ECCO
European Cybersecurity COmmunity

26 April 2024, Webinar

Digital Twins architectures and security capabilities: a Game-Changer for Cybersecurity

Javier Lopez, Cristina Alcaraz
University of Malaga, Spain

Agenda

- Introduction to DT
- DT Architectures
- DTs for the protection of digital systems
- Application of the NIST cybersecurity framework to DT
- Conclusions
- Q&A

Introduction

Introduction

- Evolution of DT as an emerging paradigm, catalysed by:
  - strong need of affordable and accessible simulation environments
  - growing demand for a cost-effective solution to experiment with IT and OT-based infrastructures
  - without the associated operational risks and financial costs

- Definitions of DT:
  - DT Consortium
    - *"a virtual representation of real-world entities and processes, synchronized with specific frequency and fidelity"*
  - W3C
    - *“a virtual representation of a device (or a group of devices) that can be used to run simulations of new applications and services, before they are deployed on real devices”*
  - Others emphasize on concepts like
    - virtual model, digital representation, software-simulation, living model, …

- Mainly composed of two spaces: virtual and physical
  - connected through bidirectional communication links
- Connecting spaces is what differentiates a DT from other correlated simulation systems
  - Digital Model: with manual data flows in both directions
  - Digital Shadow: manual data flows from the virtual space to the physical space
  - Digital Twin: automatic data flows in both directions
  - Digital Twin Predictive: DT with support in the cloud-edge

Source: Aheleroff, S., Xu, X., Zhong, R. Y., & Lu, Y. (2021). "Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model." Advanced Engineering Informatics, 47, 101225.

- Automatic bidirectionality is what makes this technology attractive
- DT simulation capabilities facilitates its use in many applications:
  - specially in those that need to predict risks and anticipate threat situations
    - critical application scenarios (e.g., healthcare, manufacturing, energy)
- Services provided that other technologies alone do not address:

  - predictive maintenance
  - real-time monitoring
  - remote control
  - process optimization
  - safety management
  - failure analysis and tracking
  - strategy evaluation
  - health monitoring
  - management of risks
  - training
  - cybersecurity

• Advantages provided by DTs:

- Troubleshoot incidents in the operational target entity
- Reduce the need for on-site attention
- Lower the operating costs of assets and services
- Build competitive advantage and export potential
- Accelerate productivity dividends
- Unlock value across industries and across supply chains
- Bring different industries, functions, and concepts together
- Enhance transparency, accountability, and trust
- Reduce risk in project and programme delivery

Source: ISO/IEC 30173:2023

- Automatic bidirectionality also allows DTs to make decisions autonomously and operate accordingly
  - Because of this autonomy, the construction of a DT entails the consideration of other technologies – IA/ML, edge/cloud, blockchain, etc.
    - altogether can explain the benefit of the business model, production, and value chain
    - *"The global DT market is expected to be worth USD 110.1 billion by 2028, growing at a CAGR of 61,3% during the forescast period"*

Source: Market and Market, Digitat Twin Market, 2024, https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html?gad_source=1&gclid=Cj0KCQjw8pKxBhD_ARIsAPrG45nAn2hPqvu-JUuLXaBi2Z5fl1W2cJme0W3huMjpi3jY1BKOLZ7Z700aAjc-EALw_wcB

- Obviously, the impact of DTs has attracted the attention of many international organizations
  - Consortia and associations are emerging to give response to current needs.
  - For instance, *Digital Twin Consortium*
    - Collaborative partnership with industry, academia, and government expertise
    - Dedicated to the overall development of DTs.
      - It drives the awareness, adoption, interoperability, and development of DT technology.
  - Also, *Industry IoT Consortium*
    - More verticalized on IoT issues for Industrial Applications
    - Covering aspects related to:

      (i) characteristics of a DT
      (ii) business value added by the DT
      (iii) internal design of the DT
      (iv) examples of the use in various industries
      (v) relationships between DTs to form composite systems

- Also standardization organizations are being involved in the standardization of reference architectures and in its enabling technologies (NIST, ISO, IRTF)

- NIST published *”Considerations for Digital Twin Technology and Emerging Standards”*
  - The report includes:
    (i) motivation and vision for DT use, (ii) common low-level operations,
    (iii) use cases
  - Also analyses novel <u>cybersecurity</u> challenges arising from the use of DT architectures

- Indeed, DTs are systems in themselves that can be adapted to multiple use cases
  - Precisely, this aspect is also shown by ISO/IEC in ISO/IEC TR 30172, and for various fields of application

- Manufacturing
- Energy
- Urban
- Healthcare
- Prototyping
- Community
- Supply Chain
- General scenario

Most relevant domain according to the standard

- Building/construction
- Urban
- Energy
- Power grid
- Transport

Most relevant domain according to the standard

Source: ISO/IEC TR 30172

Use case: Smart Mobility

- Authors in “*Mobility Digital Twin: Concept, Architecture, Case Study, and Future Challenges*” present **Mobility DT**
  - It aims to **improve driving on the road**

- It uses an AI-based data-driven cloud–edge–device framework (supported by AWS) for mobility services that simulates and represents:
  - Human ➔ Human DT with user management and driver type classification
  - Vehicle ➔ Vehicle DT with cloud-based advanced driver assistance system
  - Traffic ➔ Traffic DT flow monitoring and variable speed limit

Source: Z. Wang *et al.*, "Mobility Digital Twin: Concept, Architecture, Case Study, and Future Challenges," in *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17452-17467, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3156028

Use case: Smart Factory

- The **CyberFactory#1 Project** provides a DT to strengthen "***Factories of the Future***" under the Industry 4.0 conceptualization and considering the Airbus Cyber-Range platform
  - Supporting especially the implementation of security in the design, commissioning, and execution stages of an industrial digitization program

- The Project applies the DT in three use cases:
  - Roboshave: Connection to a robotic arm to improve traceability, monitoring and maintenance of processes
  - Autoclave: Real-time monitoring and automation of quality processes for curing and forming of composite parts
  - Gap Gun: Automation of data acquisition with centralised data storage and the possibility of data analysis

Source: ISO/IEC TR 30172
Source: https://itea4.org/project/cyberfactory-1.html

Use case: Smart Construction

- Within the ISO/IEC TR 30172, we can find the **COGITO EU Project**
  - It uses the DT to guide, monitor and optimize **real building constructions**

- Particularly, this DT aims to:
  - Control the quality of the work performed
  - Predict physical risks and reducing/ avoiding accidents
  - Provide contextualized infrastructure health
  - Guarantee safety training

Source: ISO/IEC TR 30172
Source: https://cogito-project.eu

Use case: Smart Energy and Power Grids

- **Network Digital Twin Project**
  - gives a clear overview of the status of electrical equipment and substations deployed in Catalonia, Andalusia, Aragon, the Canary Islands, the Balearic Islands and Extremadura
  - provides preventive maintenance in order to identify potential operational risks
- Aims to digitise:
  - 144000 distribution centres
  - 90000 kilometres of high and medium voltage overhead lines
  - 1311 substations
  - investment of 40 million euros

Source: ENDESA, https://www.endesa.com/es/prensa/sala-de-prensa/noticias/transicion-energetica/redes-inteligentes/endesa-despliega-50-equipos-especializados-una-inversion-40-millones-euros-crear-gemelo-digital-red-distribucion
Source: Smart Energy, "Endesa launches distribution network digital twin project", August 2023, https://www.smart-energy.com/regional-news/europe-uk/endesa-launches-distribution-network-digital-twin-project/

DT Architectures

- Several architectures and frameworks have been defined with the aim of fostering the development of specific DT solutions
- Most of solutions present common features:
  - Architectures based on layers or levels of functionality
  - Highly related to technologies, such as
    - IoT/IIoT
    - Cloud-edge
    - AI/ML models
    - Visualization systems
  - Requirements for synchronisation, accuracy and reliability
- Security is unfortunately not the current trend
  - But it is considered an essential requirement

- We can find standards and proposals in review process from standarization bodies:
  - ISO
  - IEC
  - IETF/IRTF
  - ITU
- But also several academia, and commercial and open-source solutions

ISO Technical Committee 184

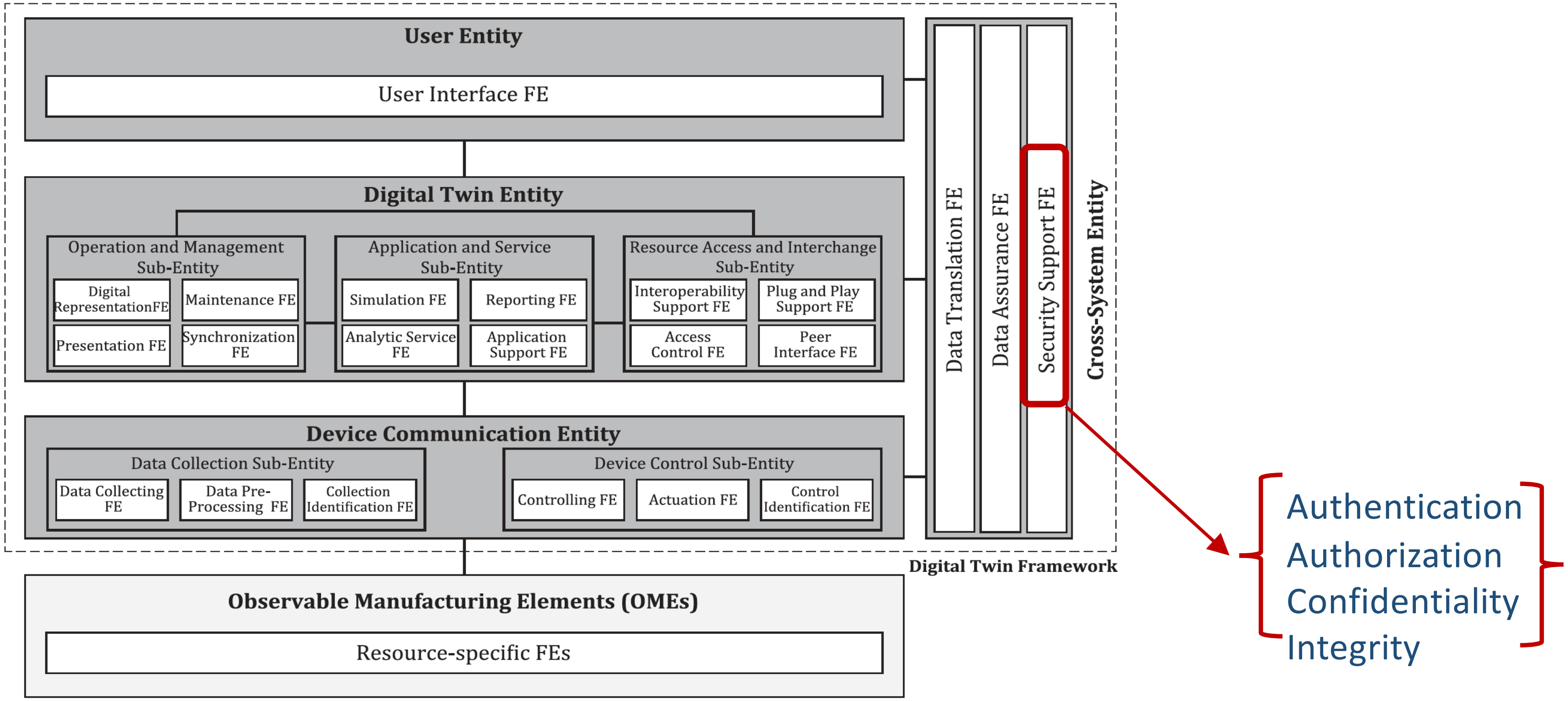
- Sub Committee 4 (Industrial Data) has created the standard ISO 23247
  - Defines a DT framework for manufacturing that supports the creation of DTs of *Observable Manufacturing Elements (OMEs) – the physical counterparts*

- Actually, ISO 23247 is a series of standards and, because of its scope, mainly focus on IoT technology
  - *Part 1: Overview and general principles*
  - *Part 2: Reference architecture*
  - *Part 3: Digital representation of manufacturing elements*
  - *Part 4: Information Exchange*
  - *Part 5: Digital thread for digital twin*
  - *Part 6: Digital twin composition*

under development

Source: ISO 23247, Automation systems and integration Digital twin framework for manufacturing, https://www.iso.org/es

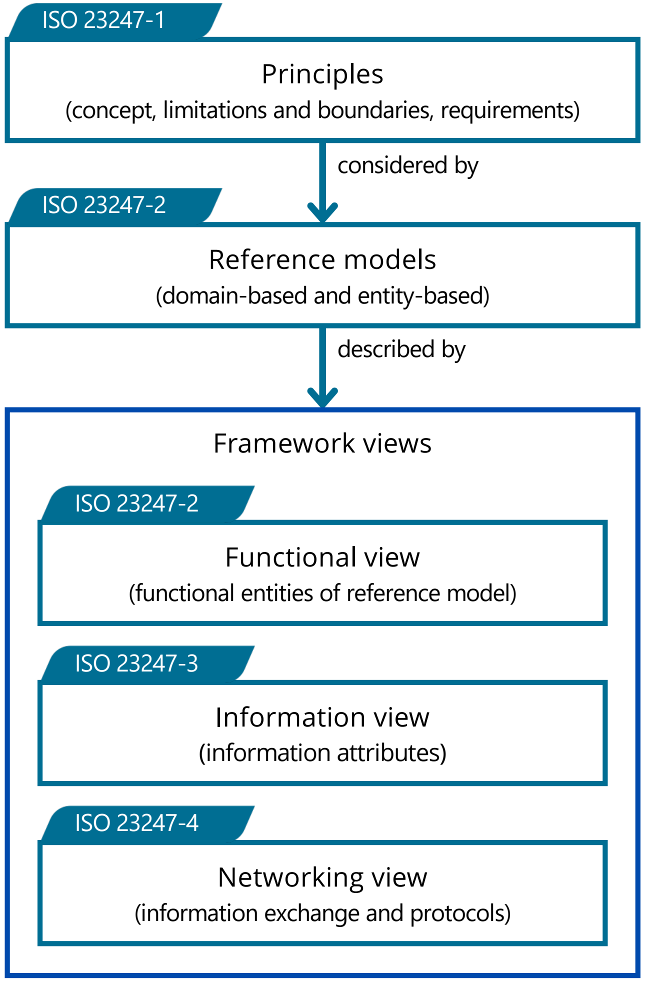
- Part 2 includes the entity-based reference model
  - It includes **the functional view of the architecture**



Source: ISO 23247, Automation systems and integration Digital twin framework for manufacturing, Part 2: Reference architecture, https://www.iso.org/standard/78743.html
Source: http://ap238.org/iso23247/

- Part 3 provides a list of basic information attributes for the OMEs, such as:
  - *personnel*
  - *equipment*
  - *material*
  - *process*
  - *facility*
  - *environment*
  - *supporting documents*

- Part 4 defines a networking view, that is, the four types of communication networks used to connect the entities:
  - *user network*
  - *service network*
  - *access network*
  - *proximity network*



Source: ISO 23247, Automation systems and integration Digital twin framework for manufacturing, https://www.iso.org/es

ISO/IEC JTC 1/SC41

- SubCommittee 41 (Internet of Things and Digital Twin)
  - Working Group 6 undertakes the development of horizontal standards for DT foundational standards, and has created:
    - ISO/IEC 20924: Internet of Things (IoT) and digital twin – Vocabulary
    - ISO/IEC 30173: Digital Twin - Concepts and terminology
    - ISO/IEC 30172: Internet of Things - Digital Twin – Use cases
    - and under development:
      - ISO/IEC 30188: Digital Twin – Reference architecture
      - ISO/IEC 30186: Digital Twin – Maturity model and guidance for a maturity assessment
      - ISO/IEC 30194: Internet of Things (IoT) and Digital Twin - Best practices for use case projects

Source: ISO/IEC JTC 1/SC41, Internet of Things and Digital Twin, https://www.iso.org/committee/6483279.html

- The purpose of ISO/IEC 30173 is to provide:
  - a common basis for understanding the concept and composition of a DT through definitions of DT-related concepts
  - an overview of the life cycle of a DT in relation to the target entity it represents
  - a basis for the development of standards, specifications and use of DTs

Source: ISO/IEC JTC 1/SC41, Internet of Things and Digital Twin, https://www.iso.org/committee/6483279.html

- ISO/IEC 30172 provides a collection of representative use cases of DT applications
  - Intended to be applicable to all types of organizations (commercial enterprises, government agencies, non-for-profit organizations), hence covering a variety of domains:

    - building and construction
    - urban
    - energy
    - healthcare
    - manufacturing
    - home appliance
    - mining
    - telecommunications
    - aerospace
    - marine
    - environmental monitoring
    - transport

Source: ISO/IEC JTC 1/SC41, Internet of Things and Digital Twin, https://www.iso.org/committee/6483279.html

ISO/IEC JTC 1/SC27

- SC 27 develops standards through its five working groups:
  - WG 1 – Information security management systems
  - WG 2 – Cryptography and Security Mechanisms
  - WG 3 – Security Evaluation, Testing and Specification
  - WG 4 – Security Controls and Services
  - WG 5 – Identity Management and Privacy Technologies
- Also involved in two joint working groups:
  - JWG 4 with ISO/TC 307 - Security, privacy and identity for Blockchain and DLT
  - JWG 6 with ISO/TC 22/SC 32 Cybersecurity requirements and evaluation activities for connected vehicle devices

ISO/IEC JTC 1/SC27, Information security, cybersecurity and privacy protection, https://www.iso.org/committee/45306.html

- It is precisely WG5 that is working on a new report:
  - “Security and Privacy of digital twins”
- The report provides:
  - a landscape on standards that can have an impact on security and privacy of DTs
    - those previously shown plus ITU ones
  - investigates stakeholders concerns
  - discusses gaps and recommendations

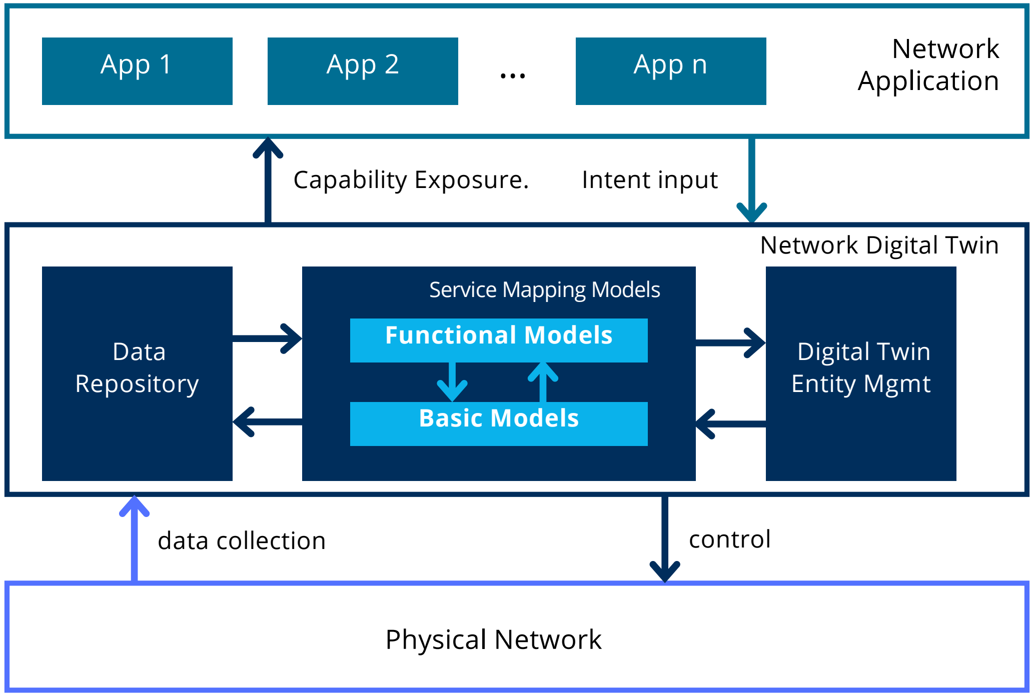
ISO/IEC JTC 1/SC27, Information security, cybersecurity and privacy protection, https://www.iso.org/committee/45306.html

- The document claims to provide a high level analysis of security and privacy of DTs
- However, it is mainly based on an academic survey paper:
  - *"A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects"*
  - focusing on IoDT scenario without exploring other existing related work
- The IoDT-based approach is based on two communication levels:
  - *Intra-twin communication*
  - *Inter-twin communication in the cloud*

Source: Wang, Yuntao, et al. "A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects." *IEEE Internet of Things Journal* (2023).

IETF

- *"Network Digital Twin: Concepts and Reference Architecture"*
  - DTs enhance the use of network applications and their management
    - Ensure network maintenance
      - by assessment of risks and effectiveness of services
    - E.g. useful for 6G-based ecosystems
    - Security considerations include:
      - Secure the digital twin system itself
      - Data privacy protection



Source: IETF, Network Digital Twin: Concepts and Reference Architecture, 2024, https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/

- *“Performance-Oriented Digital Twins for Packet and Optical Networks”*
  - Includes network DT architecture and interfaces to later detail the performance features and how to estimate them
  - For packet networks: Delay, jitter, loss, traffic demand, routing, etc.
  - For optical networks:Topology, status, etc.
- *“Functional Design Aspects of Performance-Oriented Digital Twins”*
  - Does not look at details of models or interfaces but rather at general aspects of functional design
  - Several functional design principles are considered that may apply generically to PODTs
- *“Extended information of Semantic Definition Format (SDF) for DT”*
  - Specifies the interactions and information that can be exchanged between physical and virtual objects
    - such as namespaces and location information during their interactions
    - location information attributes: Location, Type, Target, Description, Label, Property

Source: IETF, Performance-Oriented Digital Twins for Packet and Optical Networks, 2024, https://datatracker.ietf.org/doc/draft-paillisse-nmrg-performance-digital-twin/
Source: IETF, Functional Design Aspects of Performance-Oriented Digital Twins, 2023, https://datatracker.ietf.org/doc/draft-janz-nmrg-performance-digital-twin/
Source: IETF, Extended information of Semantic Definition Format (SDF) for Digital Twin, 2024, https://www.ietf.org/archive/id/draft-lee-asdf-digital-twin-01.html

Other DT reference models – Academia proposals

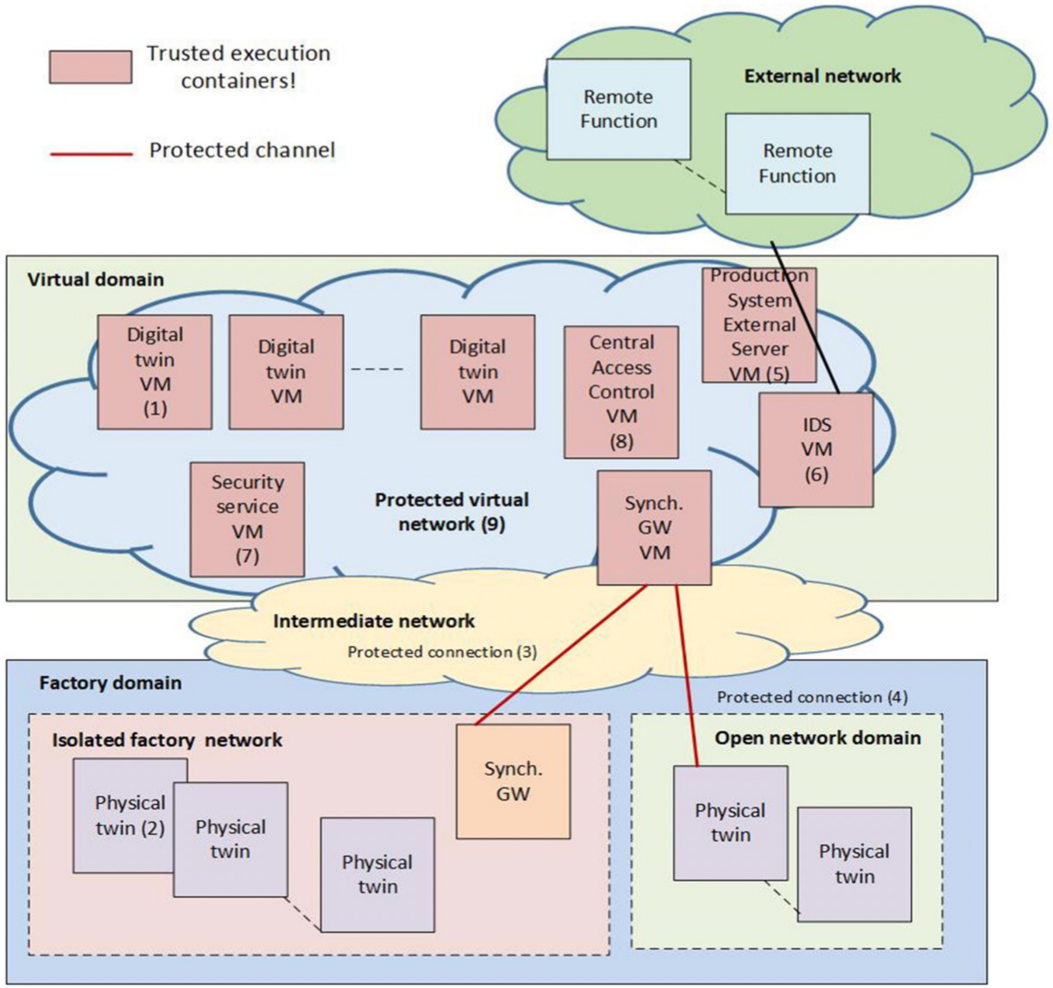
- A number of scientific contributions have arisen in the past few years

- These contributions have in common the layered approach of the architecture
  - The application of the main components is tailored to specific needs
    - For example, for Industry 4.0

Source: Aheleroff, S., Xu, X., Zhong, R. Y., & Lu, Y. (2021). “Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model.” Advanced Engineering Informatics, 47, 101225.

- DT model integrating security services for ICSs

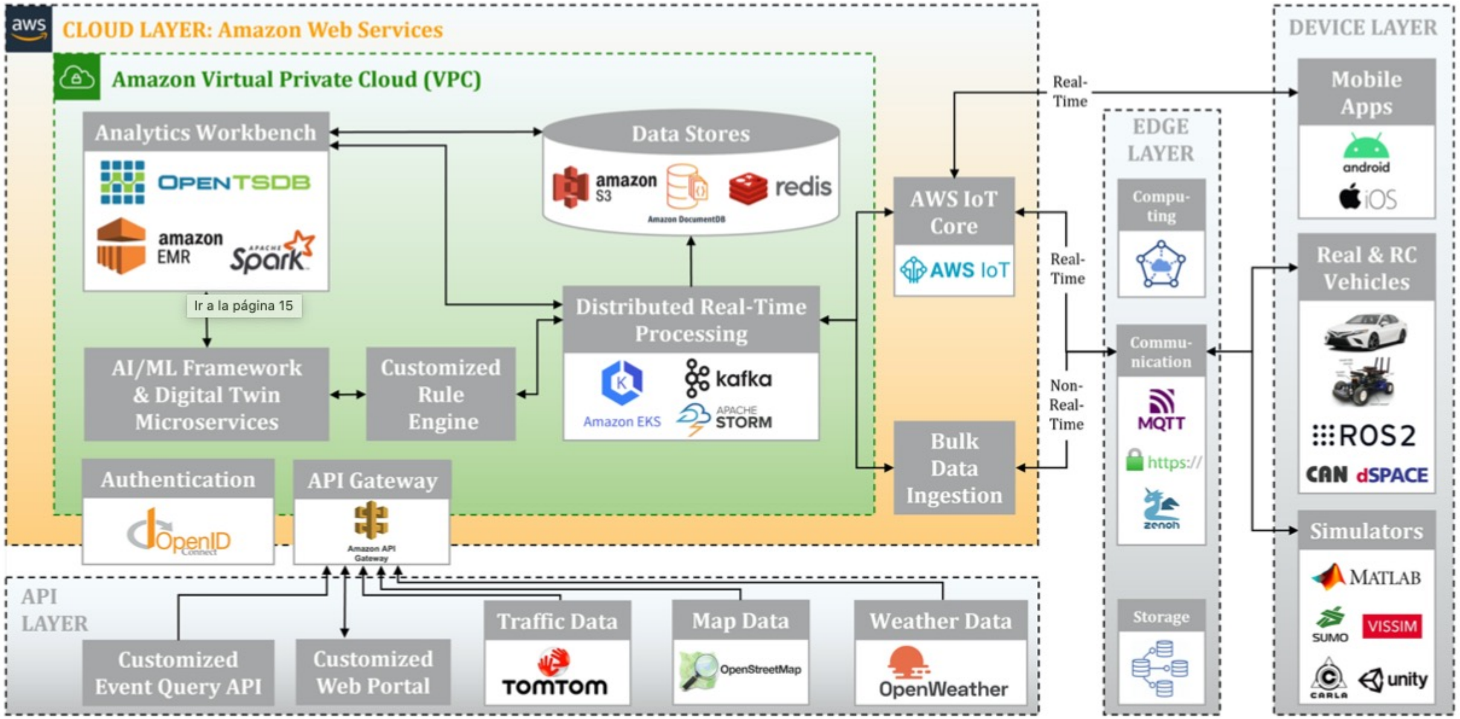
- Design-based security requirements are identified, such as:
  - Synchronization
  - Protection with respect to external connections
  - Access control
  - Software security
  - Network isolation
  - Resilience against DoS



Source: Gehrmann, Christian, and Martin Gunnarsson. "A digital twin based industrial automation and control system security architecture." IEEE Transactions on Industrial Informatics 16.1 (2019): 669-680.

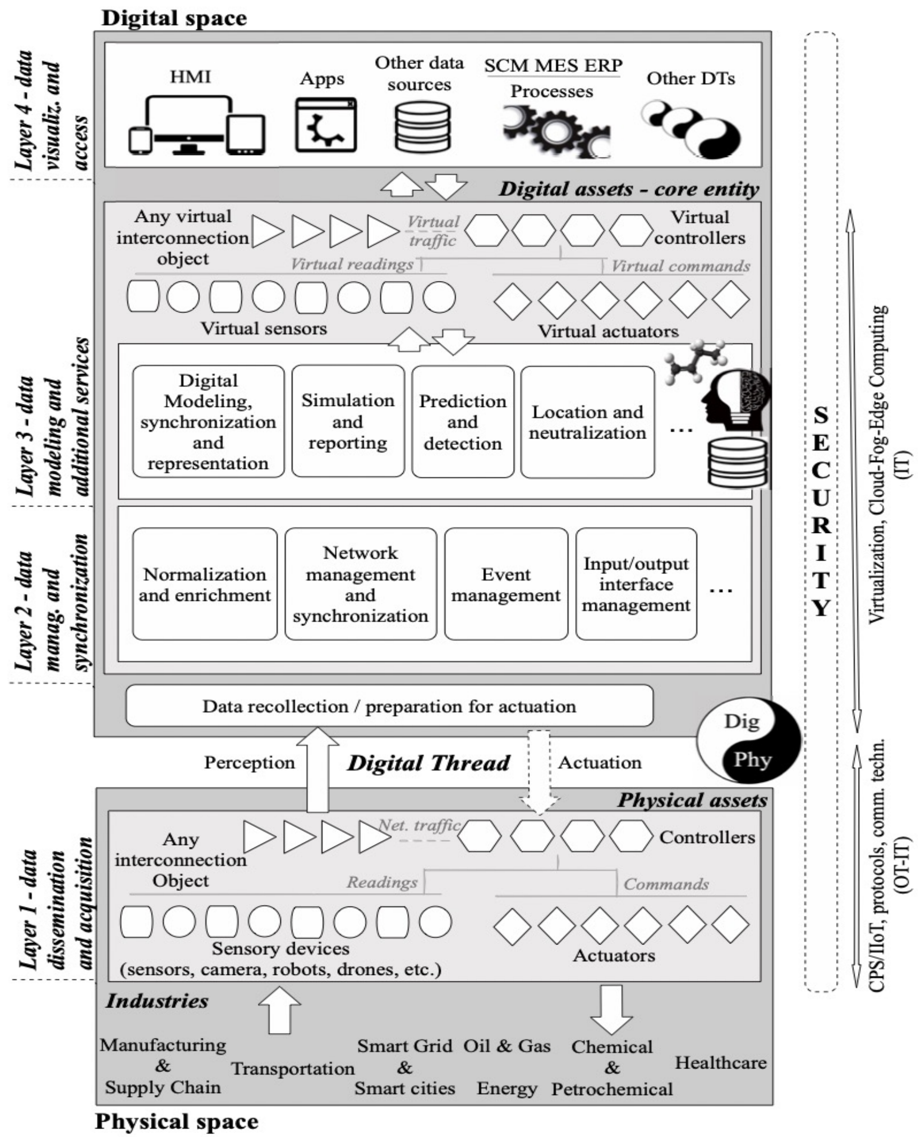
ECCO
European Cybersecurity COmmunity

- Field of vehicles (Mobility DT, previously mentioned as use case)
  - architecture supported in AWS
  - resulting in an *AI-based data-driven cloud–edge–device framework*



Source: Z. Wang *et al.*, "Mobility Digital Twin: Concept, Architecture, Case Study, and Future Challenges," in *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17452-17467, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3156028

- Layer-based DT model with transversal security
- Security recommendations are provided to create trustworthy simulation environments, such as:
  - Hardware and software security
  - Hardening of DT infrastructures and decoupling
  - Identity, authentication and authorization
  - Deception, intrusion detection and situational awareness
  - Response and recovery
  - Event management and information sharing
  - Trust management and privacy
  - Governance and security management
  - Traceability, auditing and accountability
  - Training and human aspects



Source: Alcaraz, Cristina, and Javier Lopez. "Digital twin: A comprehensive survey of security threats." *IEEE Communications Surveys & Tutorials* 24.3 (2022): 1475-1503.

Other DT reference models – Commercial solutions

- Few proprietary software solutions implementing DT technology, developed mainly by large companies in the manufacturing sector
  - But also some open-source software solutions are now available

Commercial solutions to implement DTs, vendors	Open-sources solutions to implement DTs
DT solution, General Electric (GE)	**CPS Twinning**
PTC Windchill, PTC	**Wrld3d**
3DS, Dassault Systèmes	**Mago3D**
DT solution, Seebo	**i-Maintenance**
Simulation Modeling SW tools and solutions, Anylogic	**Eclipse Ditto**
DT solution, Ansys	**imodel.js**
DT framework, IBM	…
IoT service, Microsoft Azure Digital Twin Software	
Factory I/O, Real Games	
SW development services to build DT solutions, Siemens	
…	

- *General Electric* provides DT models for power components to predict health statuses, reliability and performance

- The DT models are integrated as part of the Predix platform
  - A secure IIoT and cloud-based environment capable of processing large data volume and predicting situations through analytics
  - Predix also assesses system gaps, detects vulnerabilities, and protects the critical infrastructure and controls in compliance with cybersecurity regulations

Source: 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 2024).

- *Ansys* provides Ansys Digital Twins
  - A cloud-supported platform for developing and validating approaches, integrating a multi-domain system modeller
  - The platform:
    - facilitates real-time data connection through IIoT devices
    - automates the creation of code, compatible with web applications, Python applications and containers
    - and other multiple features

Source: https://www.ansys.com/content/dam/amp/2023/november/asset-creation/ansys-digital-twins-technical-datasheet-20231102.pdf
Source: Ansys, "Ansys Digital Twins," 2024.
Available online: https://www.ansys.com/en-gb/products/systems/digital-twin (accessed 2024).

Other DT reference models – open-source solutions

- CPS Twinning is a framework capable of generating and executing DTs of
  cyber-physical components
  - Generates virtual environments
  - Applies standardized format based on AutomationML (AML)
  - The solution is available at Github: https://github.com/sbaresearch/cps-twinning

Source: Eckhart, Matthias, and Andreas Ekelhart. "Securing cyber-physical systems through digital twins." *Ercim News* 115 (2018): 22-23.

DTs for the protection of digital systems

DTs for the protection of digital systems

- Already mentioned: *DT is a technology capable of optimizing processes, predicting failures, and detecting anomalous situations*

- But, if capabilities for cybersecurity are considered, then it would be possible to prevent and mitigate potential cyber-attacks (e.g. APTs)
  - abilities of the paradigm can cover a number of cybersecurity challenges
    - model threats, test security requirements, detect and mitigate situations
  - can increase an organization's situational awareness
    - better picture of the situation in terms of vulnerabilities, potential exploits and risks
  - as for Industry 4.0/5.0, create more secure and resilient digital ecosystems
    - reducing potential risks that can affect the quality and welfare of strategic infrastructures

- Indeed, DTs are potentially valuable assets for cybersecurity solutions, 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 behaviour 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)
- training to improve awareness and knowledge of cybersecurity and resilience

- However, DT attack surface may be large and significant for many of the ecosystems and infrastructures based on DTs

- And still not enough research and work done
  - For instance, lack of protection of DT devices
    - e.g.: configurations, IP, property industrial protocols, connections, etc.
  - Also, multiple security problems to solve at:
    - IT level (risks to confidentiality, data integrity and data availability) – cyber world
    - OT level (risks to operational availability and data integrity) – physical world
    - communication level
  - Moreover, DT-driven cybersecurity functions should not collide and impact operational tasks of their physical counterpart

- Therefore, it seems strongly necessary to explore the untapped potential of DTs beyond their conventional use

- Two different perspectives of interest:
  - Harnessing the power of DTs for protection of critical systems
  - Navigating the challenges of deploying this technology from a secure standpoint

- How to do both in a more systematic way than done until now?

Application of the NIST cybersecurity framework to DT

NIST Cybersecurity Framework

- Focus on v1.1
  - V2.0 published in February 2024, including governance as a transversal layer
- Both frameworks include five relevant cybersecurity ”functions”
  - Each function comprises a set of security categories that classify the security actions
- Provides a high-level abstraction of the cybersecurity lifecycle and a common language that facilitates
  - adaptability of technologies
  - and lifecycle phases of systems, sectors and users

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018
Source: NIST, NIST Cybersecurity Framework, CSF 2.0, NIST CSWP 29, 2024, https://doi.org/10.6028/NIST.CSWP.29

- Minimal differences between approaches and versions, but enough to generate a new version,
  - with a more simplified version
  - and an additional security function in Governance
- But in essence, both approaches retain the same objectives and main focuses

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018
Source: NIST, NIST Cybersecurity Framework, CSF 2.0, NIST CSWP 29, 2024, https://doi.org/10.6028/NIST.CSWP.29

- Both versions maintain the use of identifiers, which have also been taken into account for our analysis

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018
Source: NIST, NIST Cybersecurity Framework, CSF 2.0, NIST CSWP 29, 2024, https://doi.org/10.6028/NIST.CSWP.29

- The following is a visual indication of "how" the NIST framework (v1.1) can be interpreted:
  - For simplicity, we will consider (in this talk) the function "PROTECTION"

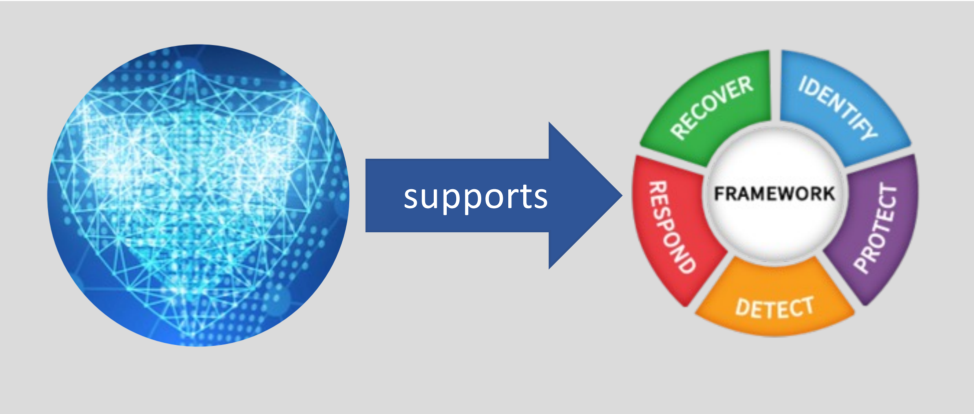
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Perspective 1

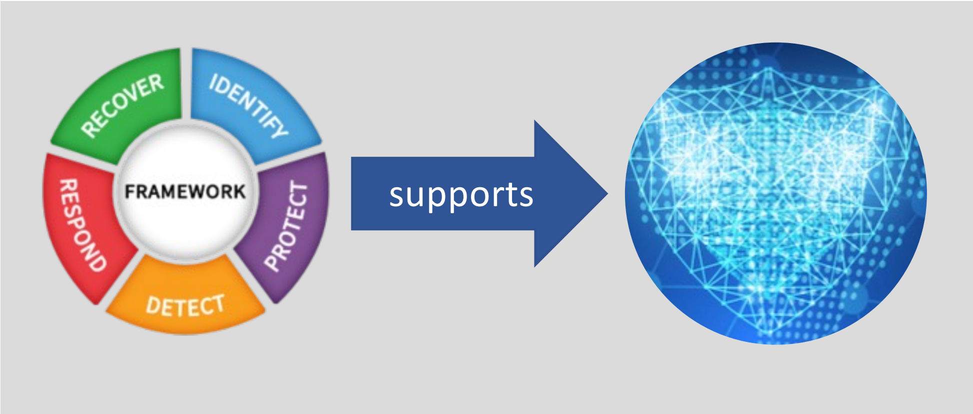
How to use DT to support NIST categories



- How to apply the DT to enable compliance with security conditions set by the framework

Perspective 2

How NIST categories are aligned with DT protection



- How to apply the framework to enable compliance with security conditions and indirectly protect the DT

Figure source: Vecteezy.com
Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Perspective 1: How to use DT to support NIST categories

ECCO European Cybersecurity COmmunity

Identify	Protect	Detect	Respond	Recover
- Identify (known and unknown) vulnerabilities - Evaluate possible exploitations of vulnerabilities - Analysis the impact of possible adverse situations and cascading effects - Assess the current cybersecurity controls in place and determine the possible gaps and improvements	- Analysis data to proactively identify errors/failures within the system - Verify and enforce privacy and security rules - Support the correct use of the system by providing awareness and training capabilities - Validate the proper functioning of protection/defence tools and policies - Verify the actual status of the system and compliance with best practices and security policies	- Test and validate new patterns, vectors and attack rules - Test the output of a specific asset for anomalous behaviour - Adjust and reenforce existing ML algorithms for early anomaly detection - Support deep inspection actions - Test and improve the strength of host/network-based intrusion detection systems patterns and rules - Support cyber situational awareness for threat detection	- Establish a response and monitoring plan, by (1) timely identifying damages and related cause, and (2) reproducing or predicting complex incidents - Support the establishment of emergency strategies - Identify the agents' role, and categorize the assets and possible attacks - Perform interactive optimizations of organizations' processes under various incident conditions - Establish controlled upgrading processes based on the recent discoveries	- Establish a recovery plan through a realistic understanding of the entire lifecycle of a system - Facilitate the development, testing and maintenance of strategies and plans for disaster recovery - Accelerate/facilitate the automated recovery processes - Test and validate the actual effectiveness of security patches at a low cost

The protection of **the entire system and its data** is transversal to these five security functions

NIST Framework Version 1.1
The Cybersecurity Framework

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Perspective 1: How to use DT to support NIST categories

Identify	Protect	Detect	Respond	Recover	The protection of **the entire system and its data** is transversal to these five security functions
- Identify (known and unknown) vulnerabilities - Evaluate possible exploitations of vulnerabilities - Analysis the impact of possible adverse situations and cascading effects - Assess the current cybersecurity controls in place and determine the possible gaps and improvements	- Analysis data to proactively identify errors/failures within the system - Verify and enforce privacy and security rules - Support the correct use of the system by providing awareness and training capabilities - Validate the proper functioning of protection/defence tools and policies - Verify the actual status of the system and compliance with best practices and security policies	- Test and validate new patterns, vectors and attack rules - Test the output of a specific asset for anomalous behaviour - Adjust and reenforce existing ML algorithms for early anomaly detection - Support deep inspection actions - Test and improve the strength of host/network-based intrusion detection systems patterns and rules - Support cyber situational awareness for threat detection	- Establish a response and monitoring plan, by (1) timely identifying damages and related cause, and (2) reproducing or predicting complex incidents - Support the establishment of emergency strategies - Identify the agents' role, and categorize the assets and possible attacks - Perform interactive optimizations of organizations' processes under various incident conditions - Establish controlled upgrading processes based on the recent discoveries	- Establish a recovery plan through a realistic understanding of the entire lifecycle of a system - Facilitate the development, testing and maintenance of strategies and plans for disaster recovery - Accelerate/facilitate the automated recovery processes - Test and validate the actual effectiveness of security patches at a low cost	

NIST Framework Version 1.1
The Cybersecurity Framework

- This table represents the DT's capabilities to meet (some) criteria of the framework
  - E.g., with the DT, we can guarantee identification of vulnerabilities and evaluate them ➔ ID.RA-1, ID.RA-4, ID.RA-5, …

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Identify	Protect	Detect	Respond	Recover
- Identify (known and unknown) vulnerabilities - Evaluate possible exploitations of vulnerabilities - Analysis the impact of possible adverse situations and cascading effects - Assess the current cybersecurity controls in place and determine the possible gaps and improvements	- Analysis data to proactively identify errors/failures within the system - Verify and enforce privacy and security rules - Support the correct use of the system by providing awareness and training capabilities - Validate the proper functioning of protection/defence tools and policies - Verify the actual status of the system and compliance with best practices and security policies	- Test and validate new patterns, vectors and attack rules - Test the output of a specific asset for anomalous behaviour - Adjust and reenforce existing ML algorithms for early anomaly detection - Support deep inspection actions - Test and improve the strength of host/network-based intrusion detection systems patterns and rules - Support cyber situational awareness for threat detection	- Establish a response and monitoring plan, by (1) timely identifying damages and related cause, and (2) reproducing or predicting complex incidents - Support the establishment of emergency strategies - Identify the agents' role, and categorize the assets and possible attacks - Perform interactive optimizations of organizations' processes under various incident conditions - Establish controlled upgrading processes based on the recent discoveries	- Establish a recovery plan through a realistic understanding of the entire lifecycle of a system - Facilitate the development, testing and maintenance of strategies and plans for disaster recovery - Accelerate/facilitate the automated recovery processes - Test and validate the actual effectiveness of security patches at a low cost
4	**5**	**6**	**5**	**4**

The protection of **the entire system and its data** is transversal to these five security functions

NIST Framework Version 1.1
The Cybersecurity Framework

DTs offer high simulation capabilities for the security and protection of critical systems

Conclusions: multiple benefits in terms of security, safety, sustainability and profitability of the value chain and business

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

ECCO European Cybersecurity COmmunity

Identify	Protect	Detect	Respond	Recover
- Identify (known and unknown) vulnerabilities - Evaluate possible exploitations of vulnerabilities - Analysis the impact of possible adverse situations and cascading effects - Assess the current cybersecurity controls in place and determine the possible gaps and improvements	- Analysis data to proactively identify errors/failures within the system - Verify and enforce privacy and security rules - Support the correct use of the system by providing awareness and training capabilities - Validate the proper functioning of protection/defence tools and policies - Verify the actual status of the system and compliance with best practices and security policies	- Test and validate new patterns, vectors and attack rules - Test the output of a specific asset for anomalous b… - Adjust and re… existing ML algorithms fo… - Support deep… inspection ac… - Test and imp… strength of host/network intrusion dete… systems patte… rules - Support cyber situational awareness for threat detection	- Establish a response and monitoring plan, by (1) timely identifying damages and related cause, and (2) reproducing … processes under various incident conditions - Establish controlled upgrading processes based on the recent discoveries	- Establish a recovery plan through a realistic understanding of the entire lifecycle of a system
4	5	6	5	4

The protection of **the entire system and its data** is transversal to these five security functions

The next step is to associate the identified DT capabilities to each security function,

- in order to verify that it is indeed useful for the fulfilment of the security framework

For the sake of simplicity, we explore here only the function "PROTECTION"

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Mapping to the NIST security categories and identifiers

Security function	Potential contribution of DTs	Support to NIST categories
PROTECT	**Analysis data** to proactively identify errors/failures within the system **Verify and enforce** privacy and security **rules**	• **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) • **Information Protection Processes and Procedures (PR.IP)** through the design of vulnerability management plans (PR.IP-12) • **Maintenance (PR.MA)** under controlled actions, access (PR.MA-2) and tools (PR.MA-1)

Protect

- Analysis data to proactively identify errors/failures within the system
- Verify and enforce privacy and security rules
- Support the correct use of the system by providing awareness and training capabilities
- Validate the proper functioning of protection/defence tools and policies
- Verify the actual status of the system and compliance with best practices and security policies

1

PR.AC	Identity Management and Access Control
PR.AT	Awareness and Training
PR.DS	Data Security
PR.IP	Information Protection Processes and Procedures
PR.MA	Maintenance
PR.PT	Protective Technology

2

HOW should we interpret this table?

DTs are able to analyse data and their statuses, as well as compliance with privacy and security rules according to policies ➔ this is in line with "PR.DS", PR.IP and PR.MA (which are essentials for protection of systems)

- with the analysis of data, we guarantee PR.DS
- with the verification of rules, we can ensure PR.IP and PR.MA

Security function	Potential contribution of DTs	Support to NIST categories
PROTECT	Analysis data to proactively identify errors/failures within the system	• 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) • Information Protection Processes and Procedures (PR.IP) through the design of vulnerability management plans (PR.IP-12) • Maintenance (PR.MA) under controlled actions, access (PR.MA-2) and tools (PR.MA-1)
	Verify and enforce privacy and security rules	
	Support the correct use of the system by providing awareness and training capabilities	• **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)

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Security function	Potential contribution of DTs	Support to NIST categories
PROTECT	Analysis data to proactively identify errors/failures within the system	• 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) • Information Protection Processes and Procedures (PR.IP) through the design of vulnerability management plans (PR.IP-12) • Maintenance (PR.MA) under controlled actions, access (PR.MA-2) and tools (PR.MA-1)
	Verify and enforce privacy and security rules	
	Support the correct use of the system by providing awareness and training capabilities	• 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/defence **tools and policies**	• **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)

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Security function	Potential contribution of DTs	Support to NIST categories
PROTECT	Analysis data to proactively identify errors/failures within the system	• 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) • Information Protection Processes and Procedures (PR.IP) through the design of vulnerability management plans (PR.IP-12) • Maintenance (PR.MA) under controlled actions, access (PR.MA-2) and tools (PR.MA-1)
	Verify and enforce privacy and security rules	
	Support the correct use of the system by providing awareness and training capabilities	• 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/defence tools and policies	• 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	• **Protective Technology (PR.PT)** through logs and audits in concordance with regulatory frameworks (PR.PT-1)

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Perspective 2: How NIST categories are aligned with DT protection

ECCO European Cybersecurity COmmunity

Identify	Protect	Detect	Respond	Recover
- Identify vulnerabilities associated with the different technologies integrated in the DT - Apply a risk assessment method to every DT block, and to the supply chain (IT/OT) - Guarantee a response, recovery plan, and testing with suppliers	- Manage unique and legitimate identities - Guarantee access, complying with the least privilege and least functionality - Create awareness. (IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities - Guarantee confidentiality and integrity - Implement report response/recovery mechanisms for information leak incident, and proactive actions - Implement response/recovery measures in a proactive manner	- Evaluate any event generated by the DT and associated IT platforms (e.g., through SOCs) - Correlate DT events to have a better understanding of security issues occurring between spaces of a DT and within a DT - Monitor/control what occurs within the DT - Guarantee detection in the different spaces of a DT - Provide adequate detection through continuous testing and validation	- Establish a response plan - Share information (both internally and externally) - CTI - Establish criteria for incident reporting - Control and investigate threat notifications and anomalous DT events - Recover configurations and data through forensic techniques, in addition to preserving evidence for the future - Set up efficient processes to receive, analyse and respond to vulnerabilities disclosed - Contain and mitigate incidents (including new vulnerabilities) occurring in DTs	- Establish a recovery plan based on lessons learned, considering metrics or indicators to improve the accuracy of the recovery process and its time
3	**6**	**5**	**7**	**1**

The protection of **the DT and its data** is also transversal to these five protection areas

NIST Framework Version 1.1
The Cybersecurity Framework

We note that the framework is useful for the protection of DTs

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Perspective 2: How NIST categories are aligned with DT protection

ECCO
European Cybersecurity COmmunity

Identify	Protect	Detect	Respond	Recover
- Identify vulnerabilities associated with the different technologies integrated in the DT - Apply a risk assessment method to every DT block, and to the supply chain (IT/OT) - Guarantee a response, recovery plan, and testing with suppliers	- Manage unique and legitimate identities - Guarantee access, complying with the least privilege and least functionality - Create awareness. (IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities - Guarantee confidentiality and integrity - Implement report response/recovery mechanisms for information leak incident, and proactive actions - Implement response/recovery measures in a proactive manner	- Evaluate any event generated by the DT and associated IT platforms (e.g., through SOCs) - Correlate DT events to have a better understanding of security issues occurring between spaces of a DT and within a DT - Monitor/control what occurs within the DT - Guarantee detection in the different spaces of a DT - Provide adequate detection through continuous testing and validation	- Establish a response plan - Share information (both internally and externally) - CTI - Establish criteria for incident reporting - Control and investigate threat notifications and anomalous DT events - Recover configurations and data through forensic techniques, in addition to preserving evidence for the future - Set up efficient processes to receive, analyse and respond to vulnerabilities disclosed - Contain and mitigate incidents (including new vulnerabilities) occurring in DTs	- Establish a recovery plan based on lessons learned, considering metrics or indicators to improve the accuracy of the recovery process and its time
3	**6**	**5**	**7**	**1**

The protection of **the DT and its data** is also transversal to these five protection areas

NIST Framework Version 1.1
The Cybersecurity Framework

- This table represents how the criteria of the framework can help maintain security in the DT
  - E.g., the framework recommends ID.RA ➔ this should be a condition to keep the DT free (as far as possible) from vulnerabilities

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Identify	Protect	Detect	Respond	Recover
- Identify vulnerabilities associated with the different technologies integrated in the DT - Apply a risk assessment method to every DT block, and to the supply chain (IT/OT) - Guarantee a response, recovery plan, and testing with suppliers	- Manage unique and legitimate identities - Guarantee access, complying with the least privilege and least functionality - Create awareness. (IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities - Guarantee confidentiality and integrity - Implement report response mechanisms for information leak incident, and proactive actions - Implement response/recovery measures in a proactive manner	- Evaluate any event generated by the DT and associated IT platforms (e.g., through SOCs) - Correlate DT events to have a bett… understandin… security issue… occurring bet… spaces of a D… - Monitor/cont… what occurs v… the DT - Guarantee de… in the differe… spaces of a D… - Provide adequ… detection through continuous testing and validation	- Establish a response plan - Share information (both internally and externally) - CTI - Establish criteria for … … processes to receive, analyse and respond to vulnerabilities disclosed - Contain and mitigate incidents (including new vulnerabilities) occurring in DTs	- Establish a recovery plan based on lessons learned, considering metrics or indicators to improve the accuracy …
3	6	5	7	1

The protection of **the DT and its data** is also transversal to these five protection areas

The next step is to associate the identified conditions of each security function to the ways to protect the DT,

- in order to verify that it is indeed useful for the protection of DTs

For the sake of simplicity, we explore here only the function "PROTECTION"

Figure Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

Security function	Potential contribution of NIST	Support to DT protection
PROTECT	**Identity Management and Access Control (PR.AC)**	Manage **unique and legitimate identities**
		Guarantee access, complying with **the least privilege and least functionality**

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

HOW should we interpret this table?

The NIST's framework adds a set of security conditions in order to guarantee security such as PR.AC

- with PR.AC and its subcategories, we then state
  - that unique identities MUST be established when using DT, and
  - we MUST ensure access that meets the least privilege

Protect

- Manage unique and legitimate identities
- Guarantee access, complying with the least privilege and least functionality
- Create awareness: (IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities
- Guarantee confidentiality and integrity
- Implement report response mechanisms for information leak incident, and proactive actions
- Implement response/recovery measures in a proactive manner

Security function	Potential contribution of NISTs	Support to DT protection
PROTECT	Identity Management and Access Control (PR.AC)	Manage unique and legitimate identities
		Guarantee access, complying with the least privilege and least functionality
	Awareness and Training (PR.AT)	(IT/OT) **Operators must be awareness** of the cybersecurity risks, and of their roles and responsibilities **with respect to the DT**

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Security function	Potential contribution of NISTs	Support to DT protection
PROTECT	Identity Management and Access Control (PR.AC)	Manage unique and legitimate identities
		Guarantee access, complying with the least privilege and least functionality
	Awareness and Training (PR.AT)	(IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities with respect to the DT
	Data security (PR.DS)	Guarantee **confidentiality and integrity**
		Implement report response **mechanisms for information leak** incident, and **proactive actions**

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Security function	Potential contribution of NISTs	Support to DT protection
PROTECT	Identity Management and Access Control (PR.AC)	Manage unique and legitimate identities
		Guarantee access, complying with the least privilege and least functionality
	Awareness and Training (PR.AT)	(IT/OT) Operators must be awareness of the cybersecurity risks, and of their roles and responsibilities with respect to the DT
	Data security (PR.DS)	Guarantee confidentiality and integrity
		Implement report response mechanisms for information leak incident, and proactive actions
	Protective Technology (PR.PT)	Implement **response/recovery measures in a proactive manner**

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Conclusions

Conclusions

- Many actions are in progress, so there is no unified way to guarantee a common implementation methodology
  - At the technical, operational and administrative levels
- It is still a challenge what the implementation of DT-based ecosystems would entail
  - Enormous technological boom that the implementation of DTs implies
  - Multiple technologies can be integrated as part of a DT:
    - AI, CPS, IIoT, edge computing, 5G/6G, …
- The challenge also lies not only with the scientific community, with more approaches and optimal approaches, but also with many other stakeholders

ECCO
European Cybersecurity COmmunity

Q&A

Digital Twins architectures and security capabilities: a Game-Changer for Cybersecurity

Javier Lopez, Cristina Alcaraz
University of Malaga, Spain