Digital Twins and Cyber Security – solution or challenge?

David Holmes
Cyber Security CRC
and Edith Cowan University
Perth, Australia 6027
djholmes@our.ecu.edu.au

Maria Papathanasaki
Department of CS
and Telecommunications
University of Thessaly, Lamia, Greece
mpapathanasaki@uth.gr

Leandros Maglaras
Cyber Technology Institute
De Montfort University
Leicester, UK
leandros.maglaras@dmu.ac.uk

Mohamed Amine Ferrag
Department of Computer Science
Guelma University,
Guelma, Algeria
ferrag.mohamedamine@univ-guelma.dz

Surya Nepal
CSIRO's Data61
and Cyber Security CRC
Sydney, Australia 2122
surya.nepal@data61.csiro.au

Helge Janicke
Cyber Security CRC
and Edith Cowan University
Perth, Australia 6027
helge.janicke@cybersecuritycrc.org.au

***Abstract*—Digital twin technology today is diverse and emerging and its full potential is not yet widely understood. The concept of a digital twin allows for the analysis, design, optimisation and evolution of systems to take place fully digital, or in conjunction with a cyber-physical system to improve speed, accuracy and efficiency when compared to traditional engineering approaches. Digital twins continue to be a technology that enables new paradigms, such as Industry 4.0 and Factories of the Future as well as generating improved efficiencies within existing systems. The development of digital twin technology in traditional industries such as manufacturing, construction, the automotive industry, agriculture and transportation has highlighted its potential, but often insufficiently explored the risks associated with their integration. In this paper we explore risks relating to the cyber-security of systems employing digital twin technology and also consider the opportunities for digital twins themselves to mitigate cyber-security risks and become an integral part of a security in-depth defence.**

1. Introduction

A Digital Twin (DT) is an evolving technology that continues to attract attention from both the academic and the smart industry communities. The potential for significant increases in business efficiency and hence profitability, make DT technology an attractive proposition for incorporation into the current industry ecosystem. However, the continuing convergence of the Industry 4.0 sectors and DT technology does raise new cybersecurity challenges and opportunities to address existing shortcomings which this paper explores.

Attacks on Cyber Physical Systems (CPS) are increasing in prominence and are a particular concern for nations' critical infrastructures. Recent examples include the BlackEnergy malware attack in 2015 on a Ukrainian utility provider; a HatMan malware attack directed toward a Schneider Electrics Safety Instrument Systems in 2017; [1] cyber attacks on three U.S. natural gas pipeline companies in 2018, and most recently [2] a Darkside Ransomware as a Service (RaaS) attack on the Colonial Pipeline in the U.S, resulting in a ransom-payment of $4.4 million. This trend toward industry focused cyber attacks continues to be driven by both lucrative financial returns and by a pervasive inadequacy in their cyber security posture. Digital Twins and Cyber Digital Twins, which focus on cyber security aspects, provide significant opportunities to improve the cyber security of critical infrastructure if applied considerately.

Given the evolving nature of DT technology, there is a diverse spectrum of definitions. Broadly stated, a DT is a digitally defined model that mirrors a unique physical object, process, service, organisation, biologic or other abstraction. Data from multiple digital twins can be federated for a synthesised depiction across a number of worldly entities, such as a manufacturing plant, smart building, utility system and their respective sub processes. Gartner [3] takes a broader view and defines a DT as a 'digital representation of a real-world entity or system'. Grieves [4] is credited for coining the term to describe a digital informational construct based upon a physical system but created as an separate entity, where the digital construct should ideally be endowed with all informational assets as those found on the physical entity. In contrast, Kritzinger et al. [5] describe a DT as a concept that is capable of being further sub-divided into variants based upon their integration status, the particular area of focus and the technology employed. These several instances include: *Digital Twin* The level of interaction between the physical and digital entities is automated, bi directional and in real-time. *Digital Shadow* The level of integration between the physical and digital entities is automated, mono directional only and in real-time. *Digital Model* The level of integration between the physical and digital entities is manual only, and a change of state on the physical entity is not able to be reflected in the digital model without manual intervention.

In contrast, Shao et.al. [6] identify DT definitions based on their respective application areas and standards: *DIN SPEC, the Asset Administration Shell (AAS)* [7]. The stated purpose of this specification is the facilitation for effective implementation of DTs in the context of Industry 4.0. The interaction between digital factory assets, manufacturing instances, production and engineering systems. *ISO 23247, DT Framework for Manufacturing* [8]. Relevant in the context of the DT within the Industry 4.0 environment, this standard defines the implementation of models and communication between DTs. *IEEE P2806, System Architecture of Digital representation for Physical Objects in Factory Environments* [9]. This standard describes the framework upon which the creation of a digital factory is possible. The standard describes build objectives, deliverables, data standards and manufacturing procedures within the context of Industry 4.0.

Not only the level of integration between the physical and DT varies, also the fidelity and accuracy of the DT to represent its physical counterpart must be considered. DT technology covers a whole spectrum ranging from approximate models to exact emulation of their physical counterpart. Understanding the difference between simulation, emulation, and DT is important to avoid misunderstandings. The IEEE 1516 high level architecture specification [10] specifies the 'standard for the modelling and simulation of distributed, heterogeneous processes'. Within this context, the U.S. National Institute of Standards and Technology (NIST) defines a DT as a digital simulator of a IEEE 1451 standard tethered network smart sensor where the DT emulates desired, non-linear behaviors and failure conditions [11] to simulate a remote hardware sensor.

Simulation models are not the same as digital twins. Between simulation and emulation there is a spectrum ranging from 'gross approximation' at one extreme to 'detailed accuracy' at the other [12]. Simulation tools provide an environment designed to 'approximate' the real world, whereas emulation tools must ensure real-time functional accuracy by replicating the real world environment with such fidelity that scientific observations are unable to distinguish the model from the real world. While a digital twin can indeed be an emulation model, it does not necessarily follow that a emulation model must be a digital twin [13]. Prock et al. [12] observe that simulation tools have traditionally occupied the 'approximation' Discrete Event Simulation end of the spectrum, while emulation tools have tended to occupy the more accurate '3D physics engine' model environment.

As these technologies are at the core of a substantial paradigm shift in system engineering, cyber security concerns should be addressed in the design and integration of DTs to avoid future failures and support a successful technology transition. As digital twins are integrated with existing cyber physical systems the potential for cyber security attacks through this new digital artifact is clear. In particular when Digital Twins and Digital Shadows are implemented. Similarly, the DT technology itself can be used to analyse the cyber physical system it represents, generating significant opportunities to use the DT to understand and mitigate cyber security risks present in the system it models.

This paper represents a step towards understanding the impact and potential of digital twins through a lens of cyber security. In the following we will review existing digital twins and their adoption in Section 2. The paper then reviews and analyses some of the cyber security challenges that are created by the use of DT technology in Section 3 before identifying cyber security challenges that can be addressed by the use of DT technology in Section 4. We conclude the paper with a review of related work and outline future research.

2. Digital Twin solutions and adoptions

The technological lineage of DTs can be traced back to the 'mirrored systems' developed by NASA for the ill-fated 1970 Apollo 13 space project [14], the digital twin has truly come of age in the last decade. In the early 1970's it was through the use of the simulated physical environment that NASA engineers were able to successfully model and analyse potential rescue solutions.

Recent advances with the use of DTs in the life sciences, may well permit the expansion of the virtual model to include that of the biological organism. One example of this is Digitalpredict [15]. Here developments in the field of medical innovation serve to illustrate new 'at the edge' DT technology to research the long term affects of the COVID virus.

Continuing advances in Artificial Intelligence (AI), serve to ensure that the cost benefit return from the business perspective, continues to ensure acceptance and traction of DT within the modern Industry 4.0 ecosystem. DTs are constantly optimised, and they are becoming more and more integrated into the automated manufacturing sector [16], [17].

It is widely accepted (e.g. [18], [19]) that DTs are one of the enabling technologies for Industry 4.0, a strategic industrial initiative [20] designed to promote the path to intelligent factories of the future based upon manufacturing processes founded upon the technologies of cloud computing, the Internet of Things (IoT) and Cyber-Physical Systems (CPSs). Within the Industry 4.0 domain, the use of DT technology to monitor a physical resource in real time, underpins an environment built upon intelligent technology to produce agile, smart, and 'on the fly' configurable industrial manufacturing processes. Readily adopted and deployed, advances in Industry 4.0 smart technology continue to drive manufacturing and industrial innovation into the future through technology platforms that enable convergence, collaboration, communication, efficiency and flexibility on a commercial level.

Another role of DTs is predicting any future failure of the physical twin [21] and thus are playing a significant role in predictive maintenance, failure analysis and recovery. Applied to system evolution a DT can be used for testing every innovation we would like to import in their physical twins and predict their behavior before the change takes place in the physical realm. This is possible through the link between the twins, which allows them to be in a

synchronous connection [22]. This raises concerns from a cyber-security point of view where this linkage to a live, operational system is problematic as any malicious update to the digital twin may directly affect the existing physical system. This is especially true in the case of predictive maintenance where if some anomaly or failure is predicted in the DT, then some tasks can be altered in the real system. Digital Twins not only simulate their physical ones, but they also uninterruptedly exchange data with them in real time, keeping them updated.

The current implementation of the Industry 4.0 framework is extensive. Deployment of manufacturing and industrial enterprise continues within all of the physical domains and with this, the associated deployment of digital twin technology where the major benefits can be defined as predictive maintenance, design and planning, and optimisation and digital prototyping. Readily adopted into manufacturing, equipment operators have come to expect increased plant reliability, the result of predictive plant maintenance schedules, improved up-time, improved productivity, and improved plant performance reflected in the business bottom-line. Digital twin generated data analysis is also able to generate a positive influence on business policy and planning decisions where business decisions are made more quickly and effectively based upon relevant information available in both a timely and accurate manner.

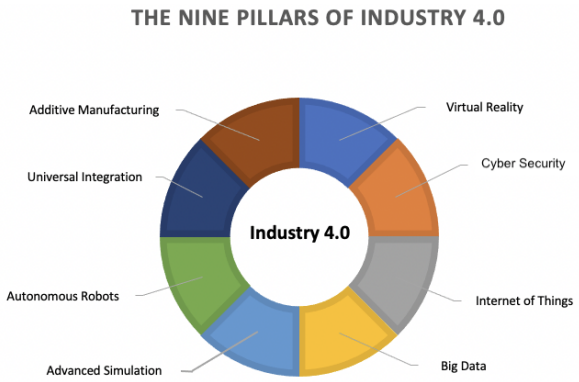

Figure 1. The Pillars of Industry 4.0

Emulation technology can also be leveraged in order to integrate with digital twin capabilities to deliver practical efficiencies to the business. Specifically, rather than the DT simply reflecting the output from sensors of the physical twin, the adoption of emulation technology presents the opportunity to leverage physics based predictive models to improve plant maintenance and run robust test solutions permitting the ability to making informed real-time business decisions.

3. Cyber Security Challenges created by DT

Widespread use of DTs raises cybersecurity concerns. The integration of DT technology into the Industry 4.0 domain should mandate 'best practice' cyber security compliance. As one of its support pillars (Fig 1), cybersecurity should be a foremost consideration in its implementation. Improved efficiencies in production, brought about by DT technology, may lead to commercial pressures to expedite a new product to market and may encourage flawed decision making. This may lead to cybersecurity best practice being overlooked in favour of a faster financial return.

In this context the concept a cyber digital twin (CDT) finds cyber defence relevance [23]. A CDT is the application of DT technology to allow for security analysis and monitoring which may not be directly feasible on the physical counterpart without causing disruption. Such CDT provides significant benefits to security professionals enabling them to perform security assessments without accessing the physical environment, and the ability to simulate security attacks and defence scenarios that would otherwise be impossible to do in the physical environment.

These benefits do not come without cost as there are some significant cybersecurity risks associated with the implementation of CDT technology. These risks need to be identified and assessed by both CDT users, i.e., security professionals and the CDT designers/developers before deployment. The following reviews some of these challenges and risks created by the use of DT technology and in particular the use of CDTs.

Availability. Financial constraints may restrict the availability of DTs and CDTs in the SME supply chain [24]. DT technology can be financially demanding, especially for SMEs seeking to remain competitive in an increasingly DT centric industrial environment.

Generally, DT technology aims to enhance the maintainability and longevity of its physical counterpart and thus supports availability over its lifetime. Implementation constraints, especially in tightly integrated DTs as opposed ot digital models, may however result in undesirable interactions that can affect the availability of the overall system. As an example if the DT is compromised by a cyber-attack, the effect on the physical twin may be catastrophic. Thus a DT can create an additional failure point in the system that can be exploited by cyber-attack.

Integrity. Unauthorised modification or destruction of data/operations while being processed, in transit or in storage must be prevented. The integrity of the system itself must be maintained to preserve confidence in the reliability and safety of the system operation. Preserving the system integrity is also essential to ensure non-repudiation and authenticity of commands/actions the system which are essential in its secure operation and also support incident response capabilities. This requires secure communication between the DT and its physical counterpart, challenging current technology deployments especially in real-time deployments.

An adversary affecting a digital twin or its physical representation can introduce divergence in the behaviour or state. Given the bi-directional link between the two

an attacker may negatively affect both through changes in either. However, this also presents an opportunity to identify malicious changes as discussed in section 4 if implemented with cybersecurity in mind. The challenge here is if the DT is used to drive system evolution and maintenance, it can result in malicious changes made to the DT being propagated to its physical counterpart. Similar concerns are present when implementing a digital shadow, and digital models, albeit in more restricted form due to their reduced integration.

Another factor is the accuracy of the twin in relation to its physical twin. For example if a digital model is affected by a cyberattack, any predictions are likely to be of restricted value, depending on data relevancy, interpretability, availability, and resulting data quality.

Whilst DT technology overall has a strong potential to improve integrity of the physical system by generating improved observation and ability to test and verify its operation, it can also be used to mislead operators and corrupt the system if compromised by an adversary and thus requires similar protections.

In the case of a cyber digital twin, the CDT helps security operators to discover security vulnerabilities in the real system by performing simulated activities against potential threats. The lessons learned from the CDT can then be applied to the real system. Furthermore, security operators often use the CDT to test different configurations of the systems before applying them to the real system.

If there is divergence between the security configurations of the CDT and the real system, these lessons learned would no longer be accurate and applying such lessons to the real system gives only a false sense of security. Hence, it is important to ensure that the CDT manifest the same security features as that of the real system to avoid flawed security decisions. This divergence is in particular likely when a Digital Model implementation is considered for a CDT implementation. On the other hand the reduced integration of Digital Model provides the ability to explore and test configurations without impact on the operational system.

Considering these challenges, an effective deployment of digital twin technology may be multifaceted, with a digital twin being deployed for system evolution, a separate digital shadow for monitoring system integrity and predictive maintenance and a digital model as a cyber digital twin. This in turn raises the question as to how to maintain integrity and avoid divergence of these multiple DT technologies and as to the amount of replication providing a larger attack surface that challenges the confidentiality of the system.

Confidentiality. Ensuring authorised access constraints to system facilities and data is paramount in protecting the confidentiality of business and personal information. With the rapidly emerging technological advances in the area of DT technology, constant vigilance is necessary in order to prevent system vulnerability creep and inadvertently exposing the system to unanticipated or unforeseen vulnerabilities.

For example, DT technology can make it easier for an adversary to learn trade-secrets. While confidentiality concerns are not created by the use of DT, they aggravate some of the concerns. For example, an existing OT installation operating a production line of a drug manufacturer already carries detailed information about the manufacturing processes that is essential for the organisation to maintain and can be used to deduct trade-secrets and IP from its operation. Such a system can be interrogated by a successful adversary, but requires significant expertise and stealth. Should an adversary obtain a copy or access to a digital twin, this information is readily available and can be interrogated at the adversaries leisure without the ability of the organisation to detect or prevent their actions. This applies equally for Digital Twin, Shadows and Models.

When we consider the use of a cyber digital twin, the CDT may contain the security configurations of all components of the ICT and/or OT infrastructure in the physical environment. Security configurations are private and should be protected from adversaries. If an adversary gains control of the security configurations, they can exploit known or zero-day vulnerabilities to launch an cyber attack or introduce an Advanced Persistent Threat (APT) to the system. Many security attacks in recent times have exploited security misconfiguration vulnerabilities that can occur due to default configurations or insecure configurations. These configurations leave the system susceptible to cyber attacks. They are often hidden within organisations and not easily detectable by attackers. In the case of the CDT, while creating the replica of the physical environment, the security configurations need to be moved across to the digital environment, with a resulting increase in the possibility that confidential information may become accessible to outside parties, some of which may be hostile.

The Cyber-Physical systems deploy a defence-in-depth security architecture to defend against potential cyber attacks by utilising a combination of different technologies and security operations. Such a security architecture works much like an onion with multiple layers of security, and inherently obscure many system assets from potential hackers. Hence, it naturally minimises the attack surfaces. However, all assets, whether they may be hardware or software, will be visible while implementing the CDT. Any attackers who gain access to the CDT have much more knowledge about the system than otherwise would be the case. Hence, the CDT increases the attack surfaces significantly.

Data ownership and IP leakage. The data required for input into the twin and the data contained in the twin will be valuable in both a practical and financial sense. A DT as a digital representation of the physical system will require similar treatment in terms of IP and export controls as the physical system itself. When DTs are used to provide a virtual model of a system integration prior to any physical components being integrated, the pace of technology transfer and potential IP leakage quickens. For example reengineering a physical device requires significant expertise and time during which the provider retains a competitive advantage over any malicious actor. With the use of DT as a model this time reduces as a DT can be much more readily

interrogated with the aim to replicate the physical device or to identify its security vulnerabilities.

To implement the CDT, one requires not only software and hardware components and their configurations, but also the interactions among those components. To address the challenges of interoperability between deferring components in the system, APIs have been used by both hardware and software components in modern systems, and these APIs are mostly standardised and use the "message" as a payload. The business logic is often encoded within the messages and interactions. It is possible to decode the business logic using reverse engineering if should the information become available. Further, such business logic is often the repository of commercial-in-confidence IP of the organisation and also of clients of the business. Subsequent release of any sensitive commercial or personal information may cause not only attract a financial penalty as commercial advantage is eroded but also as a result of contravention of legal statute such as the EU General Data Protection Regulation (GDPR) that applies to all businesses, regardless of size, with an establishment in the EU.

There is a risk of theft of IP through the DT. Legal frameworks can protect the ownership of the DT and are frequently expressed in Service-Level Agreements (SLA). Hearn and Rix [25] suggest that any DT that is going to be shared, should be encrypted and protected from third parties, addressing concerns about supply-chain manipulation through man-in-the-middle attacks.

Clear delineation and scope of data ownership will need to be agreed upon in advance among the respective stakeholders, together with arrangements for access to the data by third parties during the life cycle of the DT. International law, national and state legal obligations will also each need to be addressed to avoid disputes of a legal nature.

However, similar issues of ownership and responsibility for cyber security assurance remain for DTs as they already exist for digital and OT supply chains. This means that software hardening through a robust patch and update strategy is critically important to the security of DT and connected systems with sometimes unclear responsibilities throughout a complex supply-chain likely to create opportunities for malicious actors in the early iterations of Industry 4.0 implementations.

Safety. The CDT is a double-edged sword from the cybersecurity perspective. By definition, the CDT is designed and built to simulate a variety of cybersecurity attack scenarios with the aim of testing the potential vulnerabilities in the corresponding real system. It means an attack on CDT is highly likely to be successful in the real system. This begs a question, what happens if an attacker has an access to the CDT? The attacker can identify any weaknesses in the physical entity, test the potential success of the attack, and launch the attack in the real system with a greater confidence of success. Therefore, it is important to carefully consider the security implications of CDT use while design and implementation of a CDT, especially where security impacts safety.

4. Cyber Security Challenges solved by DT

DT technology and in particular CDT can prevent cyber attacks by providing modelling/prediction capability or through increased visibility of the system behaviours of their physical counterpart.

Using DT for improved patch management. Today many owners of Operational Technology (OT) are challenged in their patch management. This is partly due to a lack of adequate asset management and inadequate system design consideration that would allow for the OT system to be regularly updated. The complex architectures allowing for fully integrated DTs resolve these issues, however at increased upfront costs to their development/deployment.

Another challenge for patching OT infrastructure is to understand the impact of applying a (security) patch or configuration change will have on the overall system, as frequently testing a single device in isolation is either expensive, time-consuming or simply does not cover system wide impacts. Using digital twins to simulate the OT system can overcome some of these challenges. Here the impact of applying a patch can be explored without impacting the deployed infrastructure and without the need to maintain an expensive secondary system solely for testing purposes. This is a major advantage, especially when considering safety-critical applications.

Advanced system and security testing opportunities. Systems using operational technology mainly rely on system tests to assert that their overall function is correct and in some cases penetration tests to provide confidence in the installation. Digital Twins that are used in the design of the operational technology as envisioned in Industry 4.0 can enable continuous validation of security and other properties traditionally only tested in late development stages. This allows for more efficient automation of security tests as part of a more rigorous regression testing regime in the development life-cycle of the OT deployment, providing additional assurance to integrators and stakeholders alike.

CDTs in particular benefit operations management here. Cyber security risks are dynamic and fast evolving based on a wide variety of factors such as vulnerability discovery, exploit availability, and cyber threat intelligence. This means that significant cyber threats may emerge within very short time-frames that necessitate immediate response. Anthi et al. [26] suggest that DT and CDT technology allow organisations to undertake detailed assessments of potential of system vulnerabilities in anticipation of attacks on critical components of the system and also investigate and evaluate potential attack vectors.

Being able to swiftly understand and test the impact of configuration changes to the security components of the system to counteract any threats is probably the main advantage of deploying a CDT improving response and risk management.

Improved risk management. evaluation through automated analysis of a new system component using a DT thereby

reducing any potential threat to human safety, or that of the facility or environment. [27]. In addition, leveraging the big-data analysis capabilities of DT technology, automated analysis of CDT logs and reports, and points of failure are quickly identified enabling a rapid mitigation response.

Active Cyber Defence. Whether OT systems become incidental collateral damage in a wider cyber attack campaign or are the target of an more sophisticated attack, it is paramount for incident responders to understand the impact of any compromise to the system operation and its cyber safety. Pokhrel et.al. [28] review work in the area of incident prediction aimed at enabling incident responders to be prepared and understand attack vectors. Particularly relevant in the context of those legacy industrial systems prevalent in the factory today, CDT technology can reduce attack vectors and aid incident preparation.

Advanced Training and Incident Response Capability. With reference to Fig 2. the use of a digital twin cyber-range environment to encourage and promote the cyber security practitioner skill development delivered through practical engagement and war games.

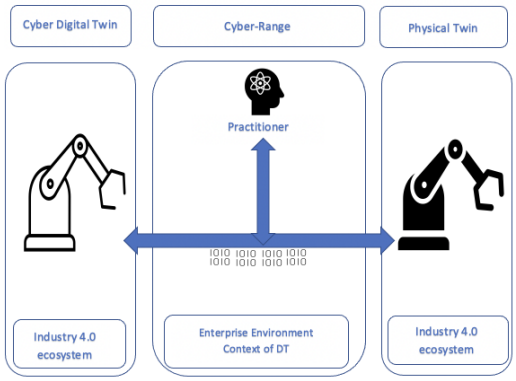

Figure 2. Semantic Modelling and the Cyber-Range

5. Related work

While Digital Twins continue to be regarded as one of the top technological trends, [27] with an increasing number of industries adopting this technology as the benefits of improved efficiencies to their systems and processes becomes manifest. However, much less is known or published on the issue of DT cybersecurity.

Anomaly Detection. Akbarian et.al. [1] explore practical aspects of using a detecting attacks on a DT in a timely manner. The detection system leverages the use of a Kalman filter [29] tuned to estimate the integrity of system input and output signals. The tuned Kalman generated system output is then compared with actual system output to identify output discrepancies that may indicate a system intrusion. Digital Twins and Digital Shadows may also significantly advance work on runtime verification [30], a specification based approach that bridges between dynamic testing and anomaly detection.

Virtual Commissioning. DTs have been described as industry efficiency enablers through the use of fault prediction, reconfiguration maintenance scheduling and virtual commissioning [31]. By leveraging the DTs physical emulation characteristics it is possible to significantly reduce the time to completion of the product commissioning stage while simultaneously reducing the likelihood of a costly prototype redesign. The data generated by the DT as the result of the commissioning process can be used to generate product operational KPIs, plan maintenance cycles, generate training data sets formulate operational anomaly detection and cybersecurity defence profiles.

Autonomy. Effective smart manufacturing is founded upon the ability to respond with agility to situational changes and developments. For this to occur in an efficient and timely manner, autonomous systems, Rosen et.al. [32] suggest that autonomous systems must have the freedom of action to deliver an effective response, unconstrained by a precondition for human intercedence. The application of system autonomy should therefore provide a operational environment capable of responding immediately to system anomalies, errors, faults and importantly, attempted cybersecurity breaches.

Predictive Analytics. With current digital manufacturing trends continuing to gravitate toward the optimisation of product planning, prototyping, development and deployment within the digital domain design space. Zacharaki et.al. [33] suggest that advantages through the use of DT predictive technology deliver solid returns on investment.

6. Future Research

Digital twinning plays a key role in many IoT operations and processes including IoT application development, testing, analysis and control. The implementation of digital twins will also enable distributed remote control of industrial assets, which will place an increasingly heavy burden on IoT identity management, authentication, and authorisation.

To implement a DT, one has to know the details of firmware used in the physical devices. Most of the firmware comes in binary form and their source code is not available. The source code is often proprietary to the individual vendor and is considered core IP. The vendors are reluctant to make details of their firmware available for DT developers. There is a need to find a common standard approach that allows the protection of IP and trade-secrets especially when DTs are m modelling software/hardware hybrids.

DTs are not going to be perfect. Most DTs are going to be developed with a specific application in mind, such as CDT, that focus on specific aspects of the real system. Achieving realism requires high-fidelity DTs. High fidelity DT must represent the complete behaviours of each device,

including their timing and performance constraints. This is very difficult to achieve for a complex system, especially as the integration of system components and their interconnectivity must model and reflect those in the real system integration. One of the approaches taken by researchers [34] is to emulate the system so that the DT environment is connected with some physical devices. The behaviour of the digital device is then always calibrated in real-time dynamically against its physical twin. To achieve the full benefits of DTs further research is needed to make the implementation of complex systems through a DT approach feasible and economical.

DTs, in particular CDTs, as an emerging technology needs to be further examined from the lens of responsible innovation concerning its ethical impacts. DTs encompasses many emerging technologies such as AI, Quantum, Robotics, Internet of Things and Big Data; hence, we need to develop an ethical framework for DT considering socio-ethical features of different technologies and the digital artifacts they generate in the DT environment. A deeper understanding of how these digital artifacts are perceived by each stakeholder in the system is required, to identify economic and social impacts of such technology. Furthermore, these artifacts not only capture device behaviours, but also human behaviours and in some cases sensitive human information (in the case of DT for healthcare).

We consider the main challenge to be the creation of DTs without increasing the cybersecurity risks for the real system. The answer lies in the technologies that help to create the realism of the physical systems without revealing the security-sensitive components, data and interactions. Existing technologies in the areas of deception and privacy-enhancing techniques may provide a good starting point, but may not be sufficient to provide a solution to the issue.

The real challenge lies in the two-way transfer of information between the physical system and the DT. For example, existing technologies might be able to help to preserve the privacy of the components, data and interactions while building DT. However, one needs to ensure that the lessons learned from DT can be transferred back to the physical environment. The trade-off between protecting the system detail in the construction of the DT and beneficial outputs from the analysis of the DT to be applied to the system, is not well understood. For example, how do you transfer the security configurations learned in the perturbed digital environment to the physical environment? DT is a complex, multi-component, interactive environment and existing technologies in privacy preservation and deception do not consider such a complex environment.

Recent exploratory research into blockchain technology with its inherently secure transactional paradigm has long been used successfully for secure financial transactions in the area of cryptocurrency, and more recently has found traction in Business to Business (B2B) supply chain systems. The benefits of Blockchain technology include encrypted, transparent, private, trustless, peer to peer transactions that produce immutable digital records, show potential for application of the DT and CDT related IoT, IIoT and ICS architectures. IOTA [35] explores a proof of concept initiative for M2M interaction.The initiative is to create a digitalised industrial supply chain ecosystem where there is a DT for every product manufactured. Within such an environment, stakeholders would be able to interact in a secure trustless enabled supply chain built upon blockchain technology.

7. Conclusion

Digital twins, as an emerging and disruptive technology, are a digital environment where physical devices, software, firmware and the interactions between them are accurately replicated in digital form. DTs play a significantrole in securing future systems deployed as part of nation's Industry 4.0 agenda and future digital supply-chains. This paper explored challenges and opportunities for cyber security of cyber-physical systems that are created or amplified by DT technology. Our contribution particularly focused on Cyber Digital Twins (CDT), DTs that are specifically designed and implemented for the purposes of cybersecurity defence. In this paper we reviewed and analysed challenges for CDT technology and the security challenges it presents in and of itself. On the one hand, CDT technology enables the cybersecurity professional to exploit tool automation and artificial intelligence to simulate and evaluate potential cyber attack scenarios to prepare and defend the physical infrastructure. On the other hand, a malicious actor can potentially leverage that same CDT technology with which to gain a greater understanding of the vulnerabilities of a physical system and from there, launch a cyber attack with a high likelihood of success. The increasingly complexity of the CDT operational environment also presents challenges for those tasked with the protection of the cybersecurity of the operational environment.

In this position paper, we have explored both the benefits and risks of CDT technology and outlined some of the core future challenges that research and practitioners should address to ensure that the full benefits that are expected of DT technology can be achieved. We hope this paper will encourage discussion and reflection upon the benefits and challenges of implementing and securing CDT technology within the context of the Industry 4.0 paradigm.

Acknowledgments

The work has been partially supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

References

[1] F. Akbarian, E. Fitzgerald, and M. Kihl, "Intrusion Detection in Digital Twins for Industrial Control Systems," *2020 28th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2020*, 2020.

[2] "The Colonial Pipeline Ransomware Attack: Everything We Know | Votiro," Jun 2021, [Online; accessed 10. Jun. 2021]. [Online]. Available: https://votiro.com/blog/the-colonial-pipeline-ransomware-attack-everything-we-know

[3] "Definition of Digital Twin - Gartner Information Technology Glossary," Jun 2021, [Online; accessed 14. Jun. 2021]. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/digital-twin

[4] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," *Transdiscipl. Perspect. Complex Syst. New Find. Approaches*, no. August, pp. 85–113, 2016.

[5] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, "Digital Twin in manufacturing: A categorical literature review and classification," *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 1016–1022, 2018. [Online]. Available: https://doi.org/10.1016/j.ifacol.2018.08.474

[6] G. N. Shao, "Use Case Scenarios for Digital Twin Implementation Based on ISO 23247," 2021. [Online]. Available: https://doi.org/10.6028/NIST.AMS.400-2

[7] Plattform Industrie 4.0, "the Asset Administration Shell : Implementing Digital Twins for Use in Industrie 4 . 0 the Asset Administration Shell – a Starter Kit for Developers," pp. 1–2, 2019.

[8] "ISO/DIS 23247-1(en), Automation systems and integration — Digital Twin framework for manufacturing — Part 1: Overview and general principles," Jun 2021, [Online; accessed 18. Jun. 2021]. [Online]. Available: https://www.iso.org/obp/ui/iso:std:iso:23247:-1:dis:ed-1:v1:en

[9] "P2806 - System Architecture of Digital Representation for Physical Objects in Factory Environments," Jun 2021, [Online; accessed 18. Jun. 2021]. [Online]. Available: https://standards.ieee.org/project/2806.html

[10] Y. Song, M. J. Burns, A. Pandey, and T. P. Roth, "IEEE 1451 Smart Sensor Digital Twin Federation for IoT/CPS Research," *NIST*, May 2019. [Online]. Available: https://www.nist.gov/publications/ieee-1451-smart-sensor-digital-twin-federation-iotcps-research

[11] M. R. Moore, K. B. Lee, and S. M. F. Smith, "The Next Step- IEEE 1451 Smart Sensor Networks," *NIST*, vol. 18, no. No. 9, Feb 2017. [Online]. Available: https://www.nist.gov/publications/next-step-ieee-1451-smart-sensor-networks

[12] T. Sprock and L. F. McGinnis, "Proceedings of the 2014 Winter Simulation Conference A. Tolk, S." *Winter Simul. Conf.*, no. 1983, pp. 2600–2608, 2014.

[13] G. Shao, S. Jain, C. Laroque, L. H. Lee, P. Lendermann, and O. Rose, "Digital Twin for Smart Manufacturing: The Simulation Aspect," *Proc. - Winter Simul. Conf.*, vol. 2019-December, no. Bolton 2016, pp. 2085–2098, 2019.

[14] B. R. Barricelli, E. Casiraghi, and D. Fogli, "A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications," *IEEE Access*, 2019.

[15] "DIGIPREDICT Project," Mar 2021, [Online; accessed 6. Jun. 2021]. [Online]. Available: https://www.digipredict.eu

[16] C. Semeraro, M. Lezoche, H. Panetto, and M. Dassisti, "Digital twin paradigm: A systematic literature review," *Computers in Industry*, vol. 130, p. 103469, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361521000762

[17] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, "Characterising the digital twin: A systematic literature review," *CIRP Journal of Manufacturing Science and Technology*, vol. 29, pp. 36–52, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1755581720300110

[18] T. Y. Melesse, V. Di Pasquale, and S. Riemma, "Digital twin models in industrial operations: A systematic literature review," *Procedia Manufacturing*, vol. 42, no. 2019, pp. 267–272, 2020. [Online]. Available: https://doi.org/10.1016/j.promfg.2020.02.084

[19] L. Oscar, M. Rooker, B. Laibarra, R. Anton, N. Bojan, and A. Gonzalez, *The Digital Shop Floor in the Industry 4.0 Era*. River Publishers, 2019, pp. 34–35. [Online]. Available: https://www.riverpublishers.com/dissertations-xml/9788770220408/9788770220408.xml

[20] C.-C. Kuo, J. Z. Shyu, and K. Ding, "Industrial revitalization via industry 4.0 – A comparative policy analysis among China, Germany and the USA," *Glob. Transitions*, vol. 1, pp. 3–14, 2019. [Online]. Available: https://doi.org/10.1016/j.glt.2018.12.001

[21] A. El Saddik, "Digital twins: The convergence of multimedia technologies," *IEEE multimedia*, vol. 25, no. 2, pp. 87–92, 2018.

[22] R. Rosen, G. Von Wichert, G. Lo, and K. D. Bettenhausen, "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.

[23] M. Eckhart and A. Ekelhart, "Towards security-aware virtual environments for digital twins," in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, ser. CPSS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 61–72. [Online]. Available: https://doi.org/10.1145/3198458.3198464

[24] "Emerging Technology Guide: Digital Twin | Digital.NSW," Jun 2021, [Online; accessed 14. Jun. 2021]. [Online]. Available: https://www.digital.nsw.gov.au/transformation/policy-lab/emerging-technology-guide-digital-twin

[25] M. Hearn and S. Rix, "Cybersecurity considerations for digital twin implementations," *IIC J. Innov*, 2019.

[26] E. Anthi, L. Williams, P. Burnap, and K. Jones, "A three-tiered intrusion detection system for industrial control systems," *J. Cybersecurity*, vol. 7, no. 1, 2021.

[27] T. R. Wanasinghe, L. Wroblewski, B. K. Petersen, R. G. Gosine, L. A. James, O. De Silva, G. K. Mann, and P. J. Warrian, "Digital Twin for the Oil and Gas Industry: Overview, Research Trends, Opportunities, and Challenges," *IEEE Access*, vol. 8, pp. 104 175–104 197, 2020.

[28] A. Pokhrel, V. Katta, and R. Colomo-Palacios, "Digital twin for cybersecurity incident prediction: A multivocal literature review," in *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, ser. ICSEW'20. New York, NY, USA: Association for Computing Machinery, 2020, p. 671–678. [Online]. Available: https://doi.org/10.1145/3387940.3392199

[29] D. Simon, *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*, 01 2006.

[30] H. Janicke, A. Nicholson, S. Webber, and A. Cau, "Runtime-monitoring for industrial control systems," *Electronics*, vol. 4, no. 4, pp. 995–1017, 2015.

[31] B. Maschler, D. Braun, N. Jazdi, and M. Weyrich, "Transfer Learning as an Enabler of the Intelligent Digital Twin," no. November, 2020. [Online]. Available: http://arxiv.org/abs/2012.01913

[32] R. Rosen, G. Von Wichert, G. Lo, and K. D. Bettenhausen, "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 28, no. 3, pp. 567–572, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.ifacol.2015.06.141

[33] A. Zacharaki, T. Vafeiadis, N. Kolokas, A. Vaxevani, Y. Xu, M. Peschl, D. Ioannidis, and D. Tzovaras, "RECLAIM: Toward a New Era of Refurbishment and Remanufacturing of Industrial Equipment," *Front. Artif. Intell.*, vol. 3, no. February, pp. 1–12, 2021.

[34] Y. Song, M. Burns, A. Pandey, and T. Roth, "Ieee 1451 smart sensor digital twin federation for iot/cps research." 2019 IEEE Sensors Applications Symposium (SAS), Sophia Antipolis, -1, 2019-05-06 2019.

[35] "IOTA Ecosystem Project - Industrial IOTA Lab Aachen," Jun 2021, [Online; accessed 13. Jun. 2021]. [Online]. Available: https://ecosystem.iota.org/projects/industrial-iota-lab-aachen