European Cyber Security Organisation

ECSO Technical Paper on Cybersecurity scenarios and Digital Twins

May 2023 – v1.0

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please contact wg6_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

ECSO is not responsible for the third-party use of the content in this paper. By using/referring to the information in this paper, no relationship is created is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

Copyright Notice

Executive Summary

Digital Twins (DTs) can be conceptualized as a technology that improves processes, predicts failures, and spots abnormal situations. For these reasons, DTs are becoming pivotal players in the global digitalisation trend that is affecting our economy, industry and society. Capable of virtualizing and simulating physical world assets to empower innovative optimization actions in many of today's application domains, the adoption of DT devices brings resilience and cybersecurity benefits in various application scenarios. Through its offline and online simulation capabilities, DT devices provide attractive services, particularly: predictive maintenance, real-time monitoring, remote control, process optimization, security management, failure analysis and tracking, strategy evaluation, health monitoring, risk management, training, and cybersecurity.

In line with the above, this ECSO technical paper explores the definition of Digital Twin, its limitations and technical dependencies, presenting challenges that the technology is currently encountering, *in primis* in the area of cybersecurity.

First and foremost, this ECSO WG6 Paper analyses discusses four different use cases covering the applications of DTS, intended as cyber-physical synergy, across a broad variety of sectors, *inter alia*: business, education and skills, collaborative industries, industrial cybersecurity. Later, emphasis will be placed on the DT architectures and frameworks designed largely by academic organizations and entities.

In addition, to fully understand the relevance of DTs, two crucial aspects of the aforementioned technology are examined: on the one hand, the simulation capabilities of DTs as a resource for cybersecurity solutions, and on the other hand, the virtualization of DTs as a one-stop laboratory to develop, validate and test security approaches to lead mitigation and preventive actions.

Given the breadth of the attack surface that characterizes DTs, the second part of the research aims to bring to light a set of recommendations and best practice guidelines to be considered in the near future in order to configure and implement reliable and secure DTs. Specifically, the paper outlines security requirements, in line with the cybersecurity framework provided by National Institute of Standards and Technology (NIST), that both practitioners and IT/OT security experts should consider in order to avoid potential attack scenarios.

Finally, ECSO WG6 provides a set of recommendations to assist various stakeholders in governing the intricate and dynamic nature of DTs. Overall, it is safe to state that this ECSO technical paper outlines the current state of the technology and its demand from the perspective of research, industry and society.

Table of Contents

Acronyms

AAA	Authentication, Authorization and Accounting
ADSS	Airbus Defence and Space
AI	Artificial Intelligence
ANGEL	Automatic Network Guardian for ELectrical systems
API	Application Programming Interface
APT	Advanced Persistent Threat
BIM	Building Information Modeling
C2PS	Cloud-based Cyber-Physical Systems
CAM	Computer-Aided Manufacturing
CAS	Computer-Aided Design
CPPS	Cyber-Physical Production System
CPS	Cyber-Physical Systems
CVE	Common Vulnerabilities Exposures
DLT	Distributed Ledger Technology
DTaaS	Digital Twin as a Service
DTN	Digital Twin Network
GE	General Electric
HMI	Human Machine Interface
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IIC	Industry IoT Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Intellectual Property
IPC	Inter-Process Communication
IPR	Intellectual Property Right
IRTF	Internet Research Task Force
ISO	International Standard Organization
IT	Information Technology
KPI	Key Performance Indicator
MDT	Mobility Digital Twin
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Tecnology
OT	Operational Technology

P2P	Peer-to-Peer
PET	Privacy Enhancing Technologies
PLC	Programmable Logic Controller
SBL	Scenario-Based Learning
SDK	Software Development Kit
SDN	Software Defined Networking
UEBA	User and Entity Behavior Analysis
V/AR	Virtual or Augmented Reality
W3C	World Wide Web Consortium

1. Introduction

Digital Twin (DT) is an emerging paradigm that is receiving increased attention from industry, research institutions and academia. The evolution is catalysed by digitization, the emergence of affordable and accessible simulation environments, and the growing demand for a cost-effective, yet realistic solution to experiment with Information Technology (IT) and Operational Technologies (OT)-based infrastructures, without the associated operational risks and financial costs.

According to the DT Consortium in [DTC22], a DT can be defined as *"a virtual representation of real-world entities and processes, synchronized with specific frequency and fidelity*", whereas some other authors, such as [WU21], classify it as (1) a virtual model / digital representation (i.e., *a DT is a set of virtual information that fully describes a potential or actual physical production from the micro atomic level to the macro geometrical level* [ZHE18]); (2) a software/simulation (i.e., *based on faster optimization algorithms, increased computer power and amount of available data* [SDE17]); and (3) an integrated system (i.e., *a DT is actually a living model of the physical asset or system, which continually adapts to operational changes based on the collected online data and information, and can forecast the future of the corresponding physical counterpart* [LIU18]). Moreover, the European Commission also compiles in [NAT20] a set of definitions drawn from different standardization communities and organizations, such as that provided by the W3C (World Wide Web Consortium). W3C states that a DT is *"a virtual representation of a device or a group of devices that resides in a cloud or edge node. It can be used to represent real-world devices that may not be continuously online, or to run simulations of new applications and services, before they are deployed on real devices"* [W3C20, NAT20].

Also, the creator of the technological concept, M. Grieves, stated in [GRI14] that the DT is mainly composed of two essential spaces (one virtual and one physical) connected through bidirectional communication links between both spaces. This way of connecting spaces is precisely what differentiates a DT from other correlated simulation systems. In [KRI18], Kritzinger *et al.* state that there are three different conceptualizations with different integration modes depending on the data flow: (i) *Digital Twin* (based on bidirectional communication links with automatic data flows in both directions), (ii) *Digital Shadow* (bidirectional communication with manual data flows from the virtual space to the physical space), and (iii) *Digital Model* (with manual data flows in both directions). The automatic bidirectionality of the DT is what makes this technology attractive, allowing DTs to make decisions for themselves and act accordingly.

Because of this autonomy, it is evident that the construction of a DT entails the consideration of other technologies that, together, can explain relevant states to the benefit of the business model, production, and value chain. Through simulation, historical data, models, and digital model specifications, it is possible to create a more holistic and standard understanding of an observed element, context and situation, improving the situational awareness of an organization, and in terms of components, processes or facilities. As stated in [DTC22], DTs are systems in themselves that can be adapted to multiple use cases, synchronized with the real world through current IT/OT technologies and their communication protocols.

In addition, this impact has attracted the attention to many international organizations. For example, standardization organizations are being involved in the standardization of reference architectures and in its enabling technologies, such as the Internet Research Task Force (IRTF) in [ZHO21] (described in detail below) or the International Standard Organization (ISO) in [ISO22]; and

consortia and associations are emerging to give response to current needs. In the particular case of ISO, a first document concerning a standard framework for DT technologies has been recently released. The standard comprises four parts: ISO 23247-[1-4]:2021. The first part [ISO21a] provides an overview and general principles of a DT framework for manufacturing, including terms and definitions and requirements of the DT framework for manufacturing, while the second part of the standard [ISO21b] shows a reference architecture.

Similarly, the National Institute of Standards and Technology (NIST) joined the debate on emerging standards for DTs. In 2021, they published their first draft on that topic called "*Considerations for Digital Twin Technology and Emerging Standards*" - NISTIR 8356 [NIST21]. The draft provides a detailed definition of DTs, the motivation and vision for their use, common low-level operations, usage scenarios, and example use cases. Focusing on technical considerations with the cybersecurity and trust of DT, the report analyses novel cybersecurity challenges arising from the use of DT architectures and examines the traditional cybersecurity challenges that apply. Finally, the draft report assesses the cybersecurity challenges of technology and discusses the impact that lack of trust and standards can have on the functionality and quality of DT.

Regarding consortia and associations, one of the most relevant is the Digital Twin Consortium [DTC22], which aims to be the new "*Authority on Digital Twins*", bringing together industry, government and academia to drive consistency in the vocabulary, architecture, security and interoperability of DT technology. It drives the awareness, adoption, interoperability, and development of DT technology. Through a collaborative partnership with industry, academia, and government expertise, the Consortium is dedicated to the overall development of DTs. The main contributions have so far been the attempt to standardize recurring terms and processes within a DT architecture. Important contributions were also given in the structuring of any business and marketplace, as well as on the open-source approach.

Another interesting consortium is the Industry IoT Consortium (IIC) [IIC22], founded in 2014. The consortium is focused on driving technology innovation that fosters business development. It aims to help organizations identify best technology practices, build credible brands, and grow their businesses by facilitating member networking, collaboration, and liaisons. Its main contribution to the DT community has been the Technical Paper [IIC20] for DTs for Industrial Applications. Unlike the previous consortium, the IIC is more verticalized on the issues of the Internet of Things. Despite this, the White Paper offers an important contribution by covering aspects related to: the definition and characteristics of a DT; the relationships between DTs to form composite systems; the role of the DT in the life cycle of entities, considering scenarios with and without DTs and the business value added by the DT; the internal design of the DT; and examples of the use of DTs in various industries.

Unfortunately, all these actions are currently in progress, so there is no unified definition [BAR19, ALC22] that guarantees a common implementation methodology at the technical, operational and administrative levels. Hence, to date, it is still a challenge to talk about what the launch of DT-based ecosystems would entail. Probably one of the main reasons for this is the enormous technological boom that the implementation of DTs could entail. In line with Industry 4.0/5.0 and related scenarios, there are multiple technologies that can be integrated as part of a DT such as: Artificial Intelligence (AI), Cyber-Physical Systems (CPS), (Industrial) Internet of Things ((I)IoT), edge computing, 5G/6G, and so on [XU21, MIH22, ALC22]. Therefore, it remains difficult to find a way to establish a unified "*one-size-fits-all*" approach to DT-based projects.

Regarding the application of DT technology for specific use cases, it is worth highlighting its great relevance today for resilience and cybersecurity. Through its simulation capabilities (both offline and online), it is possible to predict risks and anticipate threat situations [ALC22] that can be prevented and/or mitigated in time, especially in those critical application scenarios (e.g., healthcare, manufacturing, energy [NAT20]). This detail is also remarked in [AHE21], where the authors stress the feasibility of the technology for the various Industry 4.0 application scenarios. Its simulation capacities allow, for instance, to provide interesting services that other technologies alone would not be able to address, such as predictive maintenance, real-time monitoring, remote control, process optimization, safety management, failure analysis and tracking, strategy evaluation, health monitoring, management of risks, training, and cybersecurity.

In line with the above, this ECSO Technical Paper explores the basic definition of Digital Twin, its limitations and technical dependencies, and presents some of the use cases and challenges currently facing the technology, especially in the area of cybersecurity. It should be noted that the report itself is not intended to provide exhaustive research on the topic in question, but rather to illustrate the current state of the technology and its demand from a research and industry perspective.

2. General use cases

As stated above, a DT is a digital representation of a real object or system, which is updated from real-time data, machine learning models, specification models and reasoning to aid decision making. In other words, a DT creates a highly complex digital model that is the replica of a physical object. This cyber-physical synergy implies that virtual copies (composed primarily of pieces of intellectual property such as property protocols, configurations, topology information, software components, etc.) represent real-world physical assets, where behaviours, properties and states are rigorously simulated from the virtual plane. There are already several applications that make use of DTs and for various types of application scenarios, such as: business, education, industry and cybersecurity.

2.1. Use case #1: business

The use of DT-based architectures or frameworks in business modelling permits decision makers to make decisions based on real data and situational awareness. In particular, the employment of technology to simulate business flows and processes allows new or modified solutions to be introduced to deliver greater efficiency. The vision is to deploy DT as a complementary process rather than adding barriers and checkpoints, where the technology will add valuable insights and tool sets. In doing so, security or business performance issues would be detected and resolved earlier in the lifecycle.

To work properly, business modelling must constantly implement and analyse process and technology (strands). To this end, critical business systems shall be replicated in the simulation environment through the orchestration and provisioning of infrastructure and service. Current business operations where DTs can be applied are usually based on IT and OT infrastructures, with the potential involvement of multiple cloud. The DT environment must maintain the map of items used in the production infrastructure, and enable the automated provisioning, reconfiguration and decommissioning of such items, and their allocation to roles within the system as a whole. Energy is an example of an application domain where the security of the infrastructure and the business are closely interconnected. By mapping the entire electric infrastructure and connecting critical assets to business operators (both transmission system operators and distribution network operators) through DTs, it is possible to identify and analyse potential system compromises and malfunctions that could have a significant impact on the business. This approach also enables the evaluation of the return on investment of potential mitigation measures, enabling accurate assessment of how well they protect the infrastructure and, as a result, the business. The research project CyberSEAS [CYB24] examines this aspect in depth.

DT system shall support the automated management of the replicated systems, deploy, update, reconfigure and remove applications and systems in the simulated infrastructure. For this to be sustainable not only a reference system is required, but a digital library storying the system components along with the business operational Key Performance Indicators (KPIs).

2.2. Case use #2: education and skills

"*Tell me and I forget, teach me and I may remember, involve me and I learn*". Benjamin Franklin.

The affordability and accessibility of cyber ranges and simulation environments increases the integration of DT technologies into training and education programmes. According to several studies, simulation-based leaning enhances motivation, self-responsibility for learning, facilitates peer learning and improves the overall learning activity, as well as providing hands-on knowledge. During the rise of online learning, it has further become clear that simulation-based learning contributes to re-creating the social classroom experience, with more improvised classroom engagements.

Deploying DTs reduces the time and expense associated with construction and commissioning of new systems. In addition to the above, it shall be underlined that physical equipment is costly and needs space to be stored and the learning process is usually slow. DTs provide a highly flexible medium/tool, as the number of connected machines and services is easy to adjust both in nature and numbers compared to their physical counterpart. Moreover, DT technology makes the ultimate immersive learning experience possible. By using a DT, participants can learn highly engaging tasks, experience realistic hands-on activities which can be too dangerous, complex, or expensive to be executed in real world. Rather than practical experimentation of e.g. a real manufacturing or nuclear plant, participants can use a DT of the real live system and their components to exercise their skills.

DT-based virtualized competency development allows for a customized training experience, as each participant can focus on the segment or part of the big picture they would like to participate in or need to understand based on their job profile. Digital Twin-based competency development can involve a Virtual or Augmented Reality (V/AR) based learning experience, achieving maximum engagement by reading abstract concepts quickly. In addition, the simulation environment offers the opportunity to run simulations in a safe manner and to experience with the impact of those simulations. The system behaviours can be explored under different conditions, understanding system failures or parameters without endangering expensive equipment, business operations or human life.

Therefore, while cyber ranges and connected cyber competence building activities already offer hands-on experimentation capability with simulated systems, DT have enormous potential in growing skills and competences operating real systems and understanding their behaviour using real-time data and simulations.

2.3. Case use #3: collaborative Industry (4.0/5.0)

One of Industry 4.0 challenges is the way technology modifies the role of human workers, which becomes a collaboration with robots on the shop floor, rather than manual tasks or automated tasks supervised by human operators [WAN17]. In contrast, the concept of Industry 5.0 provides a different focus and highlights the importance of research and innovation to support the industry in its long-term service to humanity within planetary boundaries. One of the most important paradigmatic transitions characterising Industry 5.0 is the shift of focus from technology-driven progress to a thoroughly human-centric approach.

Human behaviour in the digital sphere has been addressed by sophisticated detection techniques known as User and Entity Behaviour Analysis (UEBA) [RAG20]. However, understanding a chain of events revealing human behavioural patterns across cyber and physical spheres remains an unaddressed challenge. The integration of human behaviour modelling in the DT will allow for the refinement of factory design from both a performance and a resilience perspective [ZAD16].

The concept of human DT has been addressed previously in the literature. For example, Bao *et al*. [BAO19] consider the DT as a method or tool to be used in the simulation and modelling of the behaviour and status of entities. Graessler and Poehle [GRA17] developed a DT that assumes the employee communication and coordination tasks with the production system. The usual concept of a DT that emulates the properties and behaviour of a system was adapted by the authors to act as a representative for a human employee in a Cyber-Physical Production System (CPPS), since the property and behaviour of the human DT need to be based on user feedback and recorded patterns instead of actual measured data. Buldakova and Suyatinov [BUL19] also developed models for assessing the status of the human operator in cyber-physical systems. These models are used to evaluate the functional state of the human operators. In [EC20a] the idea is to consider a multi-domain DT, in which human behaviour is monitored by means of non-intrusive sensors, which gather human behaviour data to support digital models. It should be noted at this point that human emotional behaviour is also considered and contributes to safety objectives.

2.4. Case use #4: industrial cybersecurity

CyberFactory#1 (ITEA4 17032) Project goal is the optimization and resilience of the Factories of the Future[1]. Coordinated by AIRBUS Cyber Security France, one of the goals of CyberFactory#1 has been to prove the hypotheses formulated by [BEC18] and [BEC20] that DT can effectively support security enforcement, notably at the design, commissioning, and execution stages of an industrial digitization program.

Airbus Defence and Space (ADSS) owns several factories in Spain, Tablada, San Pablo Sur, and Cadiz, which are dedicated to the production and final assembly of commercial and military aircrafts [AIR21]. ADSS has launched an important digital transformation program which relies on the deployment of a multi-site and multi-asset IIoT platform to support enhanced automation, optimization, and quality control on sensitive industrial processes involved in the manufacturing of flight-safety critical aeronautical parts.

A DT, supported by the Airbus CyberRange platform, was developed for three use cases. One of them is related to the Roboshave system, implemented in Tablada plant to automate rivet shaving operations on Boeing 737 [BOE21] rudders. The RoboShave system could be described as a robotic arm whose role is to shave rudder rivets and to automatically check that the shaving operation has been performed successfully. The DT includes all the physical assets, such as Robot FANUC M-20iA/35M, profilometer Gocator 2120 and Programmable Logic Controllers (PLCs), as well as system connectivity and the several protocols needed, such S7Comm link, ModbusTCP and Airbus CyberSecurity simulator (Profilometer), and Profinet. Several protocols in use within

[1] https://itea4.org/project/cyberfactory-1.html

this list were not supported by vendor solutions, such as the Profinet layer that was developed by Airbus CyberSecurity and supports certain functionalities resulting from the specifications indicated in IEC 61158-5-10 and IEC 61158-6-10 [5]. As an example, **Error! Reference source not found.** a nd **Error! Reference source not found.** illustrate the physical Robotshave system and its DT.

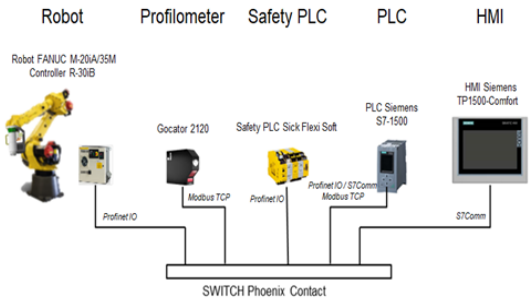

Figure 1. Roboshave System Connectivity Overview [PRA22]

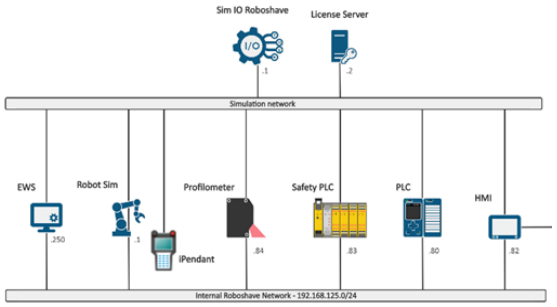

Figure 2. Roboshave DT Topology view [PRA22]

Based on risk analysis, the following attack scenarios were defined and implemented in the simulation environment [PRA22]: (1) compromise Roboshave functioning by removing connectivity between assets (loss of control from the operator point of view, on the HMI); (2) write in internal variables of the HMI to display wrong information (these will be raised into the Corporative Network); generate rogue IIoT devices accessible by legacy software; and manipulate work orders from a GapGun by adding, modifying and deleting configurations.

3. Architectures and Technologies for DTs

Several DT-based approaches already exist in the literature, either through architectures and frameworks, with the aim of fostering the development of specific DT solutions. To this end, we review the literature to show the great technological boom and the interest of industry and academia in launching DT-based technology solutions in the coming years.

Therefore, in this section, we first present some architectures and frameworks, mainly designed by organizations and academic entities. Subsequently, we mention some commercial and open-source solutions to develop DT approaches or applications.

3.1. DT-based architectures and frameworks

Despite recent efforts by international organizations, there is not a clear reference or standard Digital Twin Network (DTN) architecture generalized for every information system scenario. Based on the definition of the key elements of the DTN discussed, the most interesting formalized referenced architecture is the one described in [ZHO21] by the IRTF (Internet Research Task Force). This architecture aims to generalize the concept of Digital Twin Architecture (as also illustrated in Figure 1) for DTNs, the construction of which is very similar to that proposed by the standard ISO 23247-2 in [ISO21b] for manufacturing systems. In turn, and based on this type of reference architectures, there are already related works that propose the concept of DT in specific scenarios.

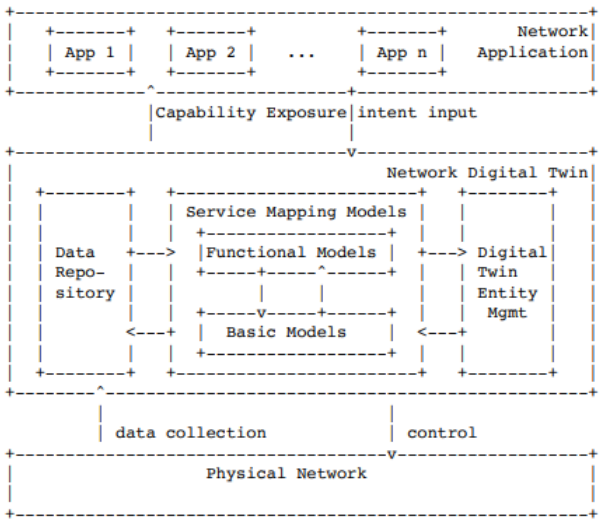

Figure 1. DT reference architecture defined by the IRTF in [ZHO21]

The related works, presented in [RED19, TAO17, ZHE19, YUQ20, JIE20], propose reference architectures for the application of DTs to specific domains, almost exclusively connected with manufacturing**.** In these proposals, the Digital Twin is mostly a gatherer of information from the physical plant, exploited for simulation, prediction, connection to disparate business applications, and storage of data. Very limited feedback from the DT to the physical system is considered, especially in terms of applying settings computed with optimization algorithms on the DT.

Of the works listed above, only [RED19] explicitly acknowledges security as a key issue for cyber-physical systems, across a six-layer architecture (L1: physical devices, L2: data sources for the physical system, L3: local data repositories, L4: IoT gateway, L5: cloud-based information repositories, L6: emulation and simulation). However, the discussion of this topic is constrained to conventional aspects of information and communications protection, secure coding, and proper implementation of AAA (Authentication, Authorization and Accounting). No mention is made of specific risks raised by the integration of DT in the system.

However, taking as a reference the architecture and the works just discussed, it can be observed that there are many similarities with those architectures based on Software Defined Network (SDN). In fact, the approach is basically the same: separate the physical layer from the control layer, from the application layer. It is therefore possible at this point to virtualize the technologies and manage them at the control level, according to the needs of the application level. The main advantage of this approach is that thus all the main logic of the architecture is reduced to the process of orchestrating the technologies involved (virtualized). This orchestration therefore has several advantages: (i) flexibility in the use of heterogeneous technologies, (ii) dynamic reconfiguration of a scenario, and (iii) portability.

Considering the SDN characteristics, the IRTF also presents in [HAL15] the technical report "*Software-Defined Networking (SDN): Layers and Architecture Terminology*", including a reference SDN architecture. From this specification, it is possible to note that levels/planes can be collocated with other planes or can be physically separated. SDN is based on the concept of separation between a controlled entity and a controller entity. The controller manipulates the controlled entity via an interface. Interfaces, when local, are mostly Application Programming Interface (API) invocations through some library or system call. However, such interfaces may be extended via some protocol definition, which may use local Inter-Process Communication (IPC) or a protocol that could also act remotely; the protocol may be defined as an open standard or in a proprietary manner.

Based on the analysis of this SDN-based reference architecture, we are then able to isolate and explain the main components of a DT architecture. Their main components are categorized upon layers, which corresponds to the layers that the DT architecture exposes in [ZHO21] to the users. Each of these layers have a specific outcome and purpose and can be summarized in upon three main layers: *physical, network*, and *application*. In the following and for each of these layers, we will discuss the fundamental blocks.

- The **physical layer** deploys all those network elements that exchange bulk network data and control with the network DT entity, through southbound interfaces. In this layer, the most important components are the communication protocols wrappers. The physical layer virtualizes the network components of the physical counterpart. For that reason, it needs to be able to also emulate the network protocols used in such virtualize environment. At this level, the DT needs to provide a network gateway protocol that is capable to allow the communication inside the physical layer.

- The **network layer** is of course the main part of the architecture and includes three subsystems: Data Repository, Service Mapping Models and DT Entity Management.

    - Data Repository: provides accurate and complete information about the network and its components for building various service models by collecting and updating

the real-time operational data of various network elements through the southbound interface.

- Service Mapping Models: completes data modelling, provides data model instances for various network capabilities, and maximizes the agility and programmability of network services.

- DT Entity Management: completes the DTN management function, records the entity lifecycle, visualizes and controls various elements of the DT network, including topology management, model management and security management. At this level, the main components that we can identify include an activity monitoring service that is able to track all tasks and functions within the DT; a data extraction service, which is able to analyze and visualize data from both the monitoring activities and the data repository; a management service, which tracks the different agents within the DT according to their privilege level.

- The **application layer**, which raises requirements that need to be addressed by the DTN. Such requirements are exchanged through a northbound interface; then the service is emulated by various service model instances. Once they are checked, changes can be safely deployed in the physical network. Note that in this layer, northbound communication is the main bottleneck/challenge. Applications at the network layer needs to be deployed without the need to add additional wrappers or gateway. For that reason, the main component here needs to be the application deployment service, which is in charge to correctly bind the application to the correspondent API of the network layer.

As aforementioned, the representation of all these layers described can be seen in Figure 1 [ZHO21], illustrating the main IRTF reference for DTs.

Other references models

Despite the lack of DT architecture standardization, based on the layered description, and on the main components that we provided, it is also possible to collect some scientific contributions regarding vertical applications of DTs. These contributions they both have in common the layered approach of the architecture, then the implementation of the main components, customized for their specific needs. These contributions are summarized in the Table 1 below.

For the purpose of this Technical Report, it is enlightening to notice that all of the referenced works, with the exception of two, never mention security.

Table 1. Other references DT models from the academy

Academic reference DT models	Their descriptions
DT-based architectures to integrate CPSs with cloud components [ALA17]	The authors propose an analytical description of a Digital Twin architecture reference model for the Cloud-based Cyber-Physical Systems (C2PS), where every physical thing accompanies a hosted cyber thing in the cloud. Two things can establish Peer-to-Peer (P2P)

	connections either through direct physical communications or through indirect cloud-based DT connections. In the proposed model, every physical thing is represented by a cloud-based DT, virtualizing its sensors, interfaces, computational and storage elements, etc. The combination of the two can give birth to a hybrid thing, which, assuming a negligible network communication cost, can perform any operation on the component (real or virtual) better suited to carry it on. In addition, the model considers the different modes of reaction to events, involving direct physical-to-physical, twin-to-twin or physical-to-twin interaction, and proposes a context-aware mechanism to allow things to autonomously choose which one to adopt. The model can be hierarchically extended to build systems-of-systems.
A DT-based industrial automation and control system security architecture [GEH20]	In this work, authors discuss how a DT replication model and corresponding security architecture can be used to allow data sharing and control of security-critical processes. Design-driving security requirements for DT-based data sharing and control are identified. Authors showed that the proposed state synchronization design meets the expected digital twin synchronization requirements and give a high-level design and evaluation of other security components of the architecture. An important development in this paper is represented by the network gateway component developed to emulate PLC traffic communication at the physical layer.
A DT architecture based on IIoT technology [SOU19]	In this work, authors propose a DT architecture, applying IIoT technologies for sense and actuate on the physical counterpart and using the OPC-UA communication protocol for structure and exchange unified data, and provide services to manage and process the data of digital counterpart of the system.
The concept of DT as a service [AHE21]	The proposed DT has been introduced to reconcile the (usually rigid) application of virtualization techniques to manufacturing with the need for massive individual customization, as promised by Industry 4.0 movement. The conceptual reference model proposed to achieve this result is composed of three layers (physical, digital,

	and cyber) and a communication model to exchange data between them. The physical layer defines the means of real attributes, including resources such as objects, assets, products, personnel, equipment, facilities, systems, processes, environment, or "things" that has material existence in the physical world. The digital layer is the recording of data in raw or different file formats such as Computer-Aided Design (CAD) or Computer-Aided Manufacturing (CAM) to support the creation, modification, analysis, optimization, or prediction of a static, dynamic, and real-time data. A bidirectional link with the physical layer exists to make modelling and simulation possible. The cyber layer includes cloud processing and storage for building a dynamic data model, which can enable digital capabilities at scale. Also, the Data model builds Information, Knowledge, and Wisdom (DIKW) by using IoT, Big Data, and cloud technologies.
Mobility DT: concept, architecture, case study, and future challenges [WAN22]	In this study, a Mobility DT (MDT) framework is developed, which is defined as an AI-based data-driven cloud-edge-device framework for mobility services. This MDT consists of three building blocks in the physical space (namely human, vehicle, and traffic), and their associated DTs in the digital space. An example cloud-edge architecture is built to accommodate the proposed MDT framework and to fulfill its digital functionalities of storage, modeling, learning, simulation, and prediction. As a validation of what we just presented, a recent article in [QIA22] shows a review of the architectures of DT, data representation, and communication protocols. Authors mention that there is not a clear standard for such architectures, but they described a pool of different network protocol component that has been developed to emulate real scenario inside a DT replica. This work points a real trend on what are the challenges in the DT world.

3.2. Technological solutions to implement DTs

So far, there are a few commercial software solutions that implement DT technology, mainly developed by large companies in the manufacturing sector. Table 2 shows a non-exhaustive list of DT technology from popular vendors.

Table 2. Available commercial solutions to implement DTs

Available commercial solutions to implement DTs, vendors	Their descriptions
DT solution, General Electric (GE)	An advanced and functional DT that integrates analytic models for components of the power plant that measure asset health, wear and performance. The DT is integrable in the GE developed distributed Predix platform for "large-scale machine data processing, management and analytics" and IIoT applications [ELE22].
PTC Windchill, PTC	A DT that enables manufacturers across industries to understand how their customers use their products. In this way, they can help them improve the design and performance of those products [PTC22].
3DS, Dassault Systèmes	A DT that allows manufacturers to make virtual products available to the market for experimentation and testing in realistic conditions before engaging in any real production [KAR22].
DT solution, Seebo	It is a graphical interface that allows the generation of actionable insights that maximize overall equipment effectiveness, reduce unplanned downtime, and uncover the root cause of issues. Dashboards allow real-time visualization of the operational health of deployed machines and display enriched alerts with predictive metrics based on key machine parameters, such as machine temperature, pressure, vibration, humidity, fatigue, and wear in order to quickly identify and solve issues remotely [SEE22].
Simulation Modeling SW tools and solutions, Anylogic	Anylogic software provides simulation capabilities in a single commercial package with special research licenses available. It is specialized in factories and production lines, with discrete-event simulation capabilities, and has libraries capable of supporting several types of fields [ANY22].
DT solution, Ansys	A DT that can be used to monitor real-time prescriptive analytics and test predictive maintenance to optimize asset performance. The DT can also provide data to be used to improve the physical product design throughout the product lifecycle [ANY22a].
DT framework, IBM	The framework allows companies to virtually create, test, build and monitor a product, reducing the latency in the feedback loop

	between design and operation. It enables to identify and fix problems and bring products to market faster [IBM22].
IoT service, Microsoft Azure Digital Twin Software	IoT service that virtually replicates the physical world by modelling the relationships between people, places and devices in a spatial intelligence graph [AZU22].
Factory I/O, Real Games	It is a software [FAC20] that allows to set up configurable 3D-simulations by plug in components of a given industrial equipment catalog. To this end, the software provides simulation aspects of DTs, explicit synchronization between real system and virtual replica is limited to the integration of several PLCs for simulatively testing the virtual factory.
SW development services to build DT solutions, Siemens	These services include a machine-human interface [WAN19] that can be used for the construction of a DT for humans and a portfolio called digital enterprise suite [SIE20], which comprises, e.g., DTs for material transport equipment.

Unlike proprietary products, opens-source solutions allow the technology to be freely redistributable and modifiable, helping manufacturers to combine legacy equipment with modern sensor-based machines and tools from different vendors. In this case, we identify a set of available frameworks, which is listed in Table 3.

Table 3. Available open-source solutions to implement DTs

Available open-sources solutions to implement DTs	Their descriptions
CPS Twinning	It is a framework for generating and executing DTs that mirror CPSs [CPS22]. Particularly, CPS Twinning is a proof of concept that can be used as first approach to model some environments, but also has some limitations such as inability to generate DTs for wireless devices [ECK18].
Wrld3d	It is an open source platform that allows the creation of DTs in a quick and easy manner, using a comprehensive set of self-serve tools, Software Development Kits (SDKs), APIs, and location intelligent services. As a dynamic 3D mapping platform, it enables to create virtual indoor and outdoor environments upon which data from sensors, systems, mobile devices, and location services can be visualized within millimeter accuracy [WRL22].

Mago3D	It is a platform for visualizing massive and complex 3D objects including Building Information Modeling (BIM) on a web browser. Thus, it is possible to model DTs that creates parallel worlds in a virtual reality with several sensors [SHI19].
i-Maintenance	It is a toolkit that enables to create a DT of an industrial asset in order to obtain information on the status of all components related to the production and maintenance of the industrial process, collect, monitor and analyze lifecycle data. It is composed of a messaging system, a set of adapters to integrate sensor/actuator systems and other software components that are used as a technical foundation for the DT development [STR18].
Eclipse Ditto	It is a DT developed by Bosch. It enables the design of DTs in a form of IoT development patterns. It can be seen as an open-source foundational layer of Bosch IoT platform [ECL22].
imodel.js	It is a platform for creating, accessing, leveraging, and integrating DTs. As what happens with Eclipse Ditto, it is a commercial initiative connected to the US infrastructure company Bentley. According to the developers it was designed to be both flexible and open, so that it can be easily used and integrated with other systems [CRE22].

At the intersection between pure proprietary and real open-source DT technology, open-source solutions are developed by big companies, which make them limited in scope, due to the commercial interests of the developers [ROE19].

To summarize the technologies mentioned, Table 4 shows the different DT technologies according to the terms and conditions of their usage, for example, whether they are open source, limited open / commercial solutions, commercial products, or prototypes. With this, we also show the influence and interest of this new technology in today's market, and how it is part of the interests of many organizations and companies.

Table 4. Grouping the above-mentioned technologies according to the terms and conditions on its usage

Type	Solutions
Open Source	*Wrld3d; Mago3D; i-Maintenance*
Limited Open / Commercial	*Eclipse Ditto; imodel.js*

Commercial Products	*PTC Windchill; Factory I/O; IBM Digital Twin framework; SIEMENS Digital Enterprise Suite; Microsoft Azure Digital Twin; Anylogic; Ansys; GE Digital Twin*
Prototypes	*CPS Twinning*

4. Cybersecurity problem statement

DT is an emerging technology capable of virtualizing and simulating physical world assets to empower innovative optimization actions in many of today's application domains. Through verification and validation, it is possible to improve diverse operating actions and processes, such automation tasks, logistics, and even aspects related to maintenance, resilience, and cybersecurity of products, processes, or systems. But DT can also be an effective tool for decision making, and especially for the field of cybersecurity, where it is necessary to anticipate potential threats and respond to them accordingly. Therefore, this document places major emphasis on protection and cybersecurity aspects, both in terms of operations for critical infrastructures and for the DT system itself.

DTs can indeed be seen as a technology capable of optimizing processes, predicting failures, and detecting anomalous situations. If these capabilities are extended for cybersecurity [GE22], then it is possible to prevent and mitigate potential cyber-attacks such as Advanced Persistent Threats (APTs) [HOL21]. In [HOL21], the authors address the potential abilities of the paradigm to cover many of today's cybersecurity challenges, exploring opportunities to model threats, test, detect and mitigate situations. These capabilities can even increase an organization's situational awareness by providing a better picture of the situation and explaining, continuously and in real time, the current status of the physical counterparties involved, and in terms of vulnerabilities, potential exploits and/or risks.

Despite the above, and although DT technology brings to Industry 4.0/5.0 new opportunities to create secure and more resilient digital ecosystems (reducing potential risks that can seriously affect the quality and welfare of many strategic sectors and infrastructures in Europe), there is still not enough research and work in this area. For example, there is a lack of dedicated support for the protection of the cyberspace of a DT device, where multiple IT components - detailing the nature of the physical's assets (e.g., property configurations, Intellectual Property (IP), property industrial protocols, connections, etc.) – are widely deployed. Unless protection measures are adequately considered at this point, multiple security problems may arise: (a) at the IT level (with risks to confidentiality, data integrity and data availability) – *cyber world* -; (b) at the OT level (with risks to operational availability and data integrity) – *physical world* -; and (c) at the communication level.

It follows that the DT attack surface can be large and significant for many of the ecosystems and infrastructures supported or based on DTs, probably due to the IT-OT interrelationships between spaces [ALC22].

Therefore, the ECSO Technical Paper focuses primarily on addressing and discussing two relevant cybersecurity issues:

- ***How to use the Digital Twin for protection*** of other infrastructures and systems.
- ***How to protect the Digital Twin and the access to its models*** to make sure its main functions without putting the security of an infrastructure and its IP at risk.

5. Digital Twins for cybersecurity

Through digital specifications, DTs are able to create unique opportunities to perform simulations and tests against HW/SW attacks and/or failures, analysing the possible consequences and impact, as well as serving as a unique laboratory to develop, validate and test security approaches and configurations to drive effective preventive and mitigating actions. These actions can even be carried out in parallel to the actual system so as not to disrupt its services or core functions of the main system. By mirroring the legitimate behaviour of devices and services within an infrastructure, DT-driven cybersecurity functions implemented on the simulation side should not collide and impact the operational tasks of their physical counterpart, mainly because they could be performed in an isolated environment parallel to the real one.

Therefore, their simulation capabilities make DTs potentially valuable assets for cybersecurity solutions. They can be beneficial for:

- monitoring and inspection of security events that occur in the physical counterpart, to identify possible threats to its operational processes;
- detection of cyber-attacks that attempt to exploit the vulnerabilities of an infrastructure, to enable the adoption of mitigation measures;
- detection of anomalous behavior exhibited by devices and services, to prevent them from being compromised by zero-day attacks;
- simulation of entire intrusion scenarios, including the possible characteristics of different cyber-attack variations and their impact on the security of the physical counterpart;
- response and recovery to face security risks by offering the system with mechanisms that help anticipate situations and provide mitigation measures;
- generation of potential sources of knowledge on which to apply learning techniques to improve other cybersecurity services (e.g. detection or response); and
- training to improve awareness and knowledge of cybersecurity and resilience issues.

These preventive and reactive capabilities can be provided in both offline and online modes. In [KRI18], Kritzinger *et al.* already mention the different ways of building different types of simulation systems, depending on the type of communication established with the physical environment. In the particular case of a DT, it is built under bidirectional and fully automatic lines of communication, allowing interaction with the real world in an autonomous and interactive way. This last feature allows, through simulation, to empower online cyber defense through more complete hybrid solutions, where it is possible to locate, predict and neutralize threats that can corrupt the real system [GE22].

While all of these simulation functions may be attractive to different communities, it is unfortunately in a very preliminary state from a research point of view, and most particularly in the field of cybersecurity and resilience. As mentioned above, there is still no standardized approach for its implementation in IT-OT networks, nor there are trustworthy research results that determine the degree of realism and fidelity to obtain highly effective results. But even in these circumstances, there is great interest from the different communities to deploy DT-based solutions, and especially for online cyber-defense in the different application scenarios (industry and manufacturing, transportation, healthcare, supply chain, etc.).

The remainder of this section will discuss some aspects of the technology's utility for governance and risk management, detection and situational awareness, resilience, privacy and training, also outlining some specific use cases for each of these application areas. In this way, we provide an overview of the current capabilities that the paradigm can give to the state of the art beyond its conventional use.

5.1. Risk management and governance

DTs have the potential to radically improve the way cyber risks are identified, measured, and managed within and across organizations. Nowadays, cyber risk governance is mainly based on process-based approaches that are carried out by C-levels (i.e. CISO and security staff). In contrast, the simulation capabilities offered by digital models (on which DTs are based) support the transition to continuous and event-driven approaches.

Events that trigger the execution of new risk assessments include changes to the cyber threat landscape, e.g. with the advent of a new cyber (or physical) threat, as well as modifications to the real infrastructure, which must be reflected by corresponding changes in the DT. In this context, the simulation capabilities offered by the model of a DT could be used to support:

- the **identification and confirmation of digital vulnerabilities** present in the physical counterpart, or that may appear as a consequence of modifications to the physical counterpart;
- the **understanding of the extent to what these vulnerabilities can be exploited** to compromise the physical counterpart's status and behaviour;
- the **simulation of cascading effects** of potential exploitations on the system itself, to understand impacts on higher-level functions like privacy, data protection, safety, operational and business continuity, etc.; and
- the **assessment of the effectiveness of "in place" and "to be" cybersecurity controls** in decreasing the risk related to specific attack techniques (e.g. ransomware), thus opening the way to more accurate protection and management strategies, compared to traditional evaluation of potential attacks and mitigation strategies, which typically have more operational relevance and shorter-term horizon.

Therefore, through simulation organizations can be able to explore, estimate and determine the existence of vulnerabilities and new security gaps, anticipating not only potential cybersecurity risks but also safety risks [HOL21]. An example of the latter is also found in [JAR20], which provides a real-time DT of the high-pressure hydrogen vessel to reduce failures and associated risks. Similarly, the work in [DAN21] presents the Automatic Network Guardian for ELectrical systems (ANGEL) DT approach to detect physical faults in a power system and classify the affected areas (IEEE 9-bus and IEEE 39-bus). This also means that essential requirements for the optimal functioning of DTs for assessing and managing cyber risks are proper knowledge of the CPS to be represented and related processes, and adequate features to describe and simulate cyber risks as precisely as they would impact the real system.

A clear **application example of how DTs can support the resilience of a CPS is healthcare**. Medical devices and their capabilities offer unprecedented opportunities to assist patients remotely and timely predict several types of emergencies (e.g., cardiopulmonary and respiratory arrest). The increasing volume of patient data collected, transmitted, and processed, as well as the

pervasiveness of medical devices require the assessment and management of cyber risks as an innovation enabler. DTs, by creating a virtual, dynamic, model of the system represent a convincing solution to carefully consider all the vulnerabilities of devices, services and networks and the impact of related threats in terms of performance, privacy, and safety. This enables different types of assessments, e.g., simulating data transfers in the system virtual replica, and getting results without compromising the physical counterpart. The virtual nature of the DT will also enable the application of advanced ML features integrating static and dynamic vulnerability detection systems, with promising potential of detecting zero-day vulnerabilities and the variants.

Another concrete example is **the employment of DTs for security purposes in the energy domain, improving the resilience of Smart Grids**. DTs play a major role in supporting the transition of grids towards complex cyber-physical systems, enabling to monitor, share and manage information exchanges between all participants and stakeholders across the value chain in near real-time. They can effectively specify the interaction dynamics between the system nodes, allowing to simulate and/or predict the cause of a given vulnerability or fault, allowing for possible preventive actuation or adequate preparedness. Acting also as excellent training tools, DTs can be implemented to simulate a security breach and evaluate operators' and engineers' capabilities to recognise symptoms of a control system compromise and select the best mitigation action accordingly.

5.2. Attack modelling and testing

Testing industrial protocols and/or testing security applications in an isolated and secure environment with the same characteristics as the physical counterpart is one of the main challenges of future industrial systems. Therefore, in this subsection, some examples of test cases of industrial scenarios are presented, focusing the discussion especially on industrial protocols and Intrusion Detection System (IDS) rules. **In other words, a simulation of attacks against a known industrial protocol is detailed along with the results obtained from [WU19], in which a DT simulating some specific test scenarios for the aerospace industry is presented.**

One of the first series of **DT-based tests** was conducted **on industrial protocols** to determine and verify how potential attack vectors and corresponding rules for an IDS could be addressed. In particular, a number of possible enumeration and disruption attacks against Modbus masters/servers were tested [MOH22]. The first set of tests aimed to determine the reachability of Modbus masters across the network, where attackers were able to scan the production network to identify and locate Modbus masters/servers. With this test, it was possible to understand the reachability between the attacker's network and the production network. Once this identification phase was completed, an enumeration phase was performed to count all the registers. Two action then are performed: (a) reading registers, and (b) writing registers.

Reading of the registers had two main objectives: (i) to enumerate the application exposing the Modbus server and (ii) to map the attack surface. In the first tests, a massive reading of registers was performed. This type of actions, if not well limited, could lead to a disclosure of the information exposed by the Modbus server, which consequently could also lead to a slowdown of the service itself, which would not be able to satisfy all requests, causing a denial of service. Once the attack surface of all exposed records was mapped, the next step was to verify where it was possible to write these records.

Writing to the logs can cause two main effects: (i) interrupting the application or (ii) changing its behaviour to a malicious one. For that reason, it was important to test a possible injection of value to the exposed register. Overall, these tests were extremely simple.

As can be seen, these tests were not initially intended to show innovative attack techniques on specific masters, but rather to demonstrate what kind of attacks or misconfigurations could be easily tested using DT technology without affecting the physical counterpart. Modbus has been chosen as a basic example, but the same type of tests can be run with more recent protocols such as: MQTT, DNP3, CAN-OPEN, etc.

The proposed DT can be also used to test defence solutions. An important defence mechanism to test, for example, are the traffic rules for an IDS. These rules are used to identify an attack according to the specific signatures of the traffic traced. The last test that can be performed goes exactly in this direction and wants to show the possibility of testing rules for a known IDS. These tools perform a detection on an anomalous behaviour such as a massive reading of Modbus registers. With a virtualized infrastructure, such as the one that implements DT, it is very easy to mirror the traffic in such a way as to redirect the cloned traffic on an ad-hoc network for this type of analysis. The effectiveness of the rules could then be tested in a secure environment.

5.3. Intrusion and anomaly detection

As mentioned, DTs can replicate the intricacies of physical and cyber systems in greater detail, being able to perform more accurate simulations to improve the security and protection of CPSs [ECK19a]. To describe these capacities, we consider the defense modes described above: online and offline mode.

In offline mode, DTs are able to **simulate threat scenarios to derive vulnerabilities** (either typical and known CVE (Common Vulnerabilities Exposures), or new and zero-day ones), **identify anomalous events caused by predefined attack vectors, test and define new attack patterns and rules** as indicated in the previous section, and **adjust and reenforce existing ML algorithms** for example, for **predictive maintenance** (the area in charge of understanding when a certain component, production line or device needs assistance or maintenance), **and intrusion and anomaly detection in critical scenarios**. Precisely, the latter DT use case is currently one of the most widespread in CPS scenarios and industrial ecosystems. In [XU21], the authors present a novel approach called "Anomaly deTection with digiTAl twIN " (called as ATTAIN), which builds DTs for anomaly detection, using live data obtained from a CPS and heuristics. Also, the work in [CAS21] shows the potential features of using semi-supervised approaches for anomaly detection in industrial environments, which make use of a DT to generate a training dataset that simulates normal machinery operation, along with a small set of labeled anomalous measurements from real machinery.

On the other hand, DTs in online mode could, in addition, **detect events that go beyond traditional IDSs**, generally based on predefined attack signatures or on the use of machine learning algorithms for anomaly detection. DTs could complement detection actions by deriving deviations based on the "semantic" behavior of the natural operations of a CPS (what we refer to below as legitimate behavior). The result would then be a hybrid detection system capable of estimating new situations based on casual events, caused by eventual behaviors of the system

and its environment (e.g. network traffic), with respect to more systematic functions of the CPS itself.

Unfortunately, the use of DTs for intrusion detection remains a relatively unexplored topic, although there has been some recent research and some use cases as study scenarios. In 2018, Eckhart and Ekelhart [ECK18a] demonstrated the applicability of DTs for attack detection in **Industrial Control Systems (ICSs)**, by monitoring their legitimate behavior of CPS. The authors introduced a specification-based framework that requires explicitly defined physics rules to create a simulation and compare it with a live system, considering inconsistencies as cyber-attacks or physical malfunctions. In 2020, Akbarian *et al*. [AKB20] also created a DT to detect attacks against an ICS, but estimating the legitimate behavior of the system using a statistical algorithm. Despite not having explainable rules, the dynamic adaptation of a virtual replica to new and more complex threats has the potential to significantly improve the resilience of ICSs.

Another application for DTs is the detection of attacks targeting **Smart Grid environments**. In 2019, Danilczyk *et al*. [DAN19] proposed the use of a simulated environment to monitor a microgrid and its communication infrastructure, using physics-based models to perform a real-time estimation of the expected behavior. The use of DTs to replicate security events of power grids and detect malicious behavior is a promising approach to protect both the physical stability and the communication network of Smart Grids.

5.4. Response and recovery

Drawing on the information offered above, it becomes evident that the automatic decisions of DT can accelerate mitigation processes in an accurate and high-fidelity way. An example of this can be found in [SAA20]. This work proposes an IoT-based Digital Twin with Cloud support for controlling the effect caused by an individual or coordinated false data injection attack, as well as denial of service cyber-attacks. Moreover, the authors of the paper in [HOL21] clearly mention the importance of applying DT approaches to test and validate the actual effectiveness of security patches at a low cost (in terms of deployment in complex IT/OT infrastructures), and without requiring the configuration and implementation of secondary systems to drive such testing processes.

Any entity, which aims to effectively implement methodology of DTs to their network, ought to previously have reached a high level of cyber maturity and resilience. It is therefore important for such entities to take a holistic approach to cybersecurity. This can be achieved through the integration of Cyber Threat Intelligence (CTI) in order to align any network strengthening prior to the implementation of DTs methodology. In particular, the implementation of CTI will have significant consequences for any organization in the response and recovery to incidents, by understanding digital and physical security architecture, mapping potential attacks and thus incorporating response and resilience into day-to-day practice, and allowing visibility over all areas of risk in terms of Confidentiality, Integrity, and Availability (CIA).

CTI is data collected, processed, and analyzed in order to understand the motivations, targets, and attack behaviors of a threat actor. It enables organizations to make faster, more informed, data-backed security decisions, and change their posture from reactive to proactive to counter threat

actors. There are three different levels of CTI, which are *operational*, *tactical* and *strategic*. Each level has a different audience, application, and nature of the information transmitted:

- *Operational CTI* refers to the investigation of the adversarial capabilities, infrastructures, and Tactics, Techniques and Procedures (TTPs), in order to use that knowledge to target and prioritize mitigation efforts. Those involved in vulnerability management, incident response and threat monitoring are the largest consumers of operational intelligence as it helps them to be more competent and effective in their day-to-day functions.

  Operational CTI is specifically important to the relevance of DTs, as it enables organizations to strengthen their networks preventatively against common TTPs and take preventive and proactive actions making networks more robust and mature. For response, this allows a quick mitigation of any impact, and assists in recovery at is allows prioritization of initial recovery efforts, particularly aligning to mitigation efforts.

  Tactical CTI focuses on performing malware analysis and enrichment. In this context, Indicators of Compromise (IoCs) – such as domains, IP addresses, emails – are particularly relevant and useful for updating signature-based defense systems in order to defend against known attack types, but they can also be useful for more proactive measures such as threat hunting exercises.

  Similar to Operational CTI, Tactical CTI is crucial for any DT implemented methodology as it allows for the mapping of different types of network threats across a wide range of models. Tactical CTI combined with Operational CTI enables detailed and proactive simulation, testing, and modelling, which sit at the heart of the DT methodology. For response, this allows proactive mitigation against identified areas of weakness. For recovery, Tactical CTI offers an overview of the cyber-security estate, and enables the swift recovery of defense systems to prevent further attack.
- *Strategic CTI* gives a comprehensive picture of a company's threat landscape. It is most useful for informing high-level executive decisions, and the information is often business-oriented and delivered through reports or briefings – materials that can only be prepared by humans with knowledge, not algorithms. Good strategic intelligence should provide insight into the risks associated with specific actions, broad patterns in threat actor tactics and targets, geopolitical events and trends, and other related themes.

  Strategic CTI can guide the implementation of DT methodology, identifying and mapping an overall threat that can disrupt both digital and physical systems. In particular, Strategic CTI can map digital threats to physical systems, clearly understanding and identifying the risks in terms of CIA.

Overall, CTI combined with DTs can contribute to help organization's security if implemented correctly and supported by a clear and structured process. Specifically, regarding DT methodologies, incorporating all levels of CTI can guide, map and mature cyber security in a number of separate use cases:

- *Red and Purple Teaming*: CTI for red and purple teaming allows the teams to **recreate realistic scenarios representing the threat landscape** most likely to apply to the organization in question. As a result, red and purple teams are able to mimic the tactics, techniques and procedures of threat actors targeting the critical functions of an entity based on the CTI provided, this is crucial when working across both the physical and the cyber estate [ECB23]. This capability is closely related to that detailed in subsections 5.1 and 5.2 above.
- *SOC Implementation*: DT-powered CTI provides valuable information to the Security Operations Center (SOC) team by collecting data on, among others, past cyber incidents, ongoing campaigns, actively exploited vulnerabilities and actively used malware, and simulating malicious scenarios. From a response and resilience perspective, this gives the SOC team the tools to **pro-actively pre-empt and respond to attacks, reducing recovery time and attack impact**.
- *Incident Response*: Utilizing DT-powered CTI mechanisms during and after a cyber incident can assist entities to be able to effectively **assess the impact of the incident**. Through DT-enabled CTI, entities can be able to assess the impact of cyber incidents based on previous similar occurrences or/and predefined simulated scenarios. Furthermore, intelligence gathered through statements and posts published by the threat actor from deep and dark web can further assist the entity for its attempts to bring all the services and functions back to normal. This is particularly important for entities which are using DT methodology, given their varied and expanded security estate.
- *Post Incident Recovery*: DT-powered CTI provides **critical insight during the post-incident recovery process**. By understanding threat paths and potential attack scenarios, impacted organizations can understand the potential impact of attack, both internal (such as impacted directories, systems, and potential for future attacks of damages), and external (potential regulatory issues, and potential financial issues). In terms or significant or potential extinction-level events, DTs can be used to identify potential paths to recovery, including identifying areas of the cyber estate which are the most priority in terms of time and impact.

As such, taking a holistic approach to cyber security and incorporating CTI into the cyber security practices can enable entities to **increase their level of cyber maturity and lifespan**. Entities implementing DT will face an increasingly complex security environment, with a significantly expanded attack landscape. As such, DT-enabled CTI will enable any organization to proactively identify potential threats and risk, and implement targeted simulation testing, red-teaming, and monitoring. These implementations are crucial for organizational response and resilience, as it enables organizations to both improve their security posture while being prepared for both the attack and response phase of a cyber incident. Furthermore, implementing DT methodology more effectively requires entities to have robust cyber security and cyber security practices. It is crucial for entities looking to implement DTs to incorporate CTI into their cyber security practices.

5.5. Situational awareness

Situational awareness corresponds to a specific area of cybersecurity that comprises a set of services that go beyond traditional detection systems and context-awareness-based systems. As

stated in [ALC13], situational awareness is a complex protection service that attempts to explain what is happening in one or more application domains and with a high level of precision and granularity, detailing: what, where, when and by whom the event has triggered.

The concept was originally defined by Endsley in 1995 to mean that situation awareness is an area that compiles three relevant actions, closely linked to cognitive processes [END95]: (i) the perception of the relevant dynamics of an environment, (ii) the comprehension of their meaning in order to understand its situation, and (iii) the projection of their states in the near future. In this sense, the advantages of using DTs to cover these actions are significantly broad, as their simulation capabilities, in offline and online mode, with high level of fidelity help to describe and localize a problem, and in the best case neutralize it in time. The latter even meets one of the main criteria for critical infrastructure protection [ALC13]. Systems that rely on situational awareness should not only **ensure rapid anticipation and detection of anomalous events, but also provide responses to improve resilience**, feeding back all knowledge to deal with similar threats in the future.

Thus, it is easy to understand that DT-assisted situational awareness comprises aspects already discussed in the last two sections. Nevertheless, we describe here some related work to clarify its current relevance. For example, Eckhart *et al.* detail in [ECK19] that the DT paradigm can be a useful tool for intensifying situational awareness in CPS-based contexts. The authors clearly describe that the use of virtual replicas running in parallel to physical counterparts could help inspection actions and determine anomalous behaviors, risks and threats without disrupting system operational processes. To demonstrate this, the work also proposes a DT-based cyber situational awareness framework (which virtualizes system topology, parameters and device software program variables) in order to provide a holistic picture of the cyber situation of CPSs and detect threats. In [MYL21], the authors provide a study on the relevance of (AI-guided) next-generation industrial immune systems in charge of protecting industrial ecosystems against sophisticated and stealthy cyber-physical attacks, further exploring how situational awareness can be improved by quickly detecting, locating and neutralizing threats.

In addition, technology integration could provide **a deeper understanding of adversaries' actual and realistic attack vectors, tools, and tactics**, enabling greater situational awareness and thus greater resilience and protection to support other related areas such as threat hunting, incident management, and cyber threat intelligence [DIE22]. In turn, these areas could even feed back into the awareness of the DT for further system prevention. This also means that DTs can be able to connect with external entities or other DTs to get a more explicit view of the situation or possible situations in the near future.

5.6. Privacy

As mentioned above, DTs can simulate services, devices, functions and interactions within the infrastructure, as well as interactions with external stakeholders (e.g., for cyber intelligence as discussed in the previous section). To function properly, the use of "real/real or synthetic" data (based on the real) of each asset in the DT is mandatory. Depending on the application domain (e.g. smart vehicles, smart factories, smart cities, etc.), different services and devices are deployed, while new technologies (5G/6G, cloud, AI, Distributed Ledger Technology (DLT), etc.) are starting to emerge with ability to manage multiple types of data (personal data and industrial secrets), maximizing the security risks to such data.

To prevent these risks, DTs can be used to **enhance privacy in such complex environments by integrating and testing all assets** (currently installed in the actual infrastructure as well as technologies planned to be used). This approach will make it possible, for example, to detect anomalies, vulnerabilities and misconfigurations that may jeopardize data privacy. To achieve this (i) multiple tests (e.g., penetration tests) based on different scenarios should be designed and executed; and (ii) adequate data collection/network traffic tools and mechanisms should be in place to properly collect and analyze the data to enable further privacy assessment. Based on the results, appropriate privacy rules can subsequently be designed using different approaches, methodologies and techniques based on the respective privacy metrics. Moreover, the use of DTs allows not only to carry out initial privacy and security testing, but also to permanently define and apply more complex privacy rules, techniques and approaches. This, in turn, helps to identify the best overall approach in a realistic environment, including all the particularities of each infrastructure. In fact, as privacy is mandatory in practically all areas of application, DTs can simulate an infrastructure, including services, data communication, organizational procedures and more.

An example of its use can be the monitoring and control of healthcare ecosystems, which include in vitro diagnostic medical devices (e.g. interconnected peacemakers and defibrillators), interconnected medical devices and life support equipment, wellbeing devices and the IT/OT infrastructure of a hospital. As it was described in Section 5.1, the data transferred throughout the entire healthcare ecosystem hold personal and sensitive information that must be protected to safeguard the privacy of the patients. Developing a DT of such complex and heterogenous ecosystem would allow to explore the vulnerabilities, misconfigurations of network devices and rules, data streams, patient and hospital behavior when connected to the network (e.g. what sites are being visited), etc. More specifically, through the simulation, it is possible to determine possible privacy violations and vulnerabilities that could lead to data leaks and theft not only in network level but also in device level (e.g., to verify the quality of ML models and their level of access to large volumes of data). Based on the findings, various mechanisms, techniques and tools can be tested under a plethora of use cases to evaluate if the privacy risk has been eliminated and the implications that could be introduced. This approach can also lead to privacy by design architecture.

5.7. Training, reskilling and upskilling

A DT can be used as a training tool, for example, for human operators and personnel in high-risk environments and hazardous utilities (e.g. heavy machinery, mines etc.). In this application context, the simulation will include and guide various information flows and processes, all working together to support the learning process, typically applied to understand the operation of a system, its management and its security in terms of safety and cybersecurity.

Indeed, in the field of operation and safety, employees/users can be trained to handle various (cyber-physical) devices, machines, systems, as well as operational processes, without risking their lives or the lives of others by causing an accident or impacting the system. In this way, **simulation-based training will prepare employees/users to handle all types of operational elements that they need to know** in a plethora of scenarios, both for day-to-day operations and for emergency/adverse situations. Moreover, this type of training/learning in highly threatening, dangerous or critical environments will help junior employees/users gain experience, knowledge, skills and competencies in terms of applicability and safety [SIN21], [BEL20]; but also for senior employees/users that need to recycle their knowledge and/or improve their expertise.

In cybersecurity domain, a DT can be used for numerous purposes such as (i) security testing and debugging (ii) products security design validation against simulated cyberattacks (e.g. penetration testing), (iii) detection of misconfigurations, (iv) testing of different settings of the security components that are being deployed in the real environment, and (v) training. Using the DT for training will **allow security experts** (e.g. SOC teams) **to interact with the system functions in offline mode and familiarize themselves with the various security solutions in realistic situations and use cases** [VIE21]. It will also make it possible to model the impacts of attacks/countermeasures on cyber-physical processes [ECK19a], and subsequently avoid major disruptions and future consequences, improving the sustainability and integrity of the entire value chain.

Continuing with the capacity of DT for cybersecurity training, and as stated in [HOL21], DTs can be effective in fostering cybersecurity competencies through hands-on digital exercises and serious games of chance. In this case, aspects related to cyber-range models can be integrated as part of the DT to consolidate competencies, learning and knowledge. Through cyber range, it is possible to implement realistic learning environments based of practical and attractive exercises related to *blue team / red team*, *capture the flag* or *hackathons*.

5.8. Exploring new simulation capacities

In this section, we associate DT technology capabilities for system protection, resilience and cybersecurity with the critical infrastructure protection requirements identified by NIST in [NIST18]. To do so, we group these capabilities according to the five cybersecurity functions given by NIST: **identify, protect, detect, respond, and recover**, and according to this grouping we link the capabilities to the protection requirements.

Table 5. Association of potential contributions of DTs with respect to the measures of defenses proposed by NIST in [NIST 18].

Sec. funct.	Potential contribution of Digital Twins	Support to NIST Categories (with respect to [NIST18])
Identify	• **Identification of (known and unknown) vulnerabilities** of the physical twin as well as possible consequences of their exploitation and corrections	• Asset Management (ID.AM), especially for asset's inventory (ID.AM-1) and prioritization (ID.AM-5) • Risk Assessment (ID.RA), especially for vulnerability's identification and documentation (ID.RA-1)
	• **Evaluation of the possible exploitation** of detected vulnerabilities	• Risk Assessment (ID.RA), especially for the likelihood estimation (ID.RA-4, ID.RA-5)
	• **Analysis of impacts of possible adverse situations** and simulation of **cascading effects**	• Risk Assessment (ID.RA), especially for the business impact estimation (ID.RA-4) • Supply Chain Risk Management (ID.SC), especially for supply chain risk assessment (ID.SC-2)

	• **Assessment of the current cybersecurity controls in place** and gap analysis to analyze the effects of possible improvements before applying them to the real system.	• Business Environment (ID.BE), especially for dependencies among assets and resilience requirements (ID.BE-4, ID.BE-5) • Governance (ID.GV), in general • Risk Assessment (ID.RA), especially for the identification and prioritization of risk responses (ID.RA-6) • Supply Chain Risk Management (ID.SC), especially for recovery testing (ID.SC-5)
Protect	• **Data analysis to proactively identify errors/failures within the system**, e.g., enabling to predict o schedule predictive maintenance (using DT technology) • **Verification and enforcement of privacy and security rules**, involving techniques and approaches to allow the identification of the best approach under a realistic environment	• Data Security (PR.DS), especially to determine the level of quality and integrity of data (e.g., PR.DS-5) and assets (PR.DS-3-4, PR.DS-6, PR.DS-8) • Maintenance (PR.MA) under controlled actions, access (PR.MA-2) and tools (PR.MA-1). • Information Protection Processes and Procedures (PR.IP) through the design of vulnerability management plans (PR.IP-12)
	• Support the secure and correct use of the system by **providing awareness and training capabilities** based on the simulation of the real system	• Awareness and Training (PR.AT), especially for users with access to operating environment (PR.AT-1), and understand their roles and responsibilities with respect to the system (PR.AT-2-5)
	• **Validate the proper functioning of protection/defense tools and policies** (e.g. access control mechanisms), and their adequacy in operating environments	• Protective Technology (PR.PT) and Identity Management Authentication and Access Control (PR.AC), following the principle of least functionality (PR.PT-3) and least privileges (PR.AC-2-4)
	• **Verify the actual status of the system and compliance with best practices and security policies** by comparing what is done in the real world with the virtual world. Therefore, DTs could support the concept of "*continuous governance and compliance*"	• Protective Technology (PR.PT) through logs and audits in concordance with regulatory frameworks (PR.PT-1)
Detect	• **Test and validate new patterns, vectors and attack rules** based on the characteristics of the physical twin • **Test the output of a specific asset** for anomalous behavior (e.g., data leakage)	• Detection activities comply with all applicable requirements, for every sensitive assets (DE.DP-2, DE.DP-3, DE.DP-4), and particular anomaly event (DE.AE-2, DE.AE-3),

	• **Adjust and reenforce existing ML algorithms for early anomaly detection,** e.g., by generating training datasets that simulates normal/anomalous system operations	• DT can improve anomaly detection. The network is monitored to detect potential cybersecurity events (DE.CM-1); Malicious code is detected (DE.CM-3); Unauthorized mobile code is detected (DE.CM-5)
	• **Support deep inspection actions** following the detection of anomalous behavior, risks and threats without disrupting operational processes of the system • **Test and improve the strength of** p(host/network)-based **intrusion detection systems** patterns and rules for cybersecurity events	• Improve post-detection analysis. Incident alert thresholds are established (DE.AE-5); Personnel activity is monitored to detect potential cybersecurity events (DE.CM-3)
	• **Support cyber situational awareness for threat detection** (virtualizing the system topology, parameters and software program variables of devices, or mobile assets) in order to provide a holistic picture on the cyber situation of CPSs	• Roles and responsibilities for detection are well defined to ensure accountability (DE.DP-1); Detection activities comply with all applicable requirements (DE.DP-2); Monitoring for unauthorized personnel, connections, devices, and software is performed (DE.CM-7); Impact of events is determined (DE.AE-4); Vulnerability scans are performed for prevention (DE.AE-4)
	• **Support cyber situational awareness** for response planning and monitoring, **by timely identifying damages and related causes**, while controlling the effect caused by an individual or coordinated false data injection attack, as well as denial of service cyber-attacks, and estimating residual functions • **Support cyber situational awareness** for response planning and monitoring**, by reproducing or predicting complex incidents**, which can guide not only normal monitoring and disaster prevention, but also incident mitigation	• Response plan is executed during or after an incident (RS.RP-1); Notifications from detection systems are investigated (RS.AN-1); The impact of the incident is understood (RS.AN-2); Forensics are performed (RS.AN-3); Incidents are categorized consistent with response plans (RS.AN-4) • Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness (RS.CO-5); Incidents are mitigated (RS.MI-2); Newly identified vulnerabilities are mitigated or documented as accepted risks (RS.MI-3)

Respond	• **Support the establishment of emergency strategies** and avoidance routes • **Identify the agent's role, and categorize the assets and possible attacks** based on the risk assessment analysis	• Personnel know their roles and order of operations when a response is needed (RS.CO-1); incidents are reported consistent with established criteria (RS.CO-2); Information is shared consistent with response plans (RS.CO-3); incidents are contained (RS.MI-1); incidents are mitigated (RS.MI-2); and processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) (RS.AN-5)
	• **Perform interactive optimizations of organizations' processes** under various incident conditions • **Establish controlled upgrading processes** based on the recent discoveries	• Response plans incorporate lessons learned (RS.IM-1); Response strategies are updated (RS.IM-2)
Recover	• **Support cyber situational awareness for recovery planning**, through the provisioning of **realistic understanding for participants throughout the life cycle of a system**, which also includes incidents and disaster periods • **Facilitate the development, testing and maintenance of strategies and plans for disaster recovery**. This particularly applies to critical systems characterized by legacy components and availability constraints (e.g. energy infrastructures), which cannot be easily tested without putting the operational continuity of the infrastructure at risk	• Recovery Planning (RC.RP), supporting actions both during and after a cybersecurity incident (RC.RP-1) • Improvements (RC.IM), recovery strategies are updated (RC.IM-2)
	• **Accelerate/facilitate the recovery processes** in very accurate, high-fidelity way (1) by means of **decisions supported by different degrees of automation**, and (2) by allowing the **correct restore of the pre-incident status and configuration of the physical twin**, which could have been stored and saved in the DT	• Recovery Planning (RC.RP), supporting actions both during and after a cybersecurity incident (RC.RP-1) • Improvements (RC.IM), supporting the update of recovery strategies (RC.IM-2)
	• **Test and validate the actual effectiveness of security patches at a low cost**, without affecting the real system	• Improvements (RC.IM), supporting both the incorporation of lessons learned (RC.IM-1) the update of recovery strategies (RC.IM-2)

From Table 5 we determine that DT is a potentially effective technology, capable of offering multiple and attractive capabilities to not only virtualize and characterize an object or a system for analysis, validation and testing tasks, but also to obtain multiple benefits in terms of security, safety, sustainability and profitability of the value chain. Through simulation (either in offline or online mode), it is possible to offer the incorporation of defensive tools capable of continuously protecting the domains of a system, detecting and responding to potential threats, and, in the worst case, recover by itself from such threats.

6. Best practices and guidelines for practitioners

As noted in [ALC22], the threat surface of DT technology extends considerably due to its ability to connect and interact with the real world, either manually or automatically. In this case, attackers may plan their threats to attack from the physical to virtual space, or from the virtual to physical, in order to exfiltrate sensitive information (e.g., intellectual property, industrial secrets) to external entities, disrupt critical functions of the real system, or destroy resources essential to the real world. In other words, attackers could be primarily interested in (i) reaching the DT to deliberately learn from the nature of the physical twin (e.g., topologies, protocols, conf, etc.), and once known, attack with more sophisticated and advanced attack vectors (e.g., more advanced and persistent threats); or (ii) taking control of the DT to subsequently access and manipulate critical resources deployed in the physical space from the digital space. In either case, the consequences would be disastrous for the organization, responsible for the actual system, and in terms of loss of essential services to the end user or loss of sensitive information that can jeopardize the value chain, the reputation of an organization and its prestige.

A complete taxonomy of attacks to DTs is also found in [ALC22], organized according to the technologies that could be integrated as part of the DT. The taxonomy contemplates attacks against (1) CPS and IIoT, typically deployed in the physical world to feed back information into the DT or receive commands for actuation, (2) computing infrastructures to host the DT resources, such as cloud and edge, (3) virtualization systems, (3) computing techniques and models to manage digital models and their data (e.g., via AI, Big Data), and (4) visualization systems, either HMI or advanced virtual, augmented, mixed or extended reality technologies. To simplify the taxonomy detailed in [ALC22] and summarize the set of attacks that may occur in DT-based environments, we highlight: software attacks (vulnerability exploits and malware), rogue nodes and man-in-the-middle (in terms of IIoT/CPS devices, digital models, virtualization systems, servers), sensitive information extraction, privilege escalation, manipulation (in terms of data, virtual nodes, digital models, knowledge, representation and visualization), denial of service and physical attacks, and privacy leakage. Therefore, it is clear that a DT can be considered a very powerful technology to improve the value chain, but at the same time it can be considered an effective and dangerous attack vector tool for attackers.

To avoid all these attack scenarios and their corresponding impact, we propose in this section a set of recommendations and best practice guidelines to be taken into account in the near future, in order to configure and implement reliable and secure DTs. Considering the cybersecurity framework given by the NIST in [NIST18], Table 6 details the security requirements that both practitioners and IT/OT security experts should consider for secure deployments of DTs.

Table 6. Possible DT-based protection solutions for future deployments

NIST Funct.	NIST cybersecurity requirements for protection	Good practices using DT technology	NIST Code
Identify	Risk Assessment (ID.RA)	• According to the different technologies integrated in the DT, an **analysis of vulnerabilities** to such technologies must be performed • Associated to every threat, a **risk assessment** of every DT block must be performed	ID.RA-1, ID.RA-4
	Supply Chain Risk Management (ID.SC)	• **A supply chain risk assessment** • **Response, recovery planning and testing** with suppliers	ID.SC-2, ID.SC-5
Protect	Identity Management, Authentication and Access Control (PR.AC)	• **Identities** assigned to cyber and physical assets should be **unique and legitimate** • Any **access** to the DT should be **controlled** and protected from internal and external entities • Comply with the **least privilege and least functionality**	PR.AC-1-2-3-4-5-6-7
	Awareness and Training (PR.AT)	• All the **IT and OT operators are awareness of the cybersecurity risks**, and the suitable use of the technology • All the **IT and OT operators are awareness of their roles and responsibilities**, including thirds parties (e.g., providers) and senior executives	PR.AT-1, PR.AT-2-5
	Data security (PR.DS)	• Guarantee **confidentiality** by performing regular stress tests over stored data or database in order to check for weaknesses over encrypted data • Apply **integrity principles/techniques** of security rules/configurations of DTs and their data, and periodically validate all these configurations including those related to privacy • Implement report response **mechanism for information leak** incident, **and proactive actions**	PR.DS-3-4-5-6, PR.DS-8
	Protective Technology (PR.PT)	• As resilience is a relevant element for DT paradigm, **response/recovery measures** must be implemented as part of the technology, in order to achieve resilience	PR.PT-5

		requirements in any type of situation, and for any space of the DT	
Detect	Anomalies and Events (DE.AE)	• **Events generated by DTs** and associated IT platforms should also be **evaluated by SOCs** to discover vulnerabilities, exploits and potential attacks • **DT events must also be correlated to have a better understanding of security issues** occurring between spaces of a DT and within a DT, further supporting situational awareness	DE.AE-2, D.AE-3
	Security Continuous Monitoring (DE.CM)	• IT administrators must **monitor and be aware constantly what occurs within the DT**	DE.CM-1, DE.CM-3
	Detection Processes (DE.DP)	• Ensure suitable **detection in the different spaces of a DT** • Provide adequate detection through continuous testing and validation (in the detection processes). Thus, it is necessary to guarantee **continuous improvement of detection processes**	DE.DP-3-4-5
Respond	Response Planning (RS.RP)	• For DT-based scenarios, a **response plan** is executed during or after an incident	RS.RP-1
	Communications (RS.CO)	• **Any information should be shared internally and externally** with stakeholders, also across a DLT network between federated DTs, and should be consistent with response plan. • Established criteria are required for incident reporting	RS.CO-2-3-4-5
	Analysis (RS.AN)	• Threat **notifications and anomalous events** of DT must always be **under control and investigated** • Through **forensic techniques**, it is possible to recover configurations, data, and preserve evidence for the future • Set up **efficient processes to receive, analyse and respond** to vulnerabilities disclosed	RS.AN-1, RS.AN-2, RS.AN-5
	Mitigation (RS.IM)	• **Incidents** occurring **in DT domains must be contained and mitigated** as well as new vulnerabilities	RS.MI-1-2-3
Recover	Recovery Planning (RC.RP)	• Recovery is a priority security approach for the deployment of DTs. For this reason, during or after a cybersecurity incident in a DT (or in some of its spaces), a **recovery plan** is executed and implemented	RC-RP-1
	Improvements (RC.IM)	• Recovery plans **incorporate lessons learned** for future activities, considering	RC.IM-1-2

		metrics or indicators that will help improve the accuracy of the recovery process and the time of recovery	

From Table 6, it is easy to note that the protection of DTs becomes necessary and mandatory, especially when they are deployed in critical operating environments. However, this table only shows a very simplified part, providing a general overview of possible preventive and corrective solutions. Other authors, such as those in the paper [ALC22], also detail many other possible solutions to be considered in the future, covering protection aspects corresponding to the regulatory level (e.g. the need to implement dynamic risk management systems, software agents working as inspectors, etc.) and to the technical level, contemplating, for example the need to implement trust management solutions, real-time attack traceability, data traceability and auditing, distributed event management systems, cyber-intelligence, continuous but controlled learning and awareness, etc.

7. Recommendations and way forward

As described throughout this ECSO Technical Paper, the DT paradigm is not standardized and is still evolving, as are the underlying technologies and models as well. Based on these technological advancements, DTs will progressively allow to simulate the functioning of increasingly complex systems and environments, from natural ecosystem to urban environments and even the human body. That will disclose unprecedented opportunities to better understand, manage and protect the physical counterparts. However, as DTs gain sophistication and connection with the real world boosting added value, they become more sensitive and increase their security requirements.

Table 7. Association of future recommendations and affected stakeholders

Recommendation / Stakeholder	European Commission / Policy makers	DT users	DT researchers	DT developers	Security providers
R1		X		X	
R2	X	X		X	X
R3	X	X			X
R4		X			X
R5	X				
R6			X	X	
R7		X	X	X	
R8		X	X	X	X
R9		X	X	X	X

This section provides a set of Recommendations (R), for different types of stakeholders, intended as a support while governing the complex and dynamic nature of DTs. They are listed as follows.

- **R1 – Tailor DTs cybersecurity to DT specificities**. DTs widely differ in terms of features, complexity, types of data managed, etc. These differences have an impact on the set of security properties that DT security should aiming at ensuring, and therefore on specific set of controls and solutions which each DT should implement. To show an example: *if the DT processes health data or simulates the functioning of a new turbine, the main security properties to enable would be respectively data privacy and model confidentiality*, which would turn into the adoption

of Privacy Enhancing Technologies (PETs) in the first case, and advanced access controls for the second.

- **R2 – Employ a well-shared and holistic methodology for securing DTs**. As from R1 above, specific solutions and controls to implement depends on DT specificities. On the other hand, the methodology to define, implement and manage DT cybersecurity should be the common ground to ensure that all possible cybersecurity issues are considered. Such a methodology, possibly promoted by regulators, should build on widely accepted security principles (as, for instance, *security by design*) and technologies (e.g., employing AI) and specialize them for DTs by considering DTs reference architectures, components and technologies.
- **R3 – Explore the usage of DTs capabilities to strengthen cybersecurity functions.** As briefly introduced in Section 5, simulation capabilities of DTs could be useful to complement analytics related to cybersecurity functions (i.e. identify, protect, detect, respond and recover). To this regard, further work is needed to better understand the real applicability and the effectiveness of this approach, as well as the constraints, implications and side-effects they could have in specific contexts (e.g. DTs for critical CPS-based critical scenarios).
- **R4 – Where relevant, explore the potential of the computing continuum**. Connecting DTs with processing devices at the edge and across the continuum discloses new opportunities for autonomous systems [FLA22]. A DT running on the edge could improve real-time monitoring and protection, prediction and control capabilities, new possibilities for data transfer. By employing real-time data and machine learning, a DT could continuously self-learn and evolve. The added value of these possibilities should be carefully assessed with respect to the related implementation and maintenance costs.
- **R5 – Link research, policy and regulatory framework concerning Data Spaces to DTs**. As DTs increase in potential and complexity, they are even more able to process and correlate different types of data coming from different domains. Scalable DTs can represent complex systems such as logistics chains, food systems, energy grids, which indeed require cooperation among different organizations. As data sharing is crucial in these interactions, data spaces and DTs will be increasingly correlated. In fact, DTs, being a reproduction as accurate as possible of a real system, represent one of the most advanced applications of the concept of data spaces. Therefore, linking DTs and data spaces at research, policy and regulatory levels.
- **R6 – Research and design lightweight (or "*green*") security approaches that do not collide with the operational requirements of the environment.** Since DTs are applied to improve operational strategies and business models, it is essential to optimize their security, but taking into account the current need to design efficient and lightweight security solutions that do not cause significant overhead in the normal development of a DT itself. Any lack of access to DT data to represent consistent scenarios may change the final decision making with impact on the business model.
- **R7 – Research and design digital models under principles of robustness and trust, and privacy criteria.** DT representations and their connections to the real world to capture the current context and reproduce a real scenario must be based on valid data, consistently protected and shared by trusted entities. This also means that digital models and the overall construction of a DT must be based on trust and least privilege principles capable of handling multiple and heterogeneous logical and physical interactions. This level of protection must not only be supported by data privacy techniques, but also by techniques that safeguard user privacy. Large volumes of data and AI techniques can corrupt this privacy condition, which must be regulated by policies and regulations, and controlled by sophisticated protection and preservation mechanisms.

- **R8 - Research ways to exploit the potential of DT for measuring security properties**. Security is mostly considered a non-functional requirement. A successful effort to devise quantitative security metrics would have potentially disruptive applications, enabling the application of optimization methods to the design of architectures, policies and mechanisms. DTs would play a twofold role in such a scenario: (1) as "generators" of metrics, both when testing new ones to evaluate their realism and usefulness, and at runtime, when they would provide access to the synthetic replica of the inner state of a complex system; (2) as testing grounds to measure the security properties of a system undergoing design or update, allowing even to automate the process of exploring alternative solutions in search of the optimal one.
- **R9** - **Be aware of upcoming technologies and the risks involved**. More research is expected in the future, and before new and emerging technologies adapt or make use of the capabilities of a DT. We refer, in this case, to the risks that quantum may, for example, entail. Quantum attacks may be part of the targets of advanced and future attackers who want to corrupt DT simulations and data.

Table 7 matches the relevance of some of the recommendations identified by stakeholders (mainly from academy and industry), and experts in DT field.

8. References

[AHE21] S. Aheleroff, X. Xu, R. Y. Zhong, Y. Lu, “Digital Twin as a Service (DTaaS) in Industry 4.0: An Architecture Reference Model,” in Advanced Engineering Informatics, Volume 47, 2021, 101225, ISSN 1474-0346, https://doi.org/10.1016/j.aei.2020.101225.

[AIE21] Airbus, "Airbus in Spain," 08 07 2021. [Online]. Available: https://www.airbus.com/company/worldwide-presence/spain.html (accessed 02-2022).

[AKB20] F. Akbarian, E. Fitzgerald, and M. Kihl, “Intrusion Detection in Digital Twins for Industrial Control Systems,” in 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2020, pp. 1–6, doi: 10.23919/SoftCOM50211.2020.9238162.

[ALA17] K. M. Alam and A. El Saddik, "C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems," in IEEE Access, vol. 5, pp. 2050-2062, 2017, doi: 10.1109/ACCESS.2017.2657006.

[ALC13] C. Alcaraz, and J. Lopez, “Wide-Area Situational Awareness for Critical Infrastructure Protection”, IEEE Computer, vol. 46, pp. 30-37, 2013.

[ALC22] C. Alcaraz and J. Lopez, "Digital Twin: A Comprehensive Survey of Security Threats," in IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1475-1503, thirdquarter 2022, doi: 10.1109/COMST.2022.3171465.

[ANG18] Angrish, B. Craver, M. Hasan and B. Starly, "A Case Study for Blockchain in Manufacturing: “FabRec”: A Prototype for Peer-to-Peer Network of Manufacturing Nodes," Procedia Manufacturing, vol. 26, pp. 1180-1192, 2018.

[ANY22] "AnyLogic simulation software," Available online: https://www.anylogic.com/ (accessed 02-2022)

[ANY22a] "Digital Twin," Available online: https://www.ansys.com/en-gb/products/systems/digital-twin (accessed 02-2022).

[AZU22] "Azure Digital Twins," Available online: https://azure.microsoft.com/en-gb/services/digital-twins/ (accessed 02-2022).

[AZU22] "Azure Digital Twins," Available online: https://azure.microsoft.com/en-gb/services/digital-twins/ (accessed 02-2022).

[BAO19] Bao, J.; Guo, D.; Li, J.; Zhang, J. The modelling and operations for the Digital Twin in the context of manufacturing. Ent. Inf. Sys. 2019, 13, 534–556.

[BAR19] B. R. Barricelli, E. Casiraghi and D. Fogli, "A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications," in IEEE Access, vol. 7, pp. 167653-167671, 2019, doi: 10.1109/ACCESS.2019.2953499.

[BEC18] A. Becue, Y. Fourastier, I. Praça, A. Savarit, C. Baron, B. Gradussofs and 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), 2018.

[BEC20] A. Becue, E. Maia, L. Feeken, P. Borchers and I. Praca, "A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future," Applied Sciences, 10(13), pp. 44-82, 2020.

[BEC20a] A. Becue, E. Maia, L. Feeken, P. Borchers and I. Praca, "A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future," Applied Sciences, 10(13), pp. 44-82, 2020.

[BEL20] Beloglazov, I. I., P. A. Petrov, and V. Yu Bazhin. "The concept of digital twins for tech operator training simulator design for mining and processing industry." *chemical industries* 18 (2020): 19.

[BOE21] Boeing, "Boeing 737," 08 07 2021. Available Online: https://www.boeing.com/commercial/737max/ (accessed 02-2022).

[BUL19] Buldakova, T.; Suyatinov, S. Hierarchy of Human Operator Models for Digital Twin. In Proceedings of the 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 8–14 September 2019.

[CAS21] A. Castellani, S. Schmitt and S. Squartini, "Real-World Anomaly Detection by Using Digital Twin Systems and Weakly Supervised Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 4733-4742, July 2021, doi: 10.1109/TII.2020.3019788.

[CPS22] "CPS Twinning," Available online: https://github.com/sbaresearch/cps-twinning (accessed 2022).

[CRE22] "Create Immersive Connections with your Infrastructure Digital Twin," Available online: https://www.imodeljs.org/ (accessed 2022).

[CYB24] Cyberseas, https://cyberseas.eu/, European Project, 2021-2024.

[DAM19] V. Damjanovic-Behrendt and W. Behrendt, "An open-source approach to the design and implementation of Digital Twins for Smart Manufacturing," International Journal of Computer Integrated Manufacturing, vol. 32, 2019.

[DAN21] W. Danilczyk, Y. L. Sun, H. He, Smart grid anomaly detection using a deep learning Digital Twin. In 2020 52nd North American Power Symposium (NAPS), IEEE, pp. 1-6, 2021.

[DIE22] M. Dietz, D. Schlette and G. Pernul, "Harnessing Digital Twin Security Simulations for systematic Cyber Threat Intelligence," 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), 2022, pp. 789-797, doi: 10.1109/COMPSAC54236.2022.00129.

[DTC22] Digital Twin Consortium, Glossary of Digital Twins, 2022. Available online: https://www.digitaltwinconsortium.org/glossary/glossary.html#digital-twin (accessed 02-2022).

[DTC22] Digital Twin Consortium, Available online: https://www.digitaltwinconsortium.org/about-us/, (accessed 2022).

[ECB23] European Central Bank, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html, 2023

[ECK18] M. Eckhart and A. Ekelhart, "A Specification-Based State Replication Approach for Digital Twins", Proceedings of the 2018 workshop on cyber-physical systems security and privacy, p. 36-47, 2018.

[ECK18a] 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, 2018, pp. 61–72, doi: 10.1145/3198458.3198464.

[ECK19] M. Eckhart, A. Ekelhart, E. Weippl, "Enhancing cyber situational awareness for cyber-physical systems through Digital Twins". In 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, pp. 1222-1225, 2019.

[ECK19a] M. Eckhart and A. Ekelhart, "Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook," in Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb, S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, Eds. Cham: Springer International Publishing, 2019, pp. 383–412.

[ECL22] "Eclipse Ditto," Available online: https://www.eclipse.org/ditto/ (accessed 2022).

[ELE22] G. Electric, "GE Digital Twin," 2016. Available online: https://www.ge.com/digital/sites/default/files/download_assets/Digital-Twin-for-the-digital-power-plant-.pdf (accessed 2022).

[END95] R. Endsley, “Toward a theory of situation awareness in dynam- ic systems”, Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 37, issue 33, pp. 32-64, 1995.

[FAC20] "Factoriy I/O Next-Gen PLC Training," Real Games, 2020. Available online: https://realgames.co/ (accessed 2022).

[FLA22] F. Flammini, C. Alcaraz, E. Bellini, S. Marrone, J. Lopez and A. Bondavalli, "Towards Trustworthy Autonomous Systems: Taxonomies and Future Perspectives," in IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2022.3227113, 2022.

[GE22] General Electric, "GE Unveils Real-time, Active Cyber-Defense Solution for Industrial Control Systems called Digital Ghost", 2022, Available online: https://www.ge.com/research/newsroom/ge-unveils-real-time-active-cyber-defense-solution-industrial-control-systems-called (accessed 02-2022).

[GEH20] C. Gehrmann and M. Gunnarsson, "A Digital Twin Based Industrial Automation and Control System Security Architecture," in IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 669-680, Jan. 2020, doi: 10.1109/TII.2019.2938885.

[GRA17] Graessler, I.; Poehler, A. Integration of a Digital Twin as human representation in a scheduling procedure of a cyber-physical production system. In Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 10–13 December 2017.

[GRI14] M. Grieves, “Digital Twin: Manufacturing excellence through virtual factory replication,” White paper, 2014. Available online: https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf

[HAL15] E. Haleplidis, K. Pentikousis, S. Denazis, J. Hadi Salim, D. Meyer, O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", IRTF, 2015. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc7426.txt.pdf (accessed 04-2022).

[HOL21] D. Holmes, M. Papathanasaki, L. Maglaras, M. Ferrag, S. Nepal, H. Janicke, “Digital Twins and Cyber Security–solution or challenge?.” In 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), pp. 1-8, IEEE, 2021.

[IBM22] "Digital Twin: Helping machines tell their story," Available online: https://www.ibm.com/internet-of-things/trending/digital-twin (accessed 02-2022).

[IIC20] Industrial IoT Consortium (IIC), Digital Twins for Industrial Applications, An Industrial Internet Consortium White Paper, Available online: https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf (accessed 2022).

[IIC22] Industrial IoT Consortium (IIC), Available online: https://www.iiconsortium.org (accessed 2022).

[ISO21a] International Standard Organization (ISO), ISO 23247-1:2021, Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles, 2021, Available online: https://www.iso.org/standard/75066.html (accessed 2022).

[ISO21b] International Standard Organization (ISO), ISO 23247-2:2021, Automation systems and integration — Digital twin framework for manufacturing — Part 2: Reference architecture, 2021, Available online: https://www.iso.org/standard/78743.html (accessed 2022).

[ISO22] International Standard Organization (ISO), Available online: https://www.iso.org/about-us.html, (accessed 2022).

[JAR20] A. Jaribion, S. H. Khajavi, M. Öhman, A. Knapen, J. Holmström, “A Digital Twin for safety and risk management: a prototype for a hydrogen high-pressure vessel.” In International Conference on Design Science Research in Information Systems and Technology, Springer, pp. 369-375, 2020.

[JIE20] L. Jiewu, L. Qiang, Y. Shide, J. Jianbo, W. Yan, Z. Chaoyang, Z. Ding, C. Xin, “Digital Twin-driven rapid reconfiguration of the automated manufacturing system via an open architecture model,” Robotics and Computer-Integrated Manufacturing, Volume 63, 2020, 101895, ISSN 0736-5845, https://doi.org/10.1016/j.rcim.2019.101895

[KAR22] Karin, "What is a 3DEXPERIENCE Twin?," 1-07-2019. Available online: https://blogs.3ds.com/exalead/2019/07/01/what-is-3dexperience-digital-twin-part-1-12-2/ (accessed 02-2022).

[KRI18] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, Digital Twin in manufacturing: A categorical literature review and classification, IFAC-PapersOnLine, 51(11), 1016-1022, 2018.

[LIU18] Z. Liu, N. Meyendorf, and N. Mrad, “The role of data fusion in predictive maintenance using Digital Twin,” vol. 1949, p. 020023, 04 2018.

[LOC20] A. Löcklin, M. Müller, T. Jung, N. Jazdi, D. White and M. Weyrich, "Digital Twin for Verification and Validation of Industrial Automation Systems – a Survey," 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2020, pp. 851-858, doi: 10.1109/ETFA46521.2020.9212051.

[MIH22] S. Mihai, M. Yaqoob, D. V. Hung, W. Davis, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, R. V. Prasad, H. Venkataraman, R. Trestian, H. X. Nguyen, "Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects," in *IEEE Communications Surveys & Tutorials*, 2022, doi: 10.1109/COMST.2022.3208773.

[MIN20] R. Minerva, G. M. Lee and N. Crespi, "Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models," in Proceedings of the IEEE, vol. 108, no. 10, pp. 1785-1824, Oct. 2020, doi: 10.1109/JPROC.2020.2998530.

[MOH22] Abubakar Sadiq Mohammed, Neetesh Saxena, and Omer Rana. 2022. Wheels on the Modbus - Attacking ModbusTCP Communications. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22). Association for Computing Machinery, New York, NY, USA, 288–289. https://doi.org/10.1145/3507657.3529654

[MYL21] M. Mylrea, M. Nielsen, J. John, M. Abbaszadeh, Digital Twin Industrial Immune System: AI-driven Cybersecurity for Critical Infrastructures. In Systems Engineering and Artificial Intelligence, Springer, pp. 197-212, 2021.

[NAT20] S. Nativi, B. Delipetrev, M. Craglia, Destination Earth: Survey on “Digital Twins” technologies and activities, in the Green Deal area, EUR 30438 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-25160-6, doi:10.2760/430025, JRC122457, 2020.

[NIST18] National Institute of Standards and Technology (NIST), Cybersecurity Framework, Version 1.1, 2018, Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed 07-2022).

[NIST21] National Institute of Standards and Technology (NIST), Considerations for Digital Twin Technology and Emerging Standards: Draft NISTIR 8356, 2021, Available online: https://www.nist.gov/news-events/news/2021/04/considerations-digital-twin-technology-and-emerging-standards-draft-nistir (accessed 07-2022).

[PRA22] N. H. Praddaude, N. Hogrel, M. Gay, U. Baumann and A. Bécue, “Modelling & Simulation of a Rivet Shaving Process for the Protection of the Aerospace Industry against Cyber Threats”, Proceedings of the 35th annual European Simulation and Modelling Conference, EUROSIS, in press.

[PTC22] "Core PLM Meets IoT and Augmented Reality," Available online: https://www.ptc.com/pt/products/plm/plm-products/windchill (accessed 02-2022).

[QIA22] Qian, C.; Liu, X.; Ripley, C.; Qian, M.; Liang, F.; Yu, W. Digital Twin—Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. Future Internet 2022, 14, 64. https://doi.org/10.3390/fi14020064

[RAG20] Raguvir, S.; Babu, S. Detecting Anomalies in Users –An UEBA Approach. In Proceedings of the International Conference on Industrial Engineering and Operations Managemen, Dubai, United Arab Emirates (UAE), 10–12 March 2020.

[RED19] A. J. H. Redelinghuys, A. H. Basson, and K. Kruger. "A six-layer architecture for the Digital Twin: a manufacturing case study implementation." Journal of Intelligent Manufacturing (2019): 1-20.

[ROE19] M. Roest, "An open source platform for Digital Twins?," 6 05 2019. Available online: https://www.linkedin.com/pulse/open-source-platform-digital-twins-mark-roest/ (accessed 2022).

[SAA20] 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 transactions on smart grid, 11(6), 5138-5150, 2020.

[SDE17] R. Sderberg, K. Wrmefjord, J. S. Carlson, and L. Lindkvist, “Toward a Digital Twin for real-time geometry assurance in individualized production,” Cirp Annals Manufacturing Technology, 2017.

[SEE22] "Seebo Industrial IoT Platform," Available online: https://www.seebo.com/iot-platform/ (accessed 2022).

[SEE22] "Seebo Industrial IoT Platform," Available online: https://www.seebo.com/iot-platform/ (accessed 2022).

[SHI19] S. Shin, "Introduction to mago3D, an Open Source Based Digital Twin Platform," 18 07 2019. Available online: https://pt.slideshare.net/endofcap/introduction-to-mago3d-an-open-source-based-digital-twin-platform (accessed 2022).

[SIE20] "The comprehensive Digital Twin for intralogistics," SIEMENS, 11 03 2020. Available online: https://press.siemens.com/global/en/feature/intralogistics (accessed 2022).

[SIN21] Singh, M.; Fuenmayor, E.; Hinchy, E.P.; Qiao, Y.; Murray, N.; Devine, D. Digital Twin: Origin to Future. *Appl. Syst. Innov.* **2021**, *4*, 36. https://doi.org/10.3390/asi4020036

[SOU19] V. Souza, R. Cruz, W. Silva, S. Lins and V. Lucena, "A Digital Twin Architecture Based on the Industrial Internet of Things Technologies," 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1-2, doi: 10.1109/ICCE.2019.8662081.

[STR18] F. Strohmeier, C. Schranz and G. Güntner, "i-Maintenance: A Digital Twin for Smart Maintenance," 23 10 2018. Available online: https://ercim-news.ercim.eu/en115/special/2095-i-maintenance-a-digital-twin-for-smart-maintenance (accessed 2022).

[TAO17] F. Tao, Y. Cheng, J. Cheng, M. Zhang, W. Xu, and Q. Qi, "Theories and technologies for cyber-physical fusion in Digital Twin shop-floor." CIMS (Computer integrated manufacturing systems), Aug. 2017, v. 23, no. 8, p. 1603-1611.

[VIE21] Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., Pernul, G. (2021). A Digital Twin-Based Cyber Range for SOC Analysts. In: Barker, K., Ghazinour, K. (eds) Data and Applications Security and Privacy XXXV. DBSec 2021. Lecture Notes in Computer Science(), vol 12840. Springer, Cham. https://doi.org/10.1007/978-3-030-81242-3_17

[W3C20] W3C, Digital Twin, Web of Things (WoT) Architecture, 2020. Available online: https://www.w3.org/TR/wot-architecture/ (accessed 2022).

[WAN17] Wang, D.; Chen, J.; Zhao, D.; Dai, F.; Zheng, C.; Wu, X. Monitoring workers’ attention and vigilance in construction activities through a wireless and wearable electroencephalography system. Autom. Constr. 2017, 82, 122–137.

[WAN19] L. Wang and A. M. Canedo, "Human programming interfaces for machine-human interfaces," 2019.

[WAN22] Z. Wang et al., "Mobility Digital Twin: Concept, Architecture, Case Study, and Future Challenges," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2022.3156028.

[WRL22] WRLD3D, Available online: https://www.wrld3d.com/ (accessed 2022).

[WU19] Wu, Mingtao. "Intrusion Detection for Cyber-Physical Attacks in Cyber-Manufacturing System." PhD diss., Syracuse University, 2019. http://dx.doi.org/10.1115/IMECE2019-10135

[WU21] Y. Wu, K. Zhang and Y. Zhang, "Digital Twin Networks: a Survey," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3079510.

[XU21] Q. Xu, S. Ali, T. Yue, Digital Twin-based anomaly detection in cyber-physical systems. In 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST), IEEE, pp. 205-216), 2021.

[Xu21] X. Xu,, Y. Lu, B. Vogel-Heuser, L. Wang, Industry 4.0 and Industry 5.0—Inception, conception and perception. Journal of Manufacturing Systems, 61, 530-535, 2021.

[YUQ20] L. Yuqian, L. Chao, I. W. Kevin, H. Huiyue, X. Xun, “Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues,” Robotics and Computer-Integrated Manufacturing, Volume 61, 2020, 101837, ISSN 0736-5845, https://doi.org/10.1016/j.rcim.2019.101837.

[ZAD16] Van Zadelhoff, M. The Biggest Cybersecurity Threats Are Inside Your Company. 2016. Available online: https: //hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company (accessed 02-2022).

[ZHE18] Y. Zheng, S. Yang, and H. Cheng, “An application framework of Digital Twin and its case study,” Journal of Ambient Intelligence & Humanized Computing, vol. 10, 2018.

[ZHE19] Y. Zheng, S. Yang, and H. Cheng, “An application framework of Digital Twin and its case study.” J Ambient Intell Human Comput 10, 1141–1153 (2019). https://doi.org/10.1007/s12652-018-0911-3

[ZHO21] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor, Q. Wu, M. Boucadair, C. Jacquenet, "Concepts of Digital Twin Network", IRTF, draft-zhou-nmrg-digitaltwin-network-concepts-03, 2021. Available online: https://datatracker.ietf.org/doc/pdf/draft-zhou-nmrg-digitaltwin-network-concepts-03.pdf (accessed 2022).

Acknowledgments

The European Cybersecurity Organisation's (ECSO) WG6 aims to contribute to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. From the analysis of the challenges of digitalisation of the society and industrial sectors this WG identifies what are the capacities and capabilities to sustain EU digital autonomy by developing and fostering trusted technologies.

The following is a special acknowledgement of the active contributions in various capacities from ECSO WG6 members.

EXPERT CONTRIBUTIONS: Cristina Alcaraz (University of Malaga), Alessandro Savini (Deloitte), Andrea Melis (University di Bologna), Adrien Becue (Airbus), Ángel J. Gavín Alarcón (GMV), Andris Soroka (DSS), Costanza Pestarino (ECSO), Csaba Virag (Talgen), David Allison (AIT Austrian Institute of Technology),Dimitris Kavallieros (Information Technologies Institute), Dimitris Lyras (Ulysses Systems), Eduard Hoeberichts (Sandgrain), Francesco Tozzi (Deloitte), Franco Callegati (University of Bologna), Herve Debar (IMT - Telecom-Sud Paris), Isabel Praça (ISEP), Jacques.Kruse-Brandao (SGS), Jeroen Doumen (Sandgrain), Lorenzo Russo (Deloitte), Marco Prandini (University of Bologna), Mario Barile (ENG), Mario Reyes De Los Mozos (Eurecat Centre Tecnològic), Martin Stierle (AIT Austrian Institute of Technology), Matthias Hiller (Fraunhofer-Institut), Paivi Mattila (Laurea University of Applied Sciences), Paolo Roccetti (ENG), Paul Smith (AIT Austrian Institute of Technology), Roberto Cascella (ECSO), Vito Morreale (ENG).