and the incorporation in real-time provides users of the testbed with excellent visibility and understanding of the conditions and performance of the whole system. Furthermore, the data analysis provides robust insights into services provision and potential interventions required to understand the impact of the key metrics behind the attacks demonstrated.

The combination of the virtual and real-world helps overcome the inherent limitations of testbeds, specifically, large-scale physical testbeds that quickly become cost-prohibitive and are restricted in scope. For example, the traditional testbeds cannot take a real environment cyber-attack test due to natural limitations, whether with a simplified physical or digital simulation. In our work, we linked the reaction with the virtual and real-world.

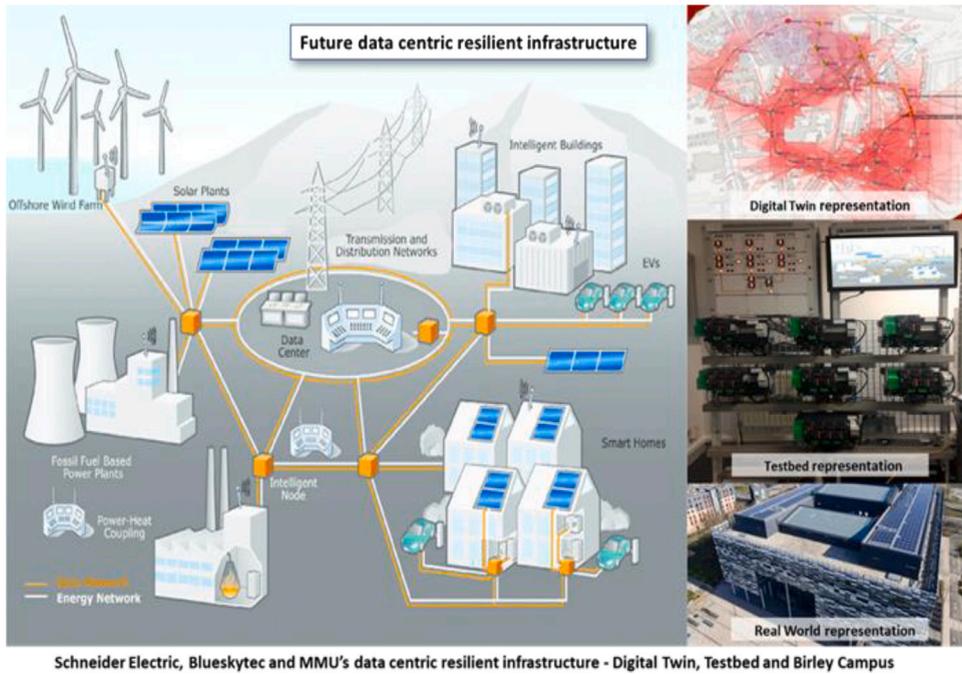


Fig. 1. An illustration of our DT testbed showing the virtual component (top right-hand corner of the screen) and physical components (campus building and power control system).

An integrated testbed and digital twin

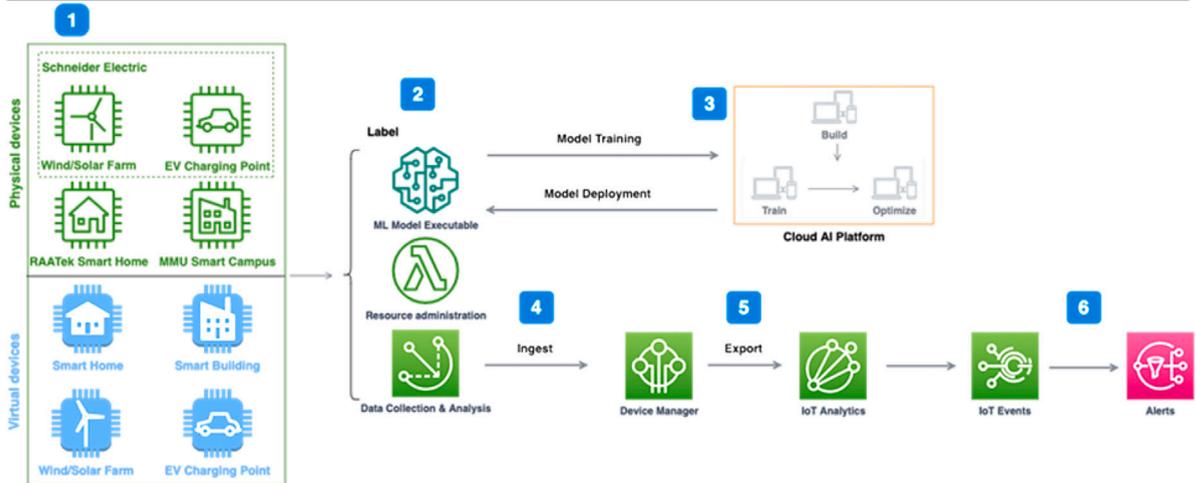


Fig. 2. Digital Twin integrated testbed.

Our DT can use AI to inject random failures and optimise resilience. AI learns with each interaction in our massive-scale CNI to connect the dots between advanced persistent threats and provide actionable insights for making informed decisions quickly and accurately. Through machine and deep learning techniques, our DT improves knowledge to understand cybersecurity vulnerabilities, threats, motives and risk and launch an orchestrated response to mitigate the threat with high confidence and speed.

In Fig. 2: (1) Shows physical and virtual CNI, including Schneider’s electrical infrastructure IoT, enabled and secured by Blueskytec’s technology, and our smart campus and smart energy nodes and services run. (2) A cloud service running serverless user code (e.g. Google Functions, IBM’s OpenWhisk, AWS Lambda) gets triggered in their applications. Data collection and close to origin analysis (e.g. AWS IoT Greengrass Core) (3) Cloud AI platform (e.g. Amazon SageMaker - AWS) to build, train, and deploy machine learning (ML) models. (4) A service (e.g. AWS and Google Cloud IoT Core) securely connects and manages globally dispersed IoT devices (5) and (6) Analysis of IoT data, builds responses and raises security alerts.

5.1. Description and scope

The maritime industry is becoming more and more digital. For decades, most maritime operators have adopted digital technology to modify their business models and improve process efficiency, thereby creating customer value, complying with legal requirements, and generating competitive advantages. For example, more than 90% of the global merchant fleet uses digital systems: connect digital navigation networks and radar; support access control to ensure personal safety, ship management or crew welfare, and ships, shippers and seaports Communication between; support cargo loading, management and control, and make cargo manifests, loading lists and other documents. As a result, essential infrastructures are becoming a popular cyber attack target, such as US fuel pipeline cyber attacks.¹

Ports are critical nodes of global trade. Approximately 80% of world trade is transported by sea, thus comprising an integral part of critical infrastructure. In addition, ports hold substantial amounts of data and are involved in many monetary transactions and stakeholders; therefore, port cybersecurity and operational safety are critical issues for the port authority responsible for ensuring port safety and security. The digital transformation of ports has also led to a change in the sector's cyber risk profile, cybersecurity incidents in ports over the past few years, such as the cyberattack in the NotPetya Ransomware incident and its impact on Maersk and the wave of ransomware attacks in Port of Barcelona.² and San Diego³

5.2. Multi-stage cyber-attack against Southampton port

Generally, the cyber threats of a port can be analysed at 25 different items in three different cybersecurity attributes: human, infrastructure, and procedure. In addition, there are 45 IoT devices/sensors-nodes in the field in the user case, including underwater devices, floating devices, stationary/mobile devices, large-area networking, heterogeneous devices, intermittent logistic unit, etc. Some of the security challenges are generic within the IT or Operational Technology (OT) environment, while others are specific to port ecosystems. Table 5 identifies the possible impact of cybersecurity incidents for a port [47].

The Port of Southampton is a cargo and passenger port in the central part of the south coast of England. It is one of the UK's busiest deep-water ports with a diverse variety of water users with approximately 1.7 million cruise passengers, around 820,00 vehicles and more than 1.5 million TEUs per year. Our use case proposes deploying intelligent monitoring IoT devices on buoys to monitor marine traffic in and out of the Port to enhance safety and security. These devices are equipped with motion, radar and other sensors to detect and measure the speed and direction of moving objects.

In our use case scenario, 32 virtual and 14 physical IoT devices are deployed over the waters of the 726 acres port (see Fig. 4). There is no publicly available sensor data from the Port that could be incorporated in the DT. Our study is based on synthetic data generated based on information obtained through trial access to The IMO-Vega Database.⁴ For our operations scenarios, we select manipulating the IoT network through (1) GPS Spoofing to cause collision between two moving vessels and (2) malware attack to allow a moving vessel to evade detection. The Security Metrics for both the operational and the technical attack scenarios are defined in Table 4.

6. Results and discussion

6.1. Port attack scenario 1: propagation of ransomware

The adversaries can develop ransomware exploiting different vulnerabilities to spread it into the port networks and encrypt the different systems and devices (workstations, servers, etc.), leading to the destruction of the infected systems and the potential loss of backups (within servers which could be encrypted). The implementation in the DT shows in Fig. 3. Table 6 shows the scenario parameters used in our scenarios.

Attack details:

- The Port updates one of its servers with a compromised update (ransomware) – other ways can be used to introduce ransomware on port systems, for example, social engineering (phishing or USB-drop for example) or wrong network segregation (broad exposure to the Internet)
- The ransomware spreads into the Port's network, using some unpatched vulnerabilities and lack of network segmentation;
- The ransomware is executed on the Port's systems and devices and steal stored credentials.
- The ransomware executes a mechanism of elevation of privileges, using wrong segregation of highly privileged accounts.
- The exact mechanism of the ransomware spreads into another part of the Port's network.
- The infected systems and devices are encrypted and cannot be used anymore.
- A ransom is required while all the systems and devices are down.

Attack implementation in the DT

¹ <https://www.bbc.co.uk/news/business-57050690>

² <https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona>

³ <https://www.portofsandiego.org/press-releases/general-press-releases/port-san-diego-releases-additional-information-cybersecurity>

⁴ <https://www.imo.org/en/publications/Pages/IMO-Vega.aspx>

Table 4
Security Metrics for both the operational and the technical attack scenarios.

Security metrics	Examples	Description
Probability (attack Graph)	AGP	Attack-based Probabilistic
	BN	Bayesian Network metrics
	AMC	Absorbing Markov chain
Structural (Attack-Graph)	SP	Shortest path
	NP	Number of paths
Temporal	MTTR	Meantime to recovery
	MTTB	Meantime to breach
	MTFF	Meantime to the first failure
	MTTA	Meantime to acknowledge
	MTBF	Meantime between failures
	MTD	Meantime to detect
Third-party response	SLA	Service level agreement compliance
	SA	System availability
Incident Management	MIRC	Mean Incident Recovery Cost
	MTID	Meantime to Incident Discovery
	NI	Number of Incidents
Vulnerability Management	VSC	Vulnerability Scanning Coverage
	PSNKSV	Per cent of Systems with No Known Severe Vulnerabilities
	MTMV	Meantime to Mitigate Vulnerabilities
	NKV	Number of Known Vulnerabilities

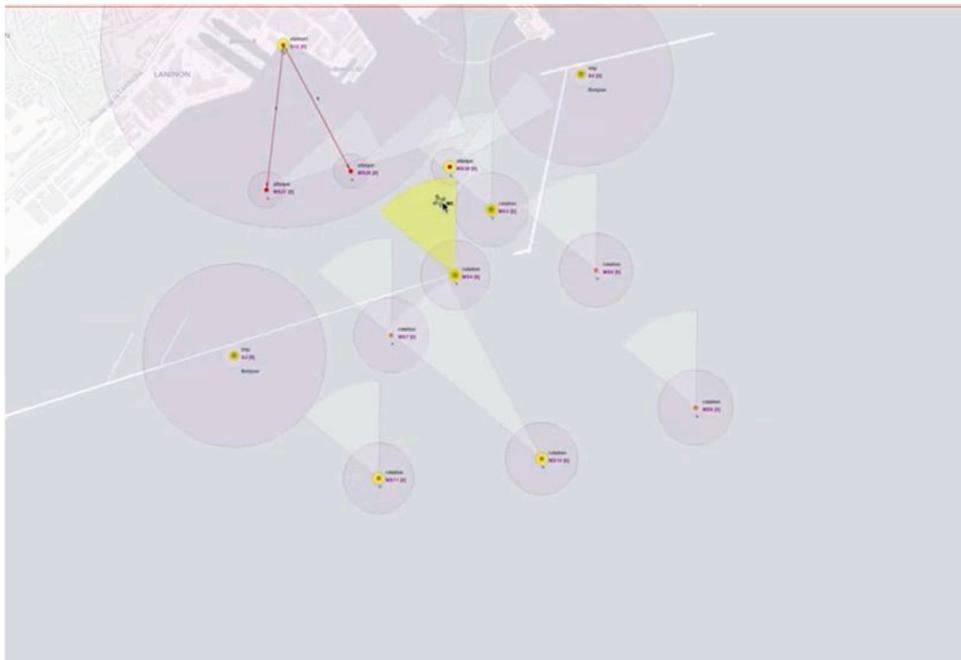


Fig. 3. Shows the ground devices, floating devices (both fixed and mobile) and the malicious vessel.

- 14 navigational buoys were implemented on a Raspberry Pi equipped with a camera, vibration, and 3D accelerator.
- 32 virtual buoys were implemented in the DT that communicate in real-time with the physical devices.
- One virtual ship was implemented in the DT as the malicious object that injected malware into the buoys.
- The ‘worm’ exploits devices with a default username and password to expose the device by opening an SSH port to the public Internet.

A simple Command & Control Centre will prevent navigational buoys from reporting a detected object to the port traffic control. We use the following software to generate and broadcast a gps signal on a Windows machine. We use GPS-SDR-SIM to generate GPS

Table 5
Possible impacts for ports cyber threats [47].

Impacts	Description
The shutdown of operations, port paralysis	The shutdown of the port operations is a much-feared impact by the port ecosystem: if it lasts more than a few hours, it can harm strongly the commercial operations (loss of money), the delivery of essential goods for a nation, especially for the islands (food, fuel, etc.) as well as pose safety and security issues (queue of several boats at the port entrance).
Human injuries or death, Kidnapping	Ports must face high security and safety challenges because many people who work in port areas can perform dangerous jobs (manipulation of cranes, dangerous goods, etc.) and because ports also must manage a large passenger flow easy to predict (ferries, large cruise vessels, etc.).
Sensitive and critical data theft	Port systems may hold critical information, whether it is personal information (crew or passenger data), critical commercial information (location and content of containers, competitive know-how) or National security information (Port being essential assets for a nation): the theft of this information can have disastrous consequences.
Cargo and goods stealing	Attackers can browse cargo and container lists to identify the most valuable goods for black markets (to be stolen in the Port or targeted for future piracy attacks when the ship is at sea).
Illegal trafficking	The marine ecosystem is one of the largest playgrounds for organised crime: ports are often used for illegal and criminal traffic.
Financial loss and costs	A port can lose money due to operations stop or for repair budget in case of damage to its systems and infrastructure
Fraud and money steal	Like any significant company, the financial systems of the ports can be compromised to steal money from them. Indeed, especially for the most important ports, the port revenues are essential. Moreover, since ports are the border between two States or continents, fraudulent companies can falsify their customs declarations (VAT fraud).
Systems damaged or worst, destruction	Due to the high complexity of port systems and infrastructure, some of which are critical (e.g. industrial systems that manage large amounts of dangerous goods), damage or worse, destruction to those systems and infrastructure has disastrous consequences for port operations and safety and security, including people. For example, tankers (especially refined products and gas) are very vulnerable to fire and explosion; local storage of flammables and chemicals is also possibly massive.
Tarnished reputation, loss of competitiveness	Nowadays, ports are in a highly competitive international ecosystem: the slightest incident or problem on its activities and operations can damage its reputation and lose customers who could direct their traffic to neighbouring ports.
Environmental disaster	As the Port is the direct interface between the hinterland and the sea, and environmental disaster in port areas can have disastrous consequences on populations, fauna and flora and human infrastructure at a very long distance (oil spill, gas explosion, ocean pollution, shipwrecks, etc.).

Table 6
Parameters for scenarios 1 and 2.

Attack impact	Assets affected
Tarnished reputation	IT systems
Financial loss and costs	OT systems and networks
Systems damaged, or worst, destruction	OT end-devices
Slow down of port operations, port paralysis	People Information and data

baseband and signal data streams, which can be converted to RF using software-defined radio (SDR) platforms⁵ such as ADALM-Pluto, BladeRF, HackRF and USRP. The software requires a GPS satellite constellation through a GPS emission ephemeris file to generate

⁵ <https://github.com/osqzss/gps-sdr-sim>

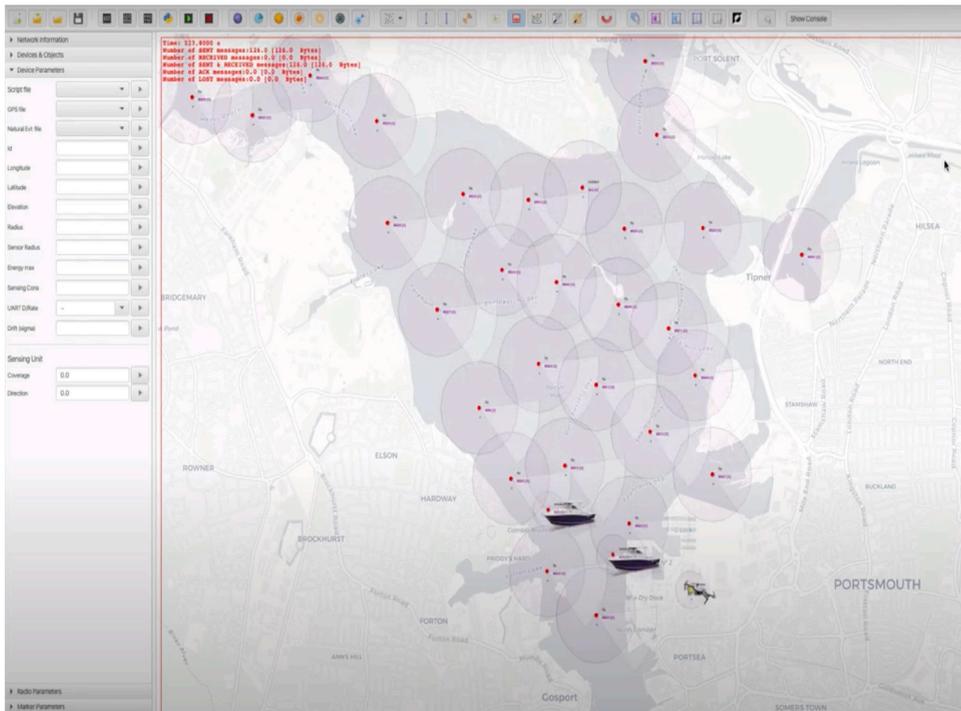


Fig. 4. Actors involved in the attack scenario.

the required signal. We downloaded the GPS broadcast ephemeris file.⁶ To communicate from our Windows machine with the HackRF device and transmit the generated file, we use the hackrf-transfer.exe.⁷

6.2. Port attack scenario 2: GNSS spoofing attack

The attacker spoofs the GNSS data of the GNSS location. Autonomous systems rely on an insecure positioning system, such as autonomous Ships – Cargo Vessels, Sailing Yachts, etc. A fake GNSS location to hide itself prevent tracking movements. It may cause a collision between two moving vessels. The attack details and implementation are as follows:

- Generate the simulated pseudo range (location data) with GPS-SDR-sim CSV file with positions, a fixed location or a user-defined trajectory.
- Generate the simulation file
- Transmitting via SDR – device (HackRF or bladeRF)
- The Cargo Vessels misleading with the wrong location information cause the ship traffic collision.

Attack implementation in the DT

- 14 navigational buoys were implemented on a Raspberry Pi equipped with a camera, vibration, and 3D accelerometer.
- 32 virtual buoys were implemented in the DT that communicates with the physical devices in real-time.
- Two virtual vessels were implemented in the DT to model vessels entering the port.
- A malicious drone flies over Vessel 1 and performs GPS spoofing attacks to change its travel course to collided with Vessel 2.

The attack demonstrated the ability of attackers to use cyber–physical systems as an entry point to the larger network. While the classical security measure on the standard computer network can detect a malware attack, cyber–physical systems devices have minimal security controls, making them easy to hack. Furthermore, in the modelled environment, the owners of the proposed system only monitored the cyber–physical system’s operational performance, meaning that the attack could go undetected for a long time.

In the GPS spoofing attack, the GPS simulator was easily used to replicate the signals as they would appear at a chosen location, misleading the receiver to calculate an incorrect position, velocity and time. This was due to the lack of any sensor/blocker to detect characteristics of interference, jamming, and spoofing signals. Such sensor/blocker can provide the needed local signs of an attack

⁶ <ftp://cddis.gsfc.nasa.gov/gnss/data/daily>

⁷ <https://github.com/pothosware/PothosCore/wiki/Downloads-windows-installer>

or malicious activity. In addition, some sensors/blockers can send alerts to a remote control/monitoring site and analyse log data for forensic purposes. While new GPS signals are more robust to jamming, it is essential to extend data spoofing whitelists to sensors to increase the system resilience in the presence of any form of interference.

The resilience of the studied system could be significantly increased through implementing simple mechanisms for auditing data and remote access rights. This can be achieved through adopting the simple principles of zero-trust security, e.g., micro-segmentation, to isolate the main computer network from the distributed sensor devices. Furthermore, regular vulnerability assessments should be performed on cyber-physical systems to patch vulnerabilities. To implement security in such highly distributed system, automated security testing processes can be key to improving cyber-resilience. Finally, at the operational level, resilience can be increased by proactively ensuring the safety of the system by tracking state awareness and physical system control.

7. Open challenges, issues and future directions

It is clear that each device or node in IoT/CPS creates its unique security issues and concerns. There is a danger in trying to force the use of the same tools that have worked before just because a device is considered connected to the Internet. This problem is further complicated when a researcher realises that IoT/CPS as a definition also extends into IoT in control systems and other connected areas.

It is also clear from the research undertaken that there are many different tools and techniques for detecting and analysing system vulnerabilities currently available. However, few tools and approaches have been built specifically for the IoT/CPS arsenal. In addition, some low-level or legacy devices (especially control systems) may have differing or bespoke protocol layers that may not respond as expected to the networking mapping techniques utilised by these products. Also, Modelling and analysing CPS requires access to spatial and temporal data properties related with cyber observables (e.g., incidents) and their impact on resilience.

The process of acquiring, measuring, and visualising this data is neither extensively specified in existing simulation standards nor adequately transformed to cyber standards. The way that target assets are characterised could also preserve certain challenges in a simulation environment. These challenges include but not limited to issues around translating security requirements, threat related information and impact metrics in M&S methods. Finally, more work is needed on the way that adversarial capabilities and objectives are standardised for use in simulations.

Due to the variety mentioned above of devices that could be considered IoT, it is challenging to develop an all-encompassing valuable toolbox in all scenarios. There are many vulnerabilities, and any device could be at risk from multiple concerns. Indeed, many of the vulnerabilities are combinations of other identified concerns, and this combination of minor weaknesses often creates new and unique problems in IoT devices. The work completed in this early stage of the project makes it apparent that many existing open-source tools are explicitly tailored to look at web interface vulnerabilities. In addition, many commercially available IoT devices utilise a web-based front end for setup and diagnostics services and are often vulnerable in the same way a standard website could be. However, issues considered solved on the broader Internet space may reoccur in the new IoT domain due to a smaller footprint or difficulty maintaining library updates.

A further research topic could concern the usefulness of the existing CVSS standard. Much work and discussion have already taken place in this area. As mentioned previously, what may be a critical issue on one device may be a concern on another. Vulnerability scoring is not an exact science, and individuals provide the metrics that make up an overall score with different biases and expertise. It is also possible that specific industrial devices require additional metrics to be considered, altering the overall score.

8. Conclusion

In this paper, we aim to influence strategic cyber decision-making in enhancing resilience within the IoT/CPS CNI by leveraging modelling and simulation tools with DT. A critical and comprehensive review of the Cyber Modelling and Simulation Standards (M&S) for cyber attack analysis is studied in this paper, furthermore, a list of recommendations is provided on their respective impact in assessing security testing scenarios in IoT simulated environments that leverage a Digital Twin (DT). Meanwhile, a thorough gap analysis in existing literature by clustering research is addressed in the areas of DT for security analysis and incident handling for physical-to-virtual security testing scenarios, and AI-enabled threat source identification, characterisation and resilience techniques.

A proof-of-concept of holistic cyber resilience testing using DT at the port of Southampton was presented that integrates cyber standards and security descriptors with emerging modelling techniques to represent the impact of cyber attacks and resilience efforts effectively. More specifically, the Port of Southampton has been selected to study the DT for cyber resilience. We analysed the operational scenarios and technical scenarios of the DT testbed. For the security analysis, six catalogues of security metrics were implemented in the DT modelling. Specifically, two attack scenarios of the Port CPS were presented to address the system resilience under cyber-attacks: The propagation of ransomware leading to a total shutdown of port operations and GNSS Spoofing attack leading to a collision of port operations. The results show that the DT could increase the resiliency of the CPS based on the attacks demonstrated against the resilience metrics. Finally, in this paper, we offered an established DT test platform of cyber effects modelling for potential collaborators across academia, industry, regulators, specialist agencies, and international organisations.

Data availability

Data will be made available on request.

Acknowledgements

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1. The authors would like to also thank Blueskytec and Schneider Electric for their invaluable support as part of this work.

References

- [1] G. Ahmadi-Assalemi, H. Al-Khateeb, C. Maple, G. Epiphaniou, Z.A. Alhaboby, S. Alkaabi, D. Alhaboby, Digital twins for precision healthcare, in: H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, J. Ibarra (Eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer International Publishing, Cham, 2020, pp. 133–158, http://dx.doi.org/10.1007/978-3-030-35746-7_8.
- [2] K. Bernsmed, D.S. Cruzes, M.G. Jaatun, M. Iovan, Adopting threat modelling in agile software development projects, *J. Syst. Softw.* 183 (2022) 111090.
- [3] J.H. Castellanos, M. Ochoa, J. Zhou, Finding dependencies between cyber-physical domains for security testing of industrial control systems, in: *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018, pp. 582–594.
- [4] R.M. Czekster, C. Morisset, J.A. Clark, S. Soudjani, C. Patsios, P. Davison, Systematic review of features for co-simulating security incidents in cyber-physical systems, *Secur. Priv.* 4 (3) (2021) e150.
- [5] Y. Fu, Z. O'Neill, Z. Yang, V. Adetola, J. Wen, L. Ren, T. Wagner, Q. Zhu, T. Wu, Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings, *Appl. Energy* 303 (2021) 117639, <http://dx.doi.org/10.1016/j.apenergy.2021.117639>, URL <https://www.sciencedirect.com/science/article/pii/S0306261921010060>.
- [6] A.A. Stüzen, A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem, *Int. J. Comput. Netw. Inf. Secur.* 12 (1) (2020).
- [7] M. Eckhart, A. Ekelhart, Digital twins for cyber-physical systems security: State of the art and outlook, in: S. Biffi, M. Eckhart, A. Lüder, E. Weippl (Eds.), *Security and Quality in Cyber-Physical Systems Engineering: With Forewords By Robert M. Lee and Tom Gilb*, Springer International Publishing, Cham, 2019, pp. 383–412, http://dx.doi.org/10.1007/978-3-030-25312-7_14.
- [8] M. Grieves, Digital twin: manufacturing excellence through virtual factory replication, Vol. 1, White Paper, Florida Institute of Technology, 2014, pp. 1–7.
- [9] L. Wan, T. Nochta, J. Schooling, Developing a city-level digital twin—propositions and a case study, in: *International Conference on Smart Infrastructure and Construction 2019 (ICSIC) Driving Data-Informed Decision-Making*, ICE Publishing, 2019, pp. 187–194.
- [10] W. Kritzinger, M. Karner, G. Traar, J. Henjes, W. Sihn, Digital twin in manufacturing: A categorical literature review and classification, *IFAC-PapersOnLine* 51 (11) (2018) 1016–1022.
- [11] E. Negri, L. Fumagalli, M. Macchi, A review of the roles of digital twin in CPS-based production systems, *Procedia Manuf.* 11 (2017) 939–948.
- [12] A. Becue, Y. Fourastier, I. Praça, A. Savarit, C. Baron, B. Gradusosfs, E. Pouille, C. Thomas, CyberFactory# 1—Securing the industry 4.0 with cyber-ranges and digital twins, in: *2018 14th IEEE International Workshop on Factory Communication Systems, WFCS, IEEE*, 2018, pp. 1–4.
- [13] M. Eckhart, A. Ekelhart, A specification-based state replication approach for digital twins, in: *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy*, 2018, pp. 36–47.
- [14] R. Mitchell, I.-R. Chen, A survey of intrusion detection techniques for cyber-physical systems, *ACM Comput. Surv.* 46 (4) (2014) 1–29.
- [15] V. Damjanovic-Behrendt, A digital twin-based privacy enhancement mechanism for the automotive industry, in: *2018 International Conference on Intelligent Systems, IS, IEEE*, 2018, pp. 272–279.
- [16] J. Lee, M. Azamfar, J. Singh, S. Siahpour, Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing, *IET Collab. Intell. Manuf.* 2 (1) (2020) 34–36.
- [17] R. Banks, J. Jones, N. Hazzazi, P. Garcia, R. Zimmermann, Extending a hybrid security risk assessment model with CWSS, in: *ITNG 2021 18th International Conference on Information Technology-New Generations*, Springer, 2021, pp. 137–143.
- [18] C. Mitre, Common attack pattern enumeration and classification, 2013, CAPEC.
- [19] V.E. Urias, W.M. Stout, B. Van Leeuwen, H. Lin, Cyber range infrastructure limitations and needs of tomorrow: A position paper, in: *2018 International Carnahan Conference on Security Technology, ICCST, IEEE*, 2018, pp. 1–5.
- [20] B. Möller, A. Dubois, P. Leydour, R. Verhage, Rpr fom 2.0: A federation object model for defense simulations, in: *2014 Fall Simulation Interoperability Workshop, Paper 14F-SIW-039*, Orlando, FL, 2014.
- [21] R. Danyliw, J. Meijer, Y. Demchenko, et al., The incident object description exchange format, *IETF Req. Comments* 5070 (2007).
- [22] M. Pradhan, C. Fuchs, F.T. Johnsen, A survey of applicability of military data model architectures for smart city data consumption and integration, in: *2018 IEEE 4th World Forum on Internet of Things, WF-IoT, IEEE*, 2018, pp. 129–134.
- [23] C. DoD, SUBJECT: Ports, Protocols, and Services Management (PPSM) References: See Enclosure, Tech. Rep., Department of Defense, 2014.
- [24] F. Björck, M. Henkel, J. Stirna, J. Zdravkovic, Cyber resilience—fundamentals for a definition, in: *New Contributions in Information Systems and Technologies*, Springer, 2015, pp. 311–316.
- [25] I. Linkov, D.A. Eisenberg, M.E. Bates, D. Chang, M. Convertino, J.H. Allen, S.E. Flynn, T.P. Seager, Measurable Resilience for Actionable Policy, ACS Publications, 2013.
- [26] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen, A. Kott, Resilience metrics for cyber systems, *Environ. Syst. Decis.* 33 (4) (2013) 471–476.
- [27] D.-J. Bodeau, R. Graubart, J. Picciotto, R. McQuaid, Cyber Resiliency Engineering Framework, Tech. Rep., MITRE CORP BEDFORD MA, 2011.
- [28] M.P. Barrett, Framework for Improving Critical Infrastructure Cybersecurity, Tech. Rep., National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.
- [29] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ICS) security, Vol. 800, NIST Special Publication, 2007, p. 82.
- [30] Z.A. Collier, M. Panwar, A.A. Ganin, A. Kott, I. Linkov, Security metrics in industrial control systems, in: *Cyber-Security of SCADA and Other Industrial Control Systems*, Springer, 2016, pp. 167–185.
- [31] S. Bologna, A. Fasani, M. Martellini, Cyber security and resilience of industrial control systems and critical infrastructures, in: *Cyber Security*, Springer, 2013, pp. 57–72.
- [32] S.Z. Yong, M.Q. Foo, E. Frazzoli, Robust and resilient estimation for cyber-physical systems under adversarial attacks, in: *2016 American Control Conference, ACC, IEEE*, 2016, pp. 308–315.
- [33] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, J. Sztipanovits, SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber-physical systems, *Proc. IEEE* 106 (1) (2017) 93–112.
- [34] T. Macaulay, B.L. Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*, CRC Press, 2011.
- [35] M.-V. Florin, I. Linkov, IRGC Resource Guide on Resilience, Tech. Rep., EPFL International Risk Governance Center (IRGC), 2016.
- [36] A. Kelic, Z.A. Collier, C. Brown, W.E. Beyeler, A.V. Outkin, V.N. Vargas, M.A. Ehlen, C. Judson, A. Zaidi, B. Leung, et al., Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks, *Environ. Syst. Decis.* 33 (4) (2013) 544–560.
- [37] I. Linkov, C. Fox-Lent, L. Read, C.R. Allen, J.C. Arnott, E. Bellini, J. Coaffee, M.-V. Florin, K. Hatfield, I. Hyde, et al., Tiered approach to resilience assessment, *Risk Anal.* 38 (9) (2018) 1772–1780.

- [38] Y.Z. Lun, A. D’Innocenzo, I. Malavolta, M.D. Di Benedetto, Cyber-physical systems security: a systematic mapping study, 2016, arXiv preprint arXiv: 1605.09641.
- [39] W. Danilczyk, Y. Sun, H. He, Angel: An intelligent digital twin framework for microgrid security, in: 2019 North American Power Symposium, NAPS, IEEE, 2019, pp. 1–6.
- [40] A. Saad, S. Faddel, T. Youssef, O.A. Mohammed, On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks, *IEEE Trans. Smart Grid* 11 (6) (2020) 5138–5150.
- [41] K.T. Park, Y.H. Son, S.W. Ko, S.D. Noh, Digital twin and reinforcement learning-based resilient production control for micro smart factory, *Appl. Sci.* 11 (7) (2021) 2977.
- [42] Q. Zhu, Z. Xu, Secure estimation of CPS with a digital twin, in: *Cross-Layer Design for Secure and Resilient Cyber-Physical Systems*, Springer, 2020, pp. 115–138.
- [43] A. Becue, E. Maia, L. Feeken, P. Borchers, I. Praca, A new concept of digital twin supporting optimization and resilience of factories of the future, *Appl. Sci.* 10 (13) (2020) 4482.
- [44] J. Zhang, L. Li, G. Lin, D. Fang, Y. Tai, J. Huang, Cyber resilience in healthcare digital twin on lung cancer, *IEEE Access* 8 (2020) 201900–201913.
- [45] K.T. Park, Y.H. Son, S.D. Noh, The architectural framework of a cyber physical logistics system for digital-twin-based supply chain control, *Int. J. Prod. Res.* 59 (19) (2021) 5721–5742.
- [46] S.P. Ramu, P. Boopalan, Q.-V. Pham, P.K.R. Maddikunta, T. Huynh-The, M. Alazab, T.T. Nguyen, T.R. Gadekallu, Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions, *Sustainable Cities Soc.* 79 (2022) 103663, <http://dx.doi.org/10.1016/j.scs.2021.103663>, URL <https://www.sciencedirect.com/science/article/pii/S2210670721009264>.
- [47] A. Drougkas, A. Sarri, P. Kyranoudi, A. Zisi, Port cybersecurity. Good practices for cybersecurity in the maritime sector, *ENSISA* 10 (2019) 328515.