Digital Twin: A Comprehensive Survey of Security Threats.

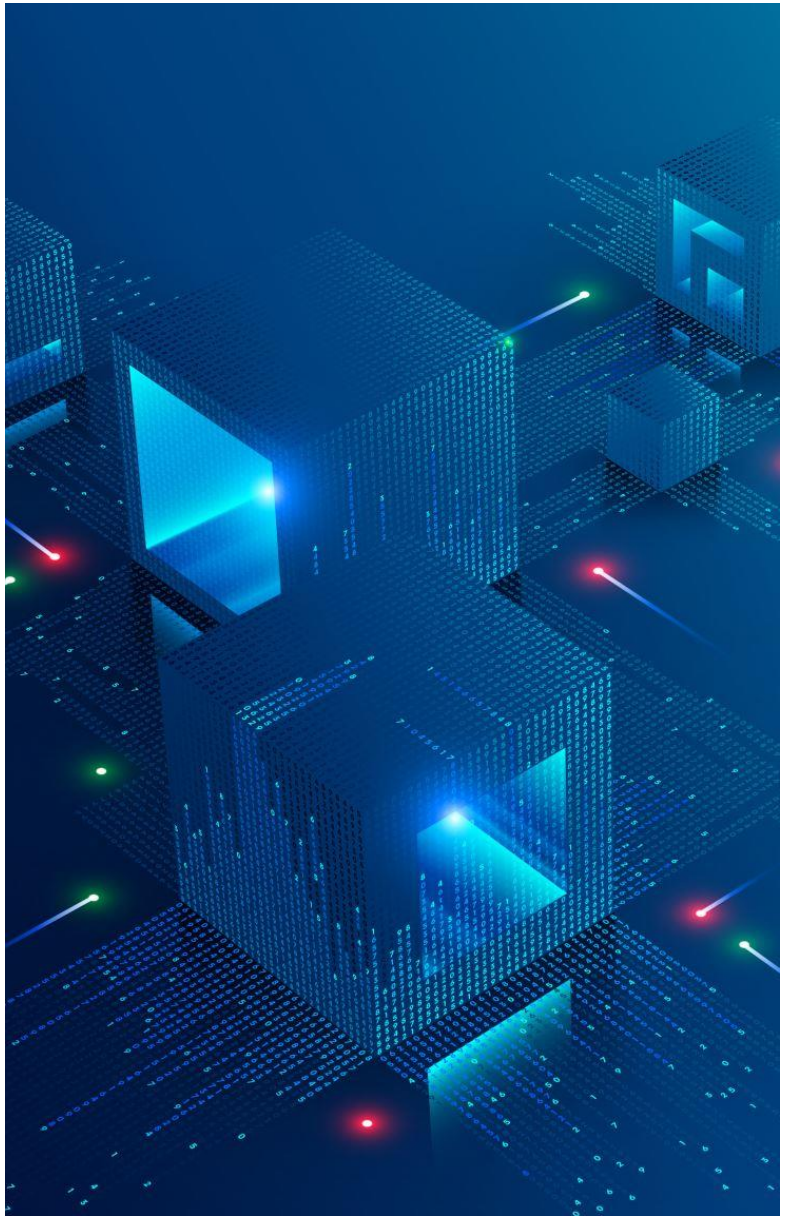
~ Part 01 ~

Written By: Alcaraz et. al,.
(Computer Science Department, University of Malaga, Spain)

Presented By: 제레미아

Course: Advanced Security in Emerging ICT

Monday, Nov-14, 2022 (Week - 11)



CONTENTS:

PART 01: (Jeremiah)

1. Introduction ~ Abstract/Background
2. DT Functional Layers & Enabling Technologies
   - A: Functional Layers
   - B : Enabling Technologies
3. Operational Requirements for a DT

PART 02: (Oscar)

4. Security Threats in DT
5. Exploration of Security Approaches
6. Final Remarks and Conclusion

1.

INTRODUCTION

Introduction / Background:

- The digital twin (DT) is one of the most cutting-edge technologies of Industry 4.0, providing simulation capabilities to forecast, optimize and estimate states and configurations. This paper analyzes the current state of the DT paradigm and classifies the potential threats associated with it.
- The DT concept originated in 1970 when NASA started to monitor its physical components for aerospace missions. Today's DT concept is much more than just a virtualization system, but an extension of Industry 4.0.
- By definition: A DT is a group of machines that are simulating, emulating, or mirroring the life of a physical entity. The DT concept as it is understood today was first introduced by Michael Grieves during his executive course on product life-cycle management (PLM).
  - ✓ **Definition:** DT is generally conceived as the grouping of "machines (physical and/or virtual) or computer- based models that are simulating, emulating, mirroring or twinning the life of a physical entity"

1.

INTRODUCTION

Introduction / Background:

- **Digital assets** are digital entities that run on servers and/or virtualized resources (e.g., virtual machines, containers and networks) and interact with real-world components. The aim of a DT is to anticipate errors, variations and relevant deviations that may change a system's natural behavior.

- DT has **three main spaces**:
  - ✓ **Physical space:** comprises the real-world operational technologies (OTs) such as sensory devices, actuators and controllers (e.g., remote terminal units (RTUs) and programmable logic controllers (PLCs)).
  - ✓ **Digital space:** represents physical assets using digital assets capable of simulating states, conditions and configurations, and of making decisions regarding the physical space.
  - ✓ **Communication space:** connects the physical and digital spaces, allowing the DT to interfere in the production operations through information flows and processes.

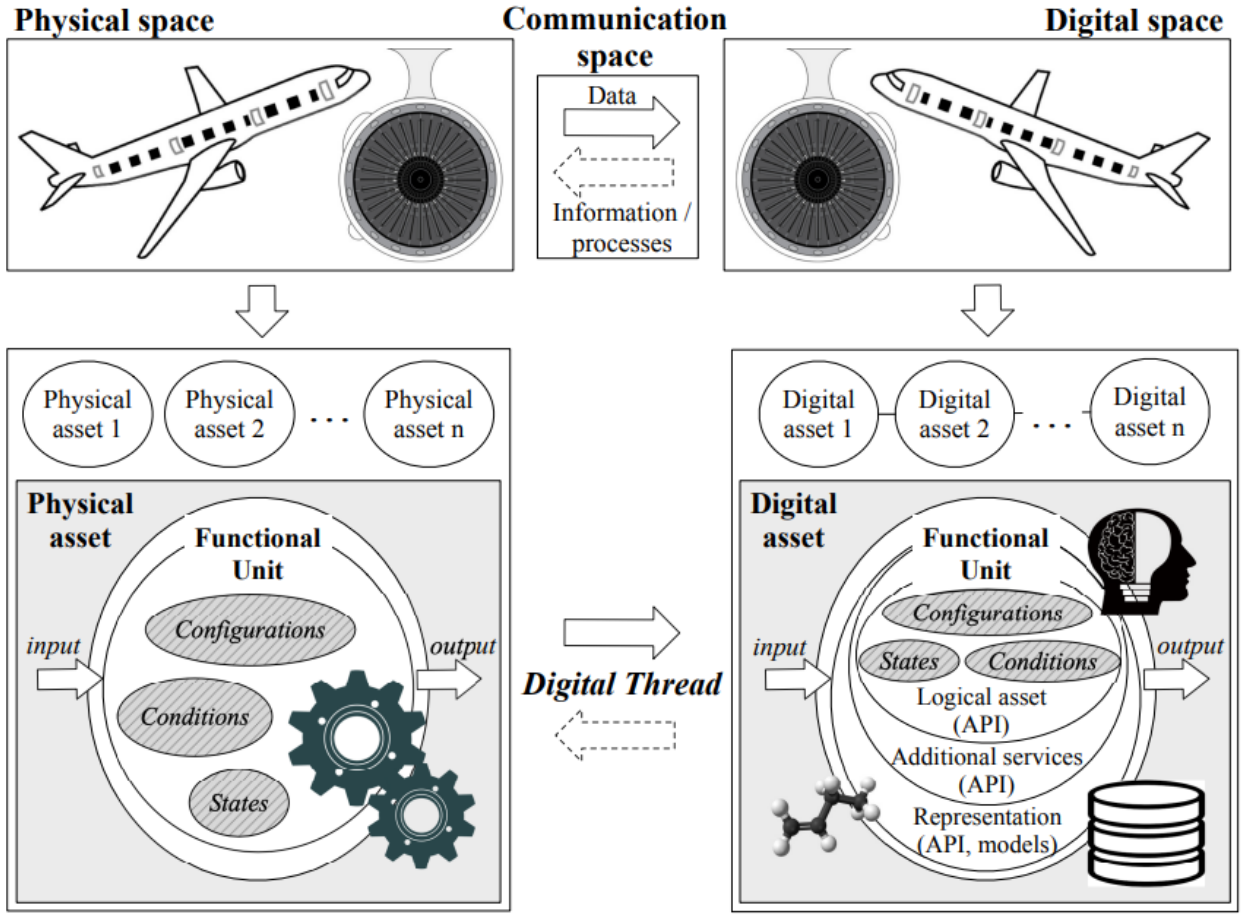


Fig. 1: DT work spaces

DT Three Main Spaces:

- This DT characterizes the behavior of an aircraft turbine in the real world, where information from physical assets (for instance, sensor data) is collected and sent to the DT in order to trigger the simulation model.
- Similarly, digital assets may establish configurations and execute commands that can change the state of the physical counterpart, either to maintain, optimize, or improve the operational performance of its components.
- For the communication space, it should be bi-directional. Reason: The data from physical assets are processed by digital assets, while the latter create new useful information that may be sent back to the physical space
  - ✓ Specifically, it is this kind of communication that differentiates a DT from traditional simulators.

1.

INTRODUCTION

Introduction / Background:

- **Variants of Mirroring Systems:** To further clarify the differences between DT, Emulators and CPS the authors defined three variants of mirroring systems as listed below:

  - ✓ **Digital model:** which is an isolated system without automatic connection to the real world.
  - ✓ **Digital shadow:** a system with an automated one-way communication between the physical space and the virtual space.
  - ✓ **Digital twin**: a system with bidirectional and automatic connection between both spaces.

1.

INTRODUCTION

Introduction / Background:

- **DT Technologies:** DT technologies range from cyber-physical systems (CPS) to industrial IoT (IIoT) and edge computing and make use of artificial intelligence (AI) and big data (BD) techniques.

- This technological heterogeneity also means that the design of a DT can vary greatly, ranging from a simple DT system to more complex designs whose logic can be spread throughout the entire system.

- **DT Application Scenarios:**
  - ✓ **A product:** a single DT observing the operation of a physical asset
  - ✓ **A process**: an observation of a larger context such as a production or assembly line
  - ✓ **A system:** a set of product and process models used to characterize a complex network or an industrial facility.

- So far, there are several use cases that have already shown the practical value of the aforementioned designs (See next slide)

TABLE I: SOME EXAMPLES OF THE USE OF THE DT PARADIGM

Oil and gas	[25]	Furnaces/preheat train/pipelines
	[25], [26]	/wells Refinery Gas turbine (SGT-A65) fleet
	[27]	
Electrical energy	[28]	Power plant/wind turbines
	[29]	Power electronic converters
	[30]	CPS for power systems
	[14], [31]	Microgrid
	[32], [33]	Smart Grid
(Petro-)chemical	[25]	Chemical plant/reactors
	[34], [35]	Production control
Water	[12], [36]	Water treatment systems
Manufacturing	[37]	Chassis welding lines
	[38]	Pneumatic cylinder lines
	[39], [40]	Manufacturing operations and control
Automotive	[41]	Safety of human operators
	[42]	Privacy leakage
	[43]	Baking system
	[44], [45]	Autonomous vehicles and driving
Healthcare	[46]	CT scanner for MRI
	[47]	Remote surgery and control
	[40], [47]	Robot surgical machines
Transportation	[28]	Engine blades (GE90) for Boeing
		train, called Trip Optimizer
	[26]	Tracking of individuals at airports

2.

DT FUNCTIONAL LAYERS & ENABLING TECHNOLOGIES

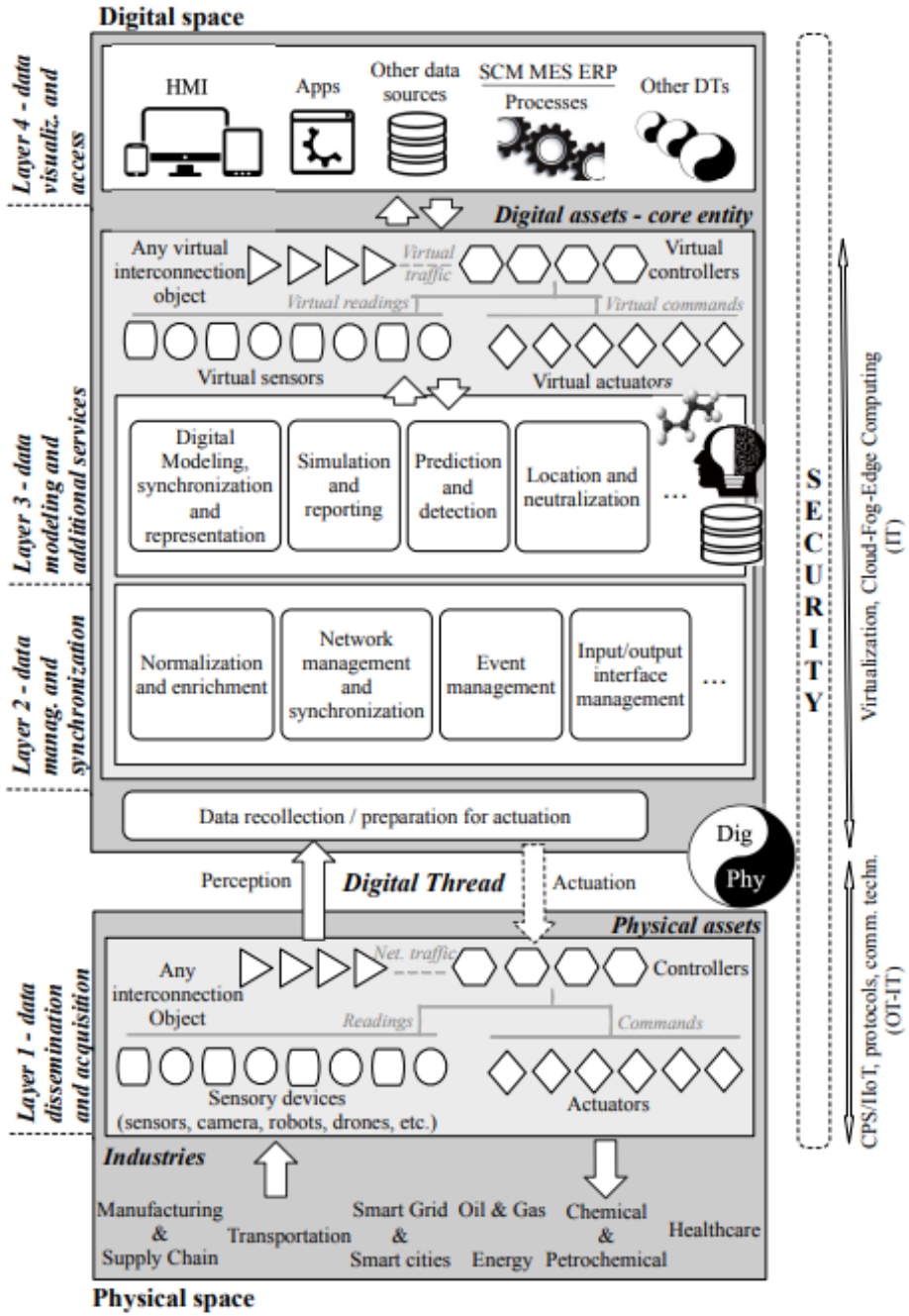


Fig. 2: A four layer-based digital twin

1. DT Functional Layers:

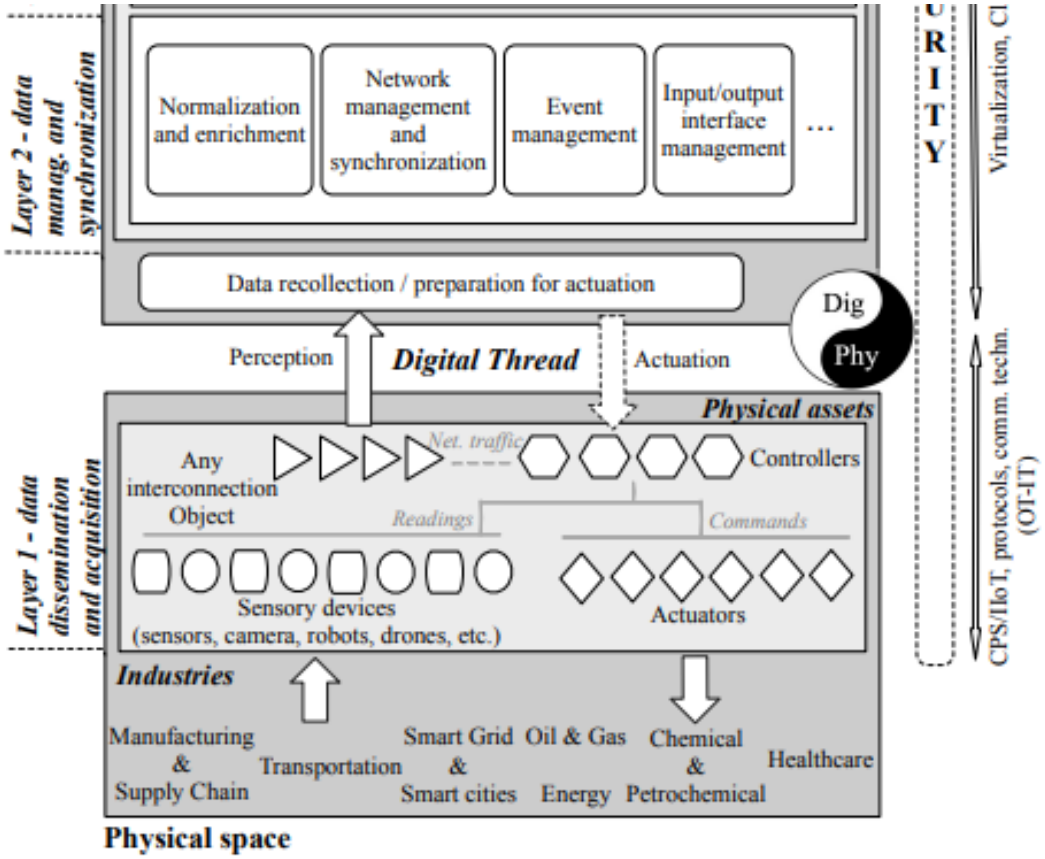


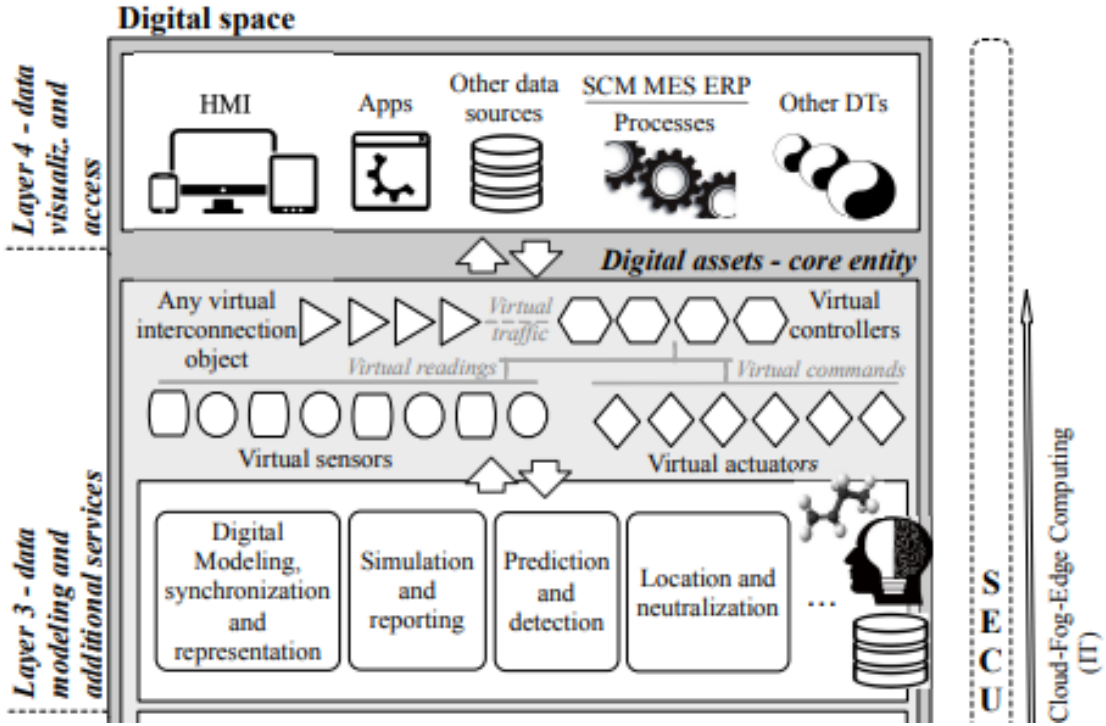
Fig. 2: A four layer-based digital twin

- **Layer 1: Data dissemination and acquisition**. Captures the dynamics from the physical space and prepares the control instructions for the physical assets.

- **Layer 2: Data management and synchronization**. Normalizes and enriches heterogeneous multisource data, allowing essential Layer 3 services to be executed. As the digital and physical space must cooperate with each other, network management and synchronization services must be considered.

  - ✓ **NOTE:** The difference btn layers relies on the level of processing of data in the DT and on the technologies involved.

DT Functional Layers:



- **Layer 3: Data modeling and additional services**. Specifies states, behavior and geometric shapes through digital models. Within this layer, it is also possible to add additional services to provide maintenance and monitoring, cybersecurity and diagnostic tasks.

- **Layer 4: Data visualization and accessibility**. Allows end users, entities and processes (e.g., supply chain management (SCM), enterprise resource planning (ERP), manufacturing execution systems (MESs) and other DTs) to visualize simulation results from digital models in order to make decisions regarding physical assets.

2. Enabling Technologies:

Layer 1: Data Dissemination and Acquisition:

- Among the existing technologies used to "perceive" the physical space, **CPS** and **IIoT** are the most common. The former was originally coined in 2006 as *"engineered systems that are built from, and depend upon, the seamless integration of computation and physical components*"
  - ✓ Embedded systems combining computation, networking and physical processes such that the latter may impact on computational results, and vice versa.
- In contrast, IIoT is a useful technology for environments where (autonomous and smart) devices need to connect to the Internet, without the need for synchronous communications among them or a closed-loop communication with the real world

2.

DT FUNCTIONAL LAYERS & ENABLING TECHNOLOGIES

2. Enabling Technologies:

Layer 2 ~ 4: Modeling, representation and visualization:

- Designs of these layer are made such that, they concentrate the core of their main computation on powerful devices whose computational logic may reside on a server or be spread throughout the system

- For this study, authors considers computing infrastructures based on **edge**, **fog** and **cloud**, mainly due to their processing and storage capabilities, which differentiate them from traditional standalone servers.
  - ✓ With regard to data management, BD and AI techniques are needed.
  - ✓ In order to represent knowledge extracted from AI techniques, the current representation and modeling tools, such as CAD/ECAD (electronic computer-aided) systems and CAM (computer-aided manufacturing) systems are used.
  - ✓ Prior mentioned software processes and data can be accessed through various communication interfaces (e.g., HTTP, REST, JavaScript object notation (JSON)), human machine interfaces (HMIs, with support for virtual, augmented or mixed reality - VR, AR and MR) and dashboard services.

2.

DT FUNCTIONAL LAYERS & ENABLING TECHNOLOGIES

In this section, authors present a complete picture of DT requirements, stressing the relevance of re-usability, interoperability, interchangeability, maintainability, extensibility and autonomy.

3.

OPERATIONAL REQUIREMENTS OF A DT.

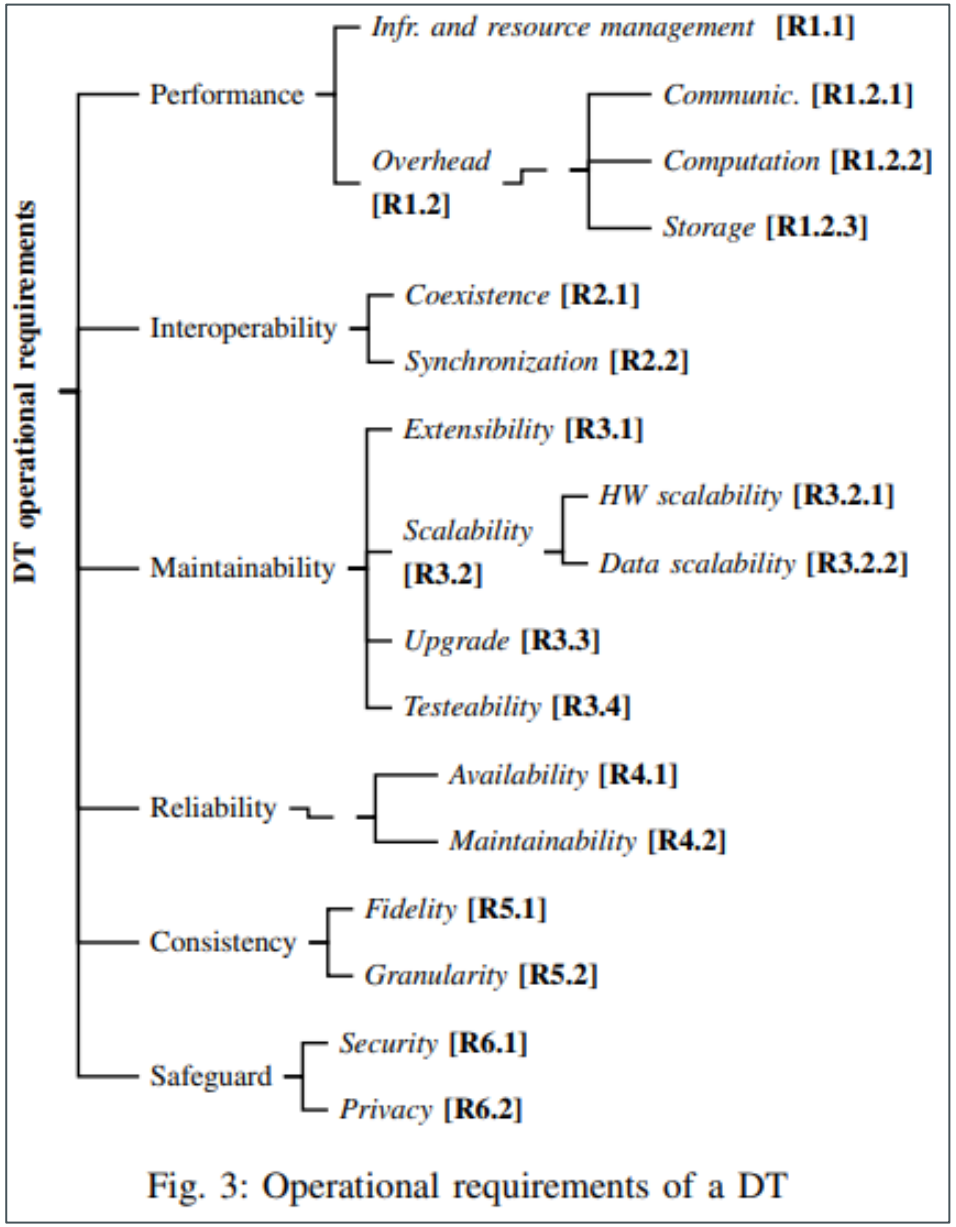


Fig. 3: Operational requirements of a DT

DT Operational Requirements:

- This figure represents the hierarchical relationships between requirements, which are also described in depth in the following subsections (next slides).

A. Operational Performance and reduction of complexities:

- One of the main objectives of the DT paradigm is to keep the digital space synchronized with the physical space. Any variation between the two spaces can lead to a significant deviation in the final representation of a physical asset.
- To avoid this, it is first necessary to address the various complexities of the system in terms of infrastructure, communication, computation and storage.
- Second, it is vital to ensure reliable connection to the physical world. Both aspects are covered in this paper, considering the following sub-requirements

    1) **Infrastructure and resource management** [R1.1]: DTs must ensure efficient connections with the real world for synchronization and efficient simulations for representation of the real world

    2) **Overhead management:** . three classes of overhead related to (i) communication; (ii) computation; and (iii) storage needs to be managed

3. OPERATIONAL REQUIREMENTS OF A DT.

B. Interoperability between assets and layers

- Interoperability is defined by IEEE as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged"
- In DT-based scenarios, this definition can be interpreted as the system's capacity to exchange and use information between spaces
- Within this concept, authors further identified two relevant sub-requirements ([R2.1] and [R2.2]):

1) **Coexistence [R2.1]:** Not only do physical assets of Layer 1 (including interfaces and communications) have to coexist in the same space, but also digital assets of Layer 3. Digital assets have to coexist in the same virtual plane to simulate states equivalent to the physical world, and thus meet the requirements of consistency between both spaces.
2) **Synchronization [R2.2]:** In order to obtain reliable simulations with executions similar to the real world, the system must find a way to synchronize the cooperation among assets of the same space or between spaces.

3. OPERATIONAL REQUIREMENTS OF A DT.

C. Maintainability of digital assets

- DT functions must operate over a long period of time. To address this challenge, maintainability issues must come into play.
- This concept gives rise to two different definitions by IEEE:

  "*the ease with which a software system or com- ponent can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment*"; and "*the ease with which a hardware system or component can be retained in, or restored to, a state in which it can perform its required functions*"

- The concept itself can be extrapolated to DT-based systems, since HW/SW conflicts, anomalies, breaches and bugs may arise in the four layers of the DT.

  1) **Extensibility [R3.1]** and **scalability [R3.2]**: Extensibility refers to the system's ability to incorporate new SW components, whilst scalability refers to the system's capacity to add new HW components.
  2) **Upgrade [R3.3]:** This procedure should not cause greater damage to the simulation stages.
  3) **Testability [R3.4]:** Given the complexities of DT-based systems, testability is also an essential requirement for detecting whether security policies and the functionality criteria needed to strengthen DT functions are properly fulfilled

3. OPERATIONAL REQUIREMENTS OF A DT.

D. Reliability of assets and data:

- **Reliability** is defined by IEEE as:

  "*the ability of a system or component to perform its required functions under stated conditions for a specified period of time*", which in turn, corresponds to "*a measure of the continuity of correct service*".

- It has three essential sub-requirements: **availability**, **maintainability** and **testability** (note that the last two have been described in prev. slides).

  1) **Availability [R4.1]:**

     - ✓ This is related to the level of access to resources, either HW/SW components or data. With regard to access, quality of service (QoS) policies are recommended, which could be supported by diverse QoS mechanisms such as fault tolerance and exception handling.
     - ✓ If QoS is associated with data quality, then this should be attributed to delivery (timelessness, priority, ordering and presentation) and durability (access time to valid data).

3. OPERATIONAL REQUIREMENTS OF A DT.

E. Consistency in reasoning and representation:

- **Consistency** is linked to digital assets' quality of reasoning and representation: what the physical asset projects must be equivalent to what its digital counterpart interprets and shows.
- With regard to consistency, authors identified two further essential sub-requirements ([R5.1] and [R5.2]):

1) Fidelity [R5.1]:

- ✓ This sub-requirement is associated with accuracy. DTs have to show an equivalent reality to their counterparts. Any deviation beyond that reality could lead to invalid interpretations and conclusions, and cause inaccurate settings and inappropriate C&C instructions that may drastically change or damage the behavior of physical assets.

2) Granularity [R5.6]:

- ✓ This sub-requirement is associated with the degree to which a DT can characterize the structures and the behavior of the observed system according to levels of granularity. This is in part thanks to the advances in SW engineering that make it possible to represent critical contexts using specific models for manufacturing domains, including reusable models.

3.

OPERATIONAL REQUIREMENTS OF A DT.

F. Safeguarding virtual resources, operations and data

- **Security** is also an important issue that must be considered within the DT paradigm. One of the main reasons is that the DT tool is being extended to multiple types of scenarios, many of which are of a critical nature
- They can be applied for monitoring, analysis, predictive maintenance, engineering design and testing.
- All these services rely heavily on SW components (algorithms, models, applications), which are usually susceptible to multiple threats due to bugs, as well as on multiple infrastructures, interfaces and network connections.

3.

OPERATIONAL REQUIREMENTS OF A DT.