C. Alcaraz and J. Lopez, "Digital Twin Security: A Perspective on Efforts From Standardization Bodies", *IEEE Security & Privacy*, vol. 23, pp. 83-90, 2025.
http://doi.org/10.1109/MSEC.2024.3504193
NICS Lab. Publications: https://www.nics.uma.es/publications

Digital Twin Security: a perspective of efforts from standarization bodies

Cristina Alcaraz and Javier Lopez
Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz, javierlopez}@uma.es

Abstract

Recent technological advancements are causing major changes in the industrial sector, especially with the innovation that Digital Twin (DT) is introducing in terms of anticipating threat situations and predicting risks. Several standardization bodies are doing efforts to propose some standards, norms and best practices. In this context, this paper explores contributions of those bodies in order to analyze whether and how security is prioritized in those proposals in terms of DT protection, classifying the contributions according to the six functions included in NIST Cybersecurity Framework. On the basis of that classification, this research identifies the standardization works that better cover the different security requirements, hence offering higher guarantees of DT protection.

Keywords: Digital Twins, Security, Standarization, Industrial Sector

1 Introduction

Digital transformation and the adaptation of new information technologies have expanded the current ways of creating business in industrial environments, improving their productivity, performance and the operability of systems and components. Among those technologies, the Digital Twin (DT) stands out on its own, capable of representing the digital mirror of a set of physical or virtual assets, processes or facilities, not only simulating scenarios and behaviors, but also estimating states, and anticipating risk conditions and threat situations [1]. This interest is outlined in [2], reporting a relevant investment of $9.9 billion in 2023 with an expected increase of $125.1 billion for 2032. DTs are also on the radar of Gartnet's leading technologies for 2024 [3], positioning it as one of the key emerging technologies for continuous business improvement and decision making. It is evident that there is a special growth in the DT market and a significant demand for the technology, although we cannot overlook some issues of interest. The versatile nature of DT and its multiple formats, protocols and

forms of deployment gives rise to multiple design and development issues that also need to be managed from a general point of view [4].

The current interest in DTs and their applications rely also on international standardization bodies. Through the implication of these bodies it will possible to facilitate the expected adoption of this technology based on a fully standardized approach, compatible with heterogeneous industrial environments. Several organizations have already started the process through various initiatives, either in the form of standards, recommendations or reports. In this paper we focus on documents (final or draft versions) that are available to the general public, produced by the International Organization for Standardization (ISO) [5], the International Electrotechnical Commission (IEC) [5], the Internet Engineering Task Force (IETF) [6], the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [7], the National Institute of Standards and Technology (NIST) [8], and the European Telecommunications Standards Institute (ETSI) [9]. A first overview of the study can be found in Table 1, which not only shows the different contributions by organization, but also how they put their interest in deploying DT technology in particular use cases. Smart cities and manufacturing systems are the most predominant, followed by communication and health. Interestingly, all these application areas address scenarios that are particularly critical, what together with the fact that DT autonomously connects to the real world and is therefore exposed to multiple types of attacks [1], impose that a minimum security and privacy criteria is considered.

Unfortunately, there is no related work that addresses this specific issue questioning the relevance of security for the protection of DT, let alone considering the organizations' vision for this kind of level of protection. There are only a few exploratory works [10, 11] on how standard bodies elaborate on DT technology, though not delving into the security offered. For this reason, this paper analyses which security requirements are key for DT protection. This entails (i) extracting such requirements, and (ii) evaluating the level of relevance by simply assessing the degree to which security has been addressed in standards and norms. In other words, *does the contribution of standarization bodies focus on just few specific security requirements and for one specific area of protection or, on the contrary, on maximizing DT protection?* The first section of the paper details the most recent contributions and their various ways of expressing standardization and best practices, and shows from a general standpoint how security is addressed. This motivates the aim of the second section, which adds the main requirements identified, grouping them in a simplified form in the third section. For this purpose and to facilitate the grouping, the six protection functions of the NIST Cybersecurity Framework (CSF) 2.0 [12] have been taken into account, also making possible to identify the contributions that best extend the security principles by addressing the broader set of CSF-2.0 areas. The final section presents conclusions and outlines future work.

Table 1: Current standardization documents for DTs and main use cases

Standards and reports on DT				Security issues			Use cases							
#	Standarization body	Document	Type of Document	Reference architecture	Cross-layer	Applied to	Manufacturing systems	Energy	Health	Transportation	Communication	Cities and buildings	Security and training	CPS
1	ISO	23247-part 1	S			D, N	✓							
2		23247-part 2	S	✓	✓	D, S	✓							
3		23247-part 3	S				✓							
4		23247-part 4	S			D, N	✓							
5	ISO/IEC	20924:2024	S											
6		30173:2023	S			D, S	✓		✓			✓		
7		30172:2023 (focused on UCs)	TR			D, S, N		✓		✓		✓		
8	IETF	draft-irtf-nmrg-network-digital-twin-arch-08	S	✓	✓	D, S, N					✓		✓	
9		draft-lee-asdf-digital-twin-04	S	✓		D								
10	ITU-T	Y.3090	R	✓	✓	D, S, N					✓		✓	
11		Y.3091	R			D, S					✓		✓	
12		Y.4224	R			D, S, N						✓		
13		Y.4600	R	✓	✓	D						✓		
14		Y.4601	R	✓	✓	D, N						✓		
15		Y.4605	R									✓		
16		Y.4489	R	✓								✓		
17		X.2011	R	✓	✓	D, S, N					✓			
18		Y Suppl. 73 (Y.4600)	R						✓			✓		
19		YSTR.BP-DTw	TR			D, S						✓		
20	NIST	NISTIR 8356	IR			D, S, N		✓	✓	✓				
21		AMS 400.2	AMS			D, S	✓							✓
22	ETSI	GR ZSM 015 V1.1.1	GR			D, N					✓			
23		GR CIM 017 V1.1.1	GR	✓		D			✓	✓		✓		✓
24		TS 103 846 V1.1.1	TS	✓		D, S, N	✓					✓		✓
25		TR 103 844 V1.1.1	TR			D, S, N					✓	✓		✓
26		TS 103 845 V1.1.1	TS			D, S, N	✓	✓	✓	✓				
27		TS 103 828 V1.1.1	TS									✓		

1-4 - Automation systems and integration — digital twin framework for manufacturing; part 1: overview and general principles; part 2: reference architecture; part 3: digital representation of manufacturing elements; part 4 - information exchange; **5** - Internet of Things (IoT) and digital twin – vocabulary; **6** - Digital Twin - concepts and terminology; **7** - Internet of things (loT) - digital twin - use cases; **8** - Network digital twin: concepts and reference architecture; **9** - Extended information of Semantic Definition Format (SDF) for digital twin; **10** - Digital twin network – requirements and architecture; **11** - Digital twin network – Capability levels and evaluation methods; **12** - Requirements for digital twin federation in smart cities and communities; **13** - Requirements and capabilities of a digital twin system for smart cities; **14** - Requirements and capability framework of a digital twin for smart firefighting; **15** - Information exchange model for digital twin federation in smart cities and communities; **16** - Reference architecture of digital twin federation in smart cities and communities; **17** - Security guidelines for digital twin network; **18** - Concept and use cases of a digital twin in smart sustainable cities; **19** - Best practices for graphical digital twins of smart cities; **20** - Considerations for digital twin technology and emerging standards; **21** - use case scenarios for digital twin implementation based on ISO 23247; **22** - Zero-touch network and Service Management (ZSM); network digital twin; **23** - Context Information Management (CIM); feasibility of NGSI-LD for digital twins; **24** - Digital twins: functionalities and communication reference architecture; **25** - Digital twins and standardization opportunities in ETSI; **26** - Digital twins communication requirements; **27** - SAREF: ontology support for urban digital twins and usage guidelines

Type of document: S - Standard, R - Recommendation, TR - Technical Report, TS - Technical Specification, IR - Internal Report, AMS - Advanced Manufacturing Series, GR - Group Report
Security applied to: D - DT Data, S - DT System, N - DT Network

2 DT Standarization

As aforementioned, there is a strong need to standardize DT technology, either through Standards (S), Technical, Group or Internal Reports (TR, GR, IR), Technical Specifications (TS), Advanced Manufacturing Series (AMS) or Recommendations (R), according to the terminology used by different standarization bodies. An overview is shown in Table 1, which includes the most recent documents. Additionally, the table highlights some other aspects of interest as most of these documents offer specific details on the concept of the technology itself and its main components, and some add reference architectures to reflect technological complexity. From the set of reference architectures proposed, we also identify the ones that consider security as a transversal requirement, in which not only the minimum security services are taken into account (such as confidentiality, integrity and availability), but also all those that guarantee an integral protection in the access to and use of the DT.

As a general rule, preventive approaches are distinguished among the existing documents, since security-related issues often apply to specific DT data, such as its digital models, attributes and properties, but also to the DT system, such as the SW-HW infrastructure, and its communication links, what takes us to use the notation Data (D), System (S) and Network (N). Indeed, Table 1 shows that all solutions, with or without cross-layer security, focus mainly on DT data (D), since it is the minimal unit to be processed within a DT, whereas only a few solutions based on cross-layer security address issues related to D, S, and N. This also means that the most complete solutions add security measures that usually run between the multiple layers of design of a DT, considering not only the secure connectivity with the physical counterpart but also the security of the simulation and representation of the final data.

It must be noted that approaches with reference architectures and cross-layer security services are #8, 10, and 17 in Table 1, and all of them focus on communication applications through the virtual representation of physical networks - referred as Network DT (NDT) in #8, and as DT Network (DTN) in #10 and 17. Likewise, there are also documents that do not offer a clear commitment to DT security and privacy, such as #3, 5, 15, 16, 18, and 27, and therefore, with no evident impact on D, S, and N in Table 1. Note also that the latter is in line with the analysis of the requirements detailed in the following section, which are drawn from each of the documents mentioned in Table 1.

3 Security Requirements

Each type of document (S, R, TR, TS, GR, IR, AMS) has been evaluated to extract the main security requirements that organizations consider relevant when standardizing the technology for a given application scenario or approach. It is worth highlighting the ones related to the construction of the technology according to its design based on layers, models and interfaces, but also those related to the use of the technology for specific use cases such as DTN, NDT

or communities, proposing for this last use case the concept of data sharing or DT Federation (DTF). Thus, based on the analysis of the documents, two large groups of security requirements have been established, classified according to the type of protection provided. Specifically, they have been grouped as: (i) basic security requirements, comprising the more essential services for the protection of D, S, and N components, such as confidentiality, integrity, availability, authentication and authorization, accountability, auditing, data traceability, non-repudiation, trust and privacy; and (ii) advanced services, whose contribution adds greater value to the protection of D, S, and N components, such as governance, reliability, monitoring and/or detection, response and recovery (resilience), maintainability, logical protection (in terms of perimeter network and infrastructure), physical protection (safety) and secure coding.

The analysis, reflected in Table 2, shows that most of the current documents include some specific security considerations among their approaches and recommendations. Starting with the group of basic requirements, we note that only a few, such as #7, 8, 10, 17, 20, and 24-26, give some prevalence to certain essential services. The most relevant are those related to access control, including authentication and authorization, followed by confidentiality, integrity and privacy, the latter in terms of data protection (including encryption and anonymization issues) and level of access and consent for correct use. In contrast, documents #8, 17, 20, and 25-26 address the large number of requirements in the advanced group, the most representative being the ones focusing on monitoring, detection and resilience to abnormal events. If in addition we compare these results with some of the most recent related works [1, 13], it is possible to discern a certain consistency of priorities. There is still a particular need to protect and control access to intellectual property, but also the functional status of the digital twin. DTs are critical systems by nature, with autonomy to make decisions on their own and interact with their physical counterparts. Any vulnerabilities, errors or unforeseen events must be detected, managed and mitigated before other effects corrupt the inherent capabilities of the DT and the expected symbiosis with its physical twin [14].

Table 2: Security analysis of current documents for standardization of DTs

	Security priorities for DTs																										
	Basic security requirements											Advanced security requirements									Matching with NIST-CSF 2.0					
#	Confidentiality	Integrity	Availability	Authentication	Authorization	Accountability	Auditing	Data traceability	Non-repudiation	Trust	Privacy	Governance	Reliability	Monitoring or detection	Response	Recovery	Maintainability	Logical protection	Physical protection	Secure coding	Identification	Protection	Detection	Response	Recovery	Governance
1		✓		✓	✓									✓			✓					✓				
2	✓	✓		✓	✓									✓			✓					✓	✓			
3																										
4	✓	✓		✓	✓						✓			✓								✓	✓			
5																										
6				✓	✓						✓	✓										✓				✓
7	✓	✓	✓	✓	✓	✓				✓	✓	✓				✓		✓				✓	✓			✓
8	✓	✓		✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
9					✓																	✓				
10	✓	✓	✓	✓	✓	✓	✓			✓	✓		✓	✓	✓	✓		✓				✓	✓	✓	✓	✓
11	✓			✓	✓						✓		✓		✓	✓						✓				
12				✓	✓	✓																✓				
13	✓										✓											✓				
14											✓			✓	✓			✓				✓	✓	✓		
15																										
16																										
17	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
18																										
19											✓															✓
20	✓	✓	✓	✓	✓			✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓
21	✓	✓		✓	✓																	✓				
22		✓	✓	✓	✓								✓	✓	✓	✓						✓	✓	✓	✓	
23				✓																		✓				
24	✓	✓	✓	✓	✓	✓							✓	✓	✓	✓	✓					✓	✓	✓	✓	
25	✓	✓		✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓
26	✓	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓
27																										

Coverage of CSF 2.0: **green** (4 to 6 functions), **orange** (1 to 3 functions), **red** (no function).

4 Mapping to the NIST Framework

One way to facilitate navigating with the security requirements of Table 2 and distinguish the main protection requirements according to priority criteria is through the use of NIST CSF-2.0 Framework [12]. Each requirement can be linked to one of the security functions and their respective categories established by the framework, resulting in a more simplified manner of encompassing and characterizing basic and advanced security requirements. Specifically, we start with the six protection functions (identification - ID, protection - PR, detection - DE, response - RS, recovery - RC, and governance - GV), and based on the characteristics of the requirements identified in the previous section, we then explore which category of the framework can best match the properties of the requirement. The procedure is completely systematic for each requirement, allowing us to obtain a more general and clearer view of the problem presented in this paper.

After crossing-referencing between requirements and categories, it is possible to identify the most representative CSF-2.0 functions. Specifically, Table 2 shows that the "protection" function is the most representative of the set of the six protection functions of the framework, which is consistent with the most relevant requirements of the set considered as essential or basic, such as authentication, authorization, confidentiality and integrity. Namely, authentication and authorization are directly linked to the category "Identity Management, Authentication and Access Control" (PR.AA in [12]), while confidentiality and integrity fall under "Data Security" (PR.DS in [12]). The same is true for the CSF-2.0 detection, response and recovery functions, which are in turn linked to monitoring and detection, response and recovery for the group of advanced security requirements. Monitoring and detection are associated to "Continuous Monitoring" (DE.CM in [12]), response to "Incident Management" (RS.MA in [12]), and recovery to "Incident Recovery Plan Execution" (RC.RP in [12]). The procedure ends by establishing a color-coded correspondence to visually indicate which standardized documents are the most comprehensive in terms of security and privacy principles, and in accordance with the six CSF-2.0 protection functions. For this purpose, we establish the following quantification criteria: (i) green color illustrates the documents that complete at least four (to six) functions of the CSF-2.0; (ii) orange color for the documents that contain at least one (to three) functions; and (iii) red color the ones that do not consider any function of the CSF-2.0. It can be observed that, on the one hand, #8, 10, 17, 20, 22, and 24-26 are the most outstanding documents in this regard, the majority belonging to ETSI. On the other hand, the results obtained for #17 and 20 are quite consistent with respect to the scope of application of the documents, since both are specific to security. In addition, on comparing Tables 1 and 2, it can be seen that those marked with green color are the most complete with respect to DT data (D), its system (S), and network (N); #8, 10, 17, 20, and 24-26 apply security in the technology's most extended fields of application, in terms of security of the DT data itself, its infrastructure and communication channels.

5 Conclusions

This paper reviews not only the most recent DT standards and existing alternatives (reports, recommendations), but also the highest priority security requirements in those contributions. As a result, two relevant sets of security requirements have been identified, which have been further simplified by considering the NIST CSF-2.0. This procedure, in turn, has allowed us to identify which standards, recommendations and reports provided by standardization bodies cover most of the six areas of the framework and therefore offer the greatest guarantee of protection for the digital twin. This paper also gives an overview of the standardization of technology and its level of security according to priorities and requirements, in addition to introducing a way to group and organize security requirements.

As future work, we will explore in more detail how to approach DT security, though from a more hands-on perspective, taking as a basis the recommendations given by all these analyzed documents and the lessons learned from this study.

REFERENCES

[1] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Communications Surveys & Tutorials*, vol. 24, no. thirdquarter 2022, pp. 1475 – 1503, 2022.

[2] Global Market Insights (GMI), "The NIST Cybersecurity Framework (CSF) 2.0, https://www.gminsights.com/industry-analysis/digital-twin-market." Digital Twin Market Size &, Growth Analysis 2032, 2024.

[3] L. Perri, "30 Emerging Technologies That Will Guide Your Business Decisions, https://www.gartner.com/en/articles/30-emerging-technologies-that-will-guide-your-business-decisions." Gartner, 2024.

[4] J. Voas, P. Mell, and V. Piroumian, "Considerations for Digital Twin Technology and Emerging Standards, https://doi.org/10.6028/NIST.IR.8356-draft." NISTIR 8356, 2024.

[5] ISO/IEC, "International Organization for Standardization/International Electrotechnical Commission, https://www.iso.org," 2024.

[6] IETF, "Internet Engineering Task Force, https://www.ietf.org," 2024.

[7] ITU-T, "International Telecommunication Union Telecommunication Standardization Sector, https://www.itu.int," 2024.

[8] NIST, "National Institutes and Technology, https://www.nist.gov," 2024.

[9] ETSI, "European Telecommunications Standards Institute, https://www.etsi.org," 2024.

[10] W. Sun, W. Ma, Y. Zhou, and Y. Zhang, "An introduction to digital twin standards," *GetMobile: Mobile Computing and Communications*, vol. 26, no. 3, pp. 16–22, 2022.

[11] K. Wang, Y. Wang, Y. Li, X. Fan, S. Xiao, and L. Hu, "A review of the technology standards for enabling digital twin," *Digital Twin*, vol. 2, p. 4, 2022.

[12] NIST, "The NIST Cybersecurity Framework (CSF) 2.0, https://doi.org/10.6028/NIST.CSWP.29," 2024.

[13] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2019.

[14] ITU-T, "Recommendation ITU-T Y.3091 - Digital twin network – Capability levels and evaluation methods." SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3091-202312-I!!PDF-E&type=items, 2023.