# How to Build Realistic Security Testbeds Using Digital Twin and Data Spaces Technology

**Luigi Romano**

University of Naples «Parthenope»

luigi.romano@uniparthenope.it

FITNESS
FAULT AND INTRUSION TOLERANT NETWORKED SYSTEMS

**The European Network for Cybersecurity (NeCS) PhD School**

**January 8-12, 2024 - Cortina d'Ampezzo (BL)**

# Roadmap

- **Rationale and contribution**
- **Digital Twins**
- **Data Spaces**
- **An enabling DT/DS technology**
- **Case studies in multiple application domains:**
  - Smart Grid
  - Sensitive Industrial Plant
  - Flexible Manufacturing System
- **Acknowledgements and contacts**
- **Pointers for individual follow-ups**

# Why this talk and what you will get out of it

# Problem Statement

- Testbeds are a key research asset, since they are one of the most effective tools for validating research outputs/findings
- Unfortunately, they are a scarce resource, for a number of reasons (including, but not limited to):
  - In the design phase, the physical system is not – or is only partly – available → hence, the testbed is not available
  - In the operational phase, the system is physically available, but it is not available for experiments
  - The system is physically available and it is also available for experiments … but not for all types of experiments

**This is especially true for cybersecurity experiments**

# Claims - 1/2

- Creating testbeds which can be used in all phases of a system’s lifetime (from early design stages to full operation) and for all types of experiments is of paramount importance
- This ambitious goal can be achieved via combined use of two promising – and somehow complementary – technologies, namely: Digital Twins (DT) and Data Spaces (DS)
- Not only testbeds resulting from combined use of DT and DS technologies have the aforementioned unique capability, but they also bring about important advantages which alternative approaches do not have, notably:
  - They successfully capture the ever increasing complexity of real world setups

# *Claims – 2/2*

- They successfully capture event patterns resulting from interactions of the system with the surrounding environment
- They enable effective implementation of Human In The loop (HIL) approaches in the analysis
- They have a dramatic potential in terms of reduction of the effort needed for building the testbed
- They enable use of potentially sensitive input data in a controlled and policy-compliant fashion
- They enable the sharing and reuse of research output data in a controlled and policy-compliant fashion
- They support continuous and bidirectional transfer of knowledge from the current version of the system to the future versions of it

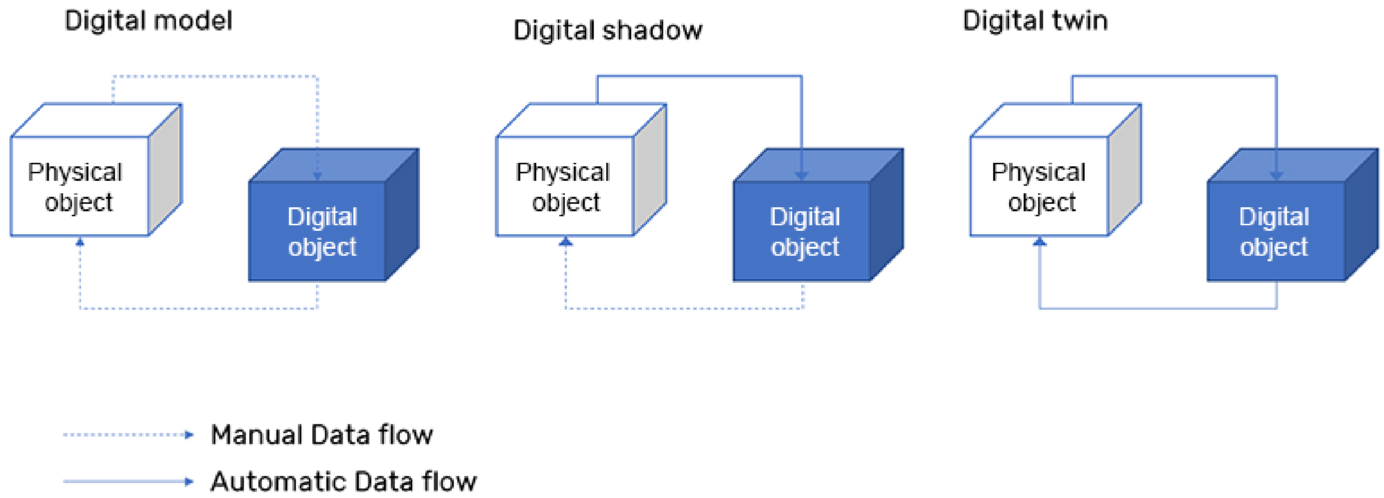
# Takeaways

- You will be initiated to DT and DS technologies
- You will learn how to use these technologies to build experimental testbeds using a sound methodological approach
- You will receive valuable hints, taken from real use cases in multiple application domains
- And, with some additional efforts:
  - You will have the opportunity of “getting your hands dirty” in a practical experience using a specific DT+DS emerging technology, namely FIWARE
  - Important additional information in the last slides

# Digital Twin technology

# Digital Model, Digital Shadow, and Digital Twin

- Digital Model (DM): communication between Physical and Digital space is manual
- Digital Shadow (DS): communication from digital to physical space is manual, communication from physical to digital space is automatic
- Digital Twin (DT): automatic communication physical to digital and vice versa

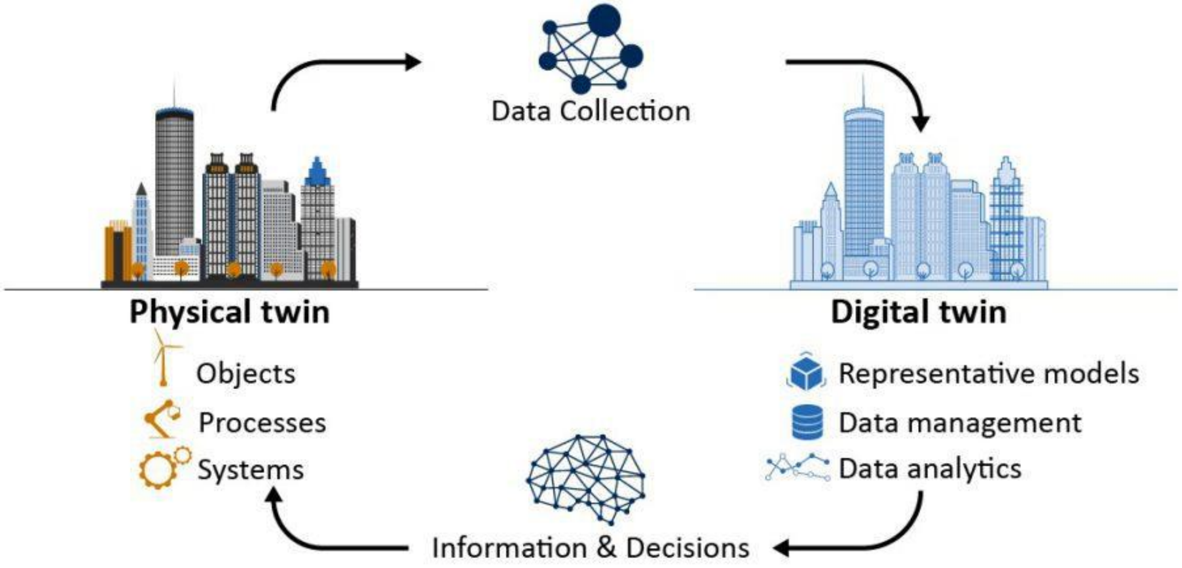


# Digital Twin definition

The Digital Twin Consortium defines a Digital Twin as follows:

**"A virtual representation of real-world entities and processes, synchronized with specific frequency and fidelity"**

**https://www.digitaltwinconsortium.org/hot-topics/the-definition-of-a-digital-twin/**




Sources: GAO; ladoga/stock.adobe.com. | GAO-23-106453

# *The OODA loop*

- Developed by military strategist and United States Air Force Colonel John Boyd
- Assumes that individuals and organizations engage in an ongoing interaction with their surroundings
- Defines a decision-making framework for responding to events, breaking down the decision cycle into four interconnected and constantly cycling processes:

  **O**bservation

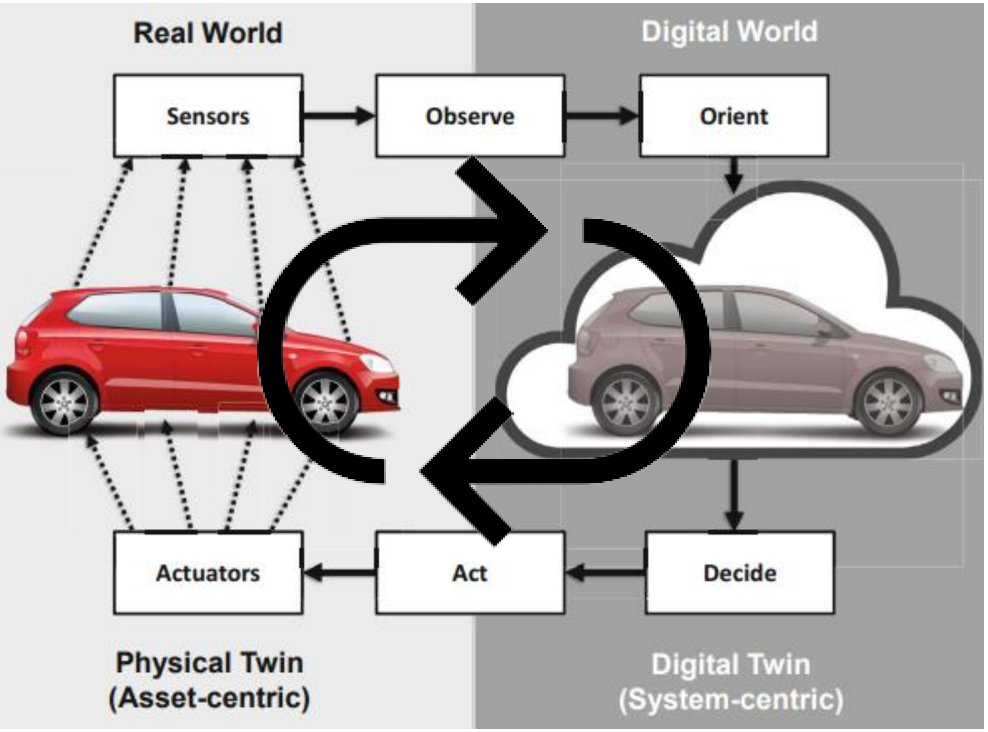
  **O**rientation

  **D**ecision

  **A**ction

# DT and OODA

- **Observation**: involves collecting data from the smart environment to gain insights into the current state
- **Orientation**: entails examination and synthesis of data to form an evaluation of the conditions within the smart environment, progressing from raw data to meaningful information, then knowledge, and finally valuable insights
- **Decision**: various options are considered to determine the most suitable course of action, with the overarching aim of optimizing the operation of the smart environment (predictive modeling can be a pivotal tool in this step)



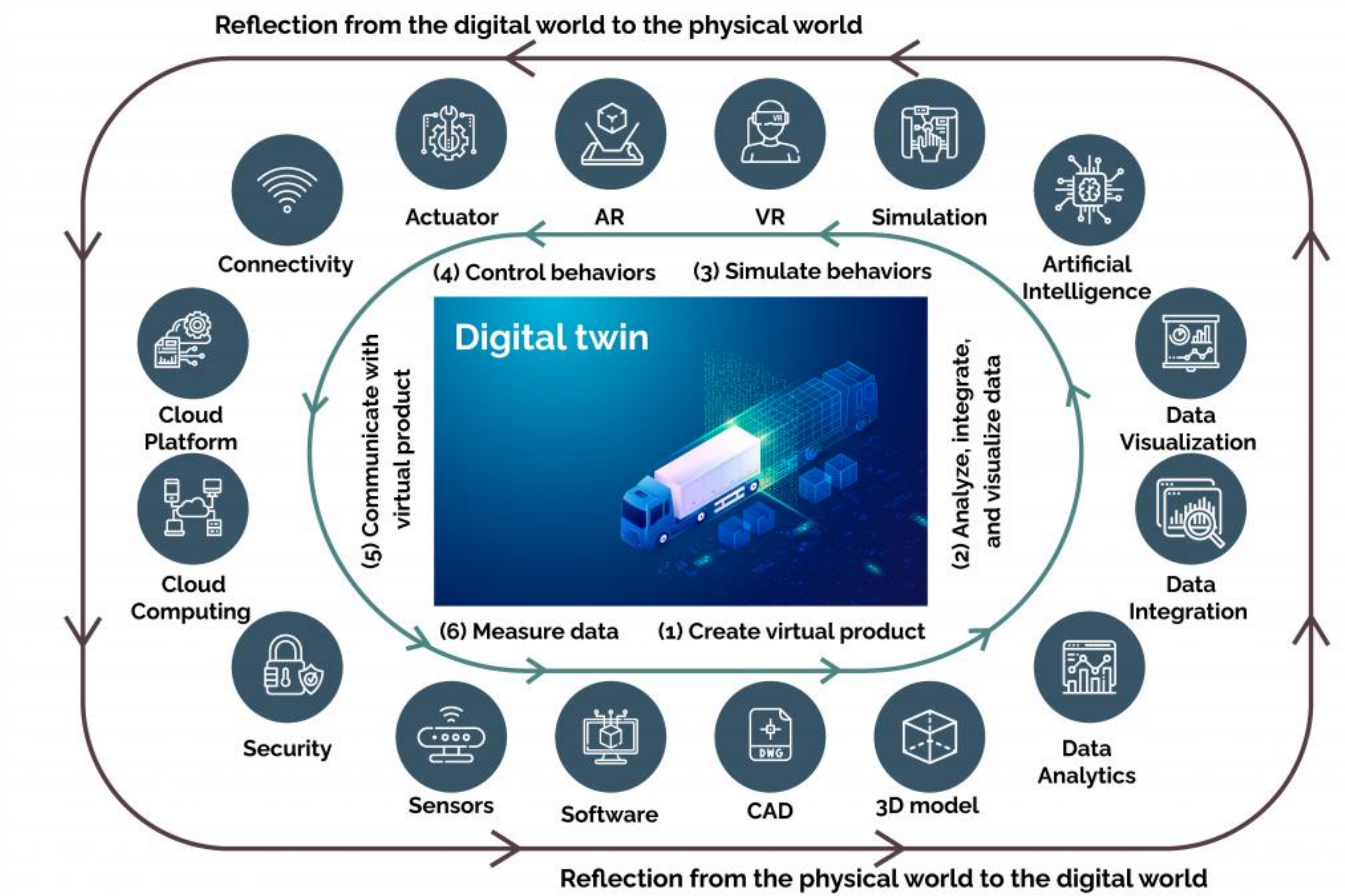

- **Action**: the tangible implementation of decisions, involving both automated and human-driven processes

# DT – Functional Architecture

```
+--------------------------------------------------------------+
|  +--------+   +--------+         +--------+          Network|
|  | App 1 |   | App 2 |    ...    | App n |      Application|
|  +--------+   +--------+         +--------+                 |
+---------------^---------------------+------------------------+
                |Capability Exposure|intent input
                |                    |
+------------------------------------v------------------------+
|                                            Network Digital Twin|
|  +---------+   +-------------------------+   +---------+     |
|  |         |   | Service Mapping Models  |   |         |     |
|  |         |   |  +-------------------+  |   |         |     |
|  | Data    +--->  |Functional Models |  +---> Digital|     |
|  | Repo-   |   |  +------+------^-------+  |   | Twin    |     |
|  | sitory  |   |         |      |          |   | Entity  |     |
|  |         |   |  +------v------+-------+  |   |  Mgmt   |     |
|  |         <---+  |  Basic Models      |  <---+         |     |
|  |         |   |  +-------------------+  |   |         |     |
|  +---------+   +-------------------------+   +---------+     |
+--------^----------------------------------------------------+
         |                             |
         | data collection             | control
+--------------------------------------v----------------------+
|                    Physical Network                          |
|                                                              |
+--------------------------------------------------------------+
```

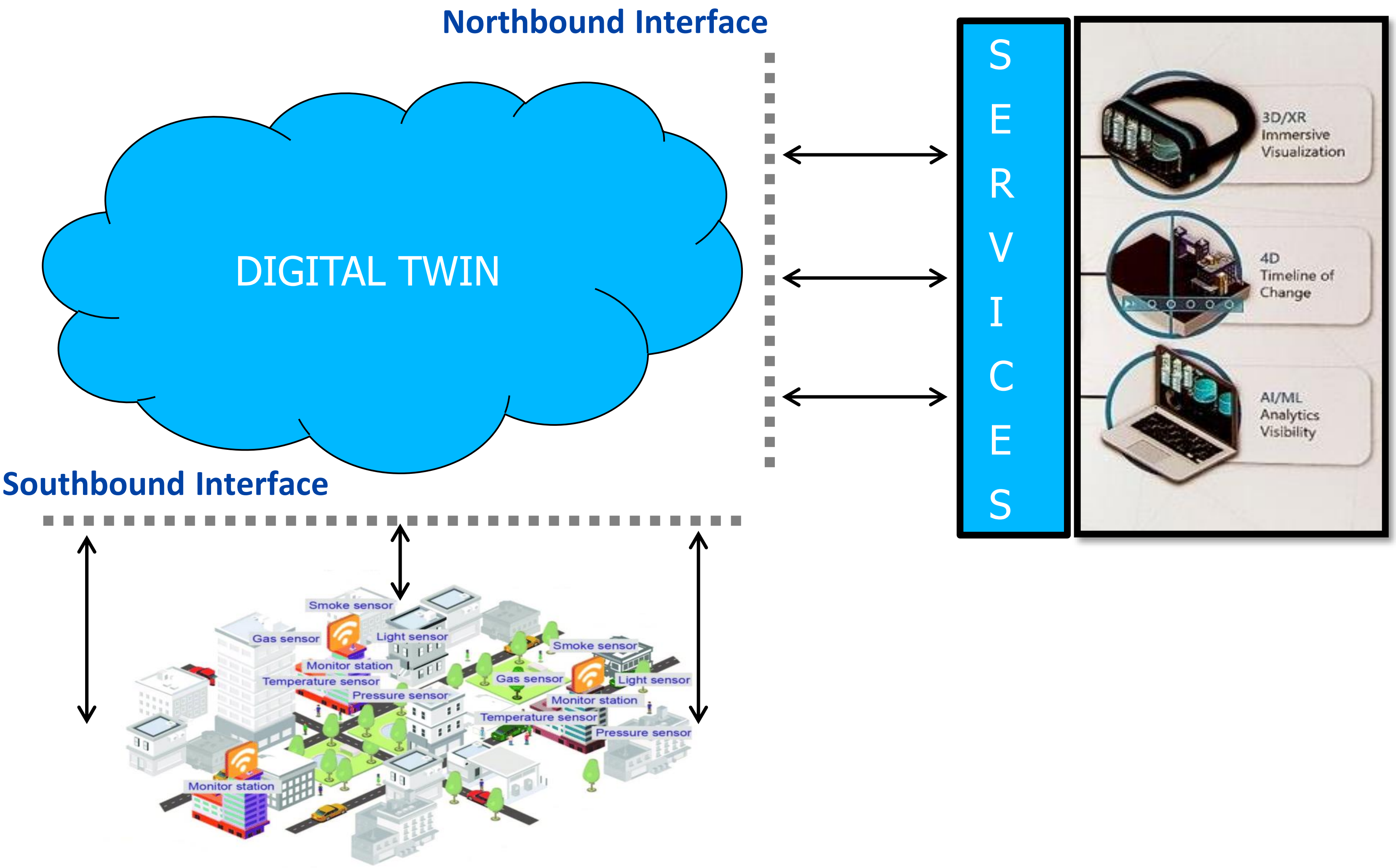
- Application Layer
- Digital Twin Layer
- Physical Layer

# DT Benefits



Reflection from the digital world to the physical world
Connectivity
Actuator
AR
VR
Simulation
Artificial Intelligence
(4) Control behaviors
(3) Simulate behaviors
Cloud Platform
Digital twin
(5) Communicate with virtual product
(2) Analyze, integrate, and visualize data
Data Visualization
Cloud Computing
Data Integration
(6) Measure data
(1) Create virtual product
Security
Sensors
Software
DWG
CAD
3D model
Data Analytics
Reflection from the physical world to the digital world

# *Interfaces*



Northbound Interface
DIGITAL TWIN
Southbound Interface
SERVICES
3D/XR Immersive Visualization
4D Timeline of Change
AI/ML Analytics Visibility
Smoke sensor
Gas sensor
Light sensor
Monitor station
Temperature sensor
Pressure sensor

# *Physical Layer*

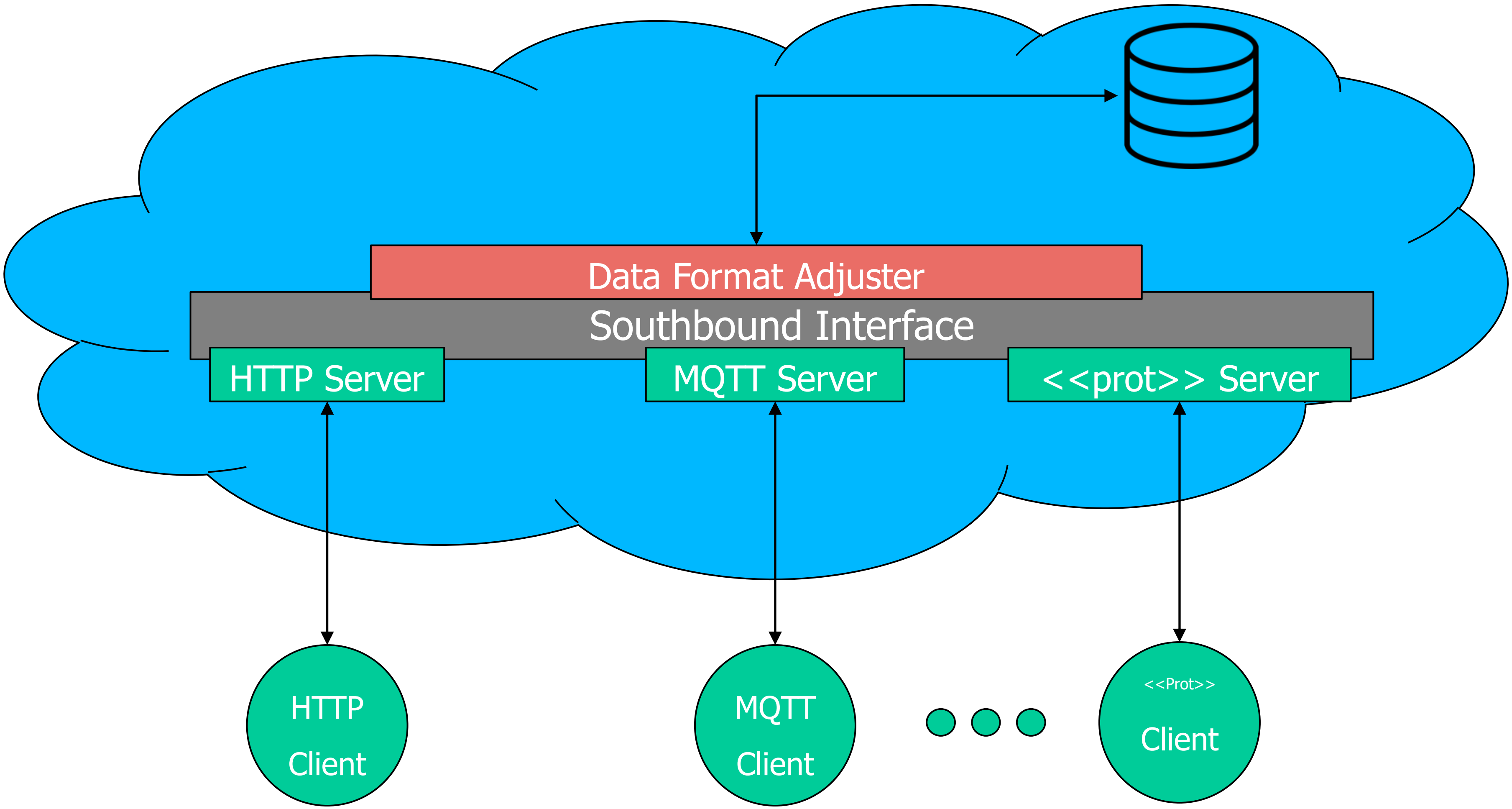
- **Devices Specification:**
  Defining the hardware components and sensors required for data collection

- **Network Design:**
  Address issues such as network topology, bandwidth allocation, redundancy, and security measures to ensure efficient and secure communication

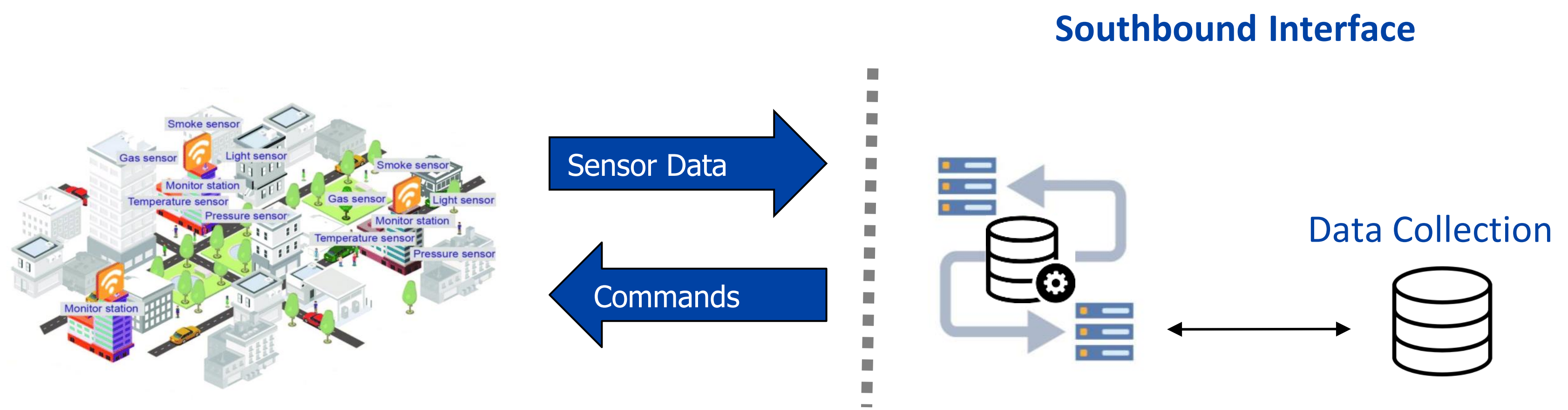
- **Communication Protocol Specification:**
  Select the right protocols (e.g., MQTT, CoAP, HTTP), to facilitate data exchange between devices and the digital twin platform

- **Domain Based QoS**:
  Tailor quality of service parameters (e.g., latency, reliability, bandwidth) to meet the specific requirements of the digital twin application domain

# BW Physical and DT Layer: the Southbound Interface

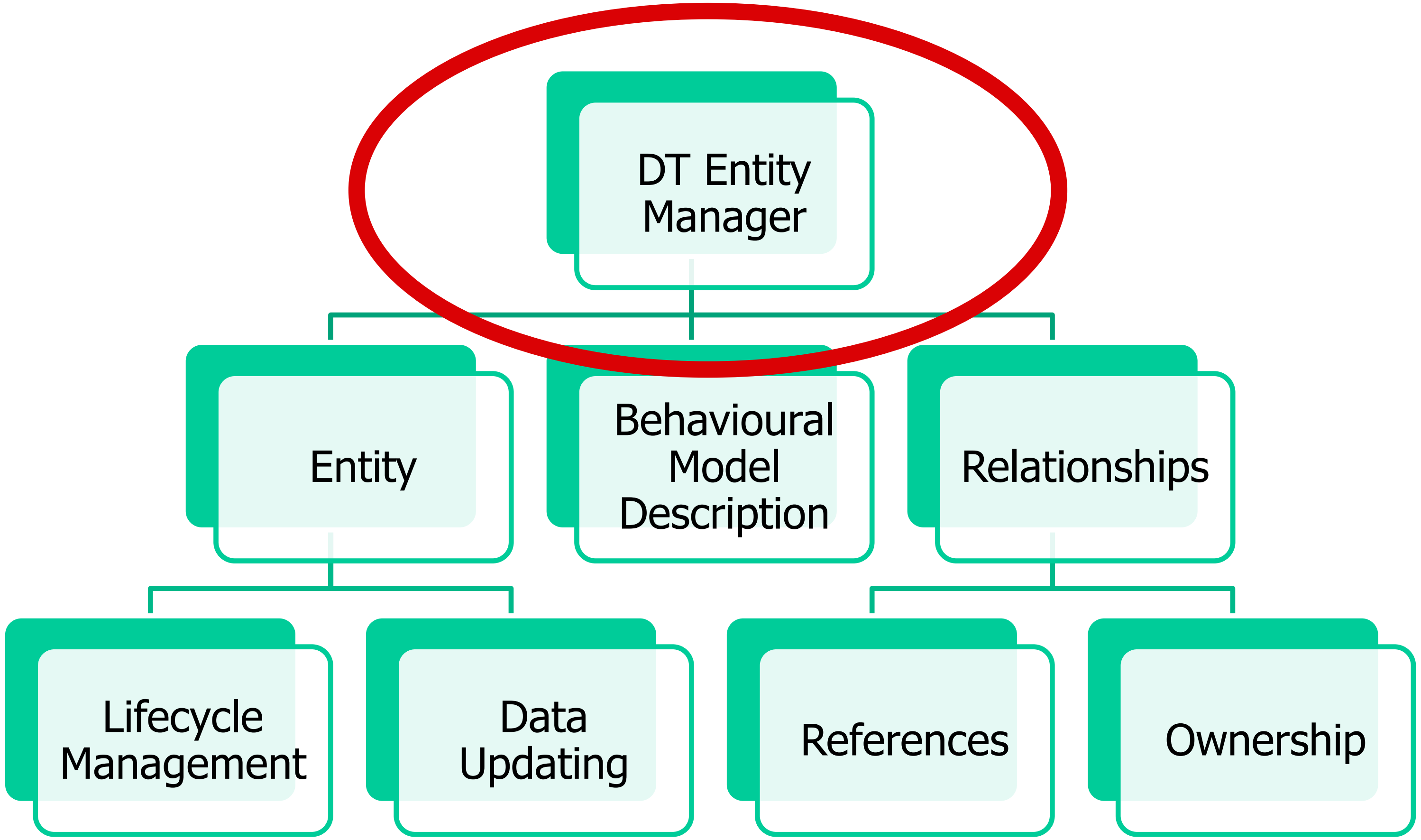


# DT Layer: Data Repository




- **Southbound Interface Specification:**
  Defines the communication methods and protocols for data exchange and control commands
- **Data Adjustment Procedures:**
  Standardization ensures that data from diverse sources conform to a common format and unit of measurement, enhancing consistency and comparability
- **RT Data Collection:**
  Captures dynamic physical conditions accurately and handles synchronization with low latency parts, to ensure that the digital model remains up-to-date with real-world changes

# DT Layer: Digital Twin Entity Mgmt

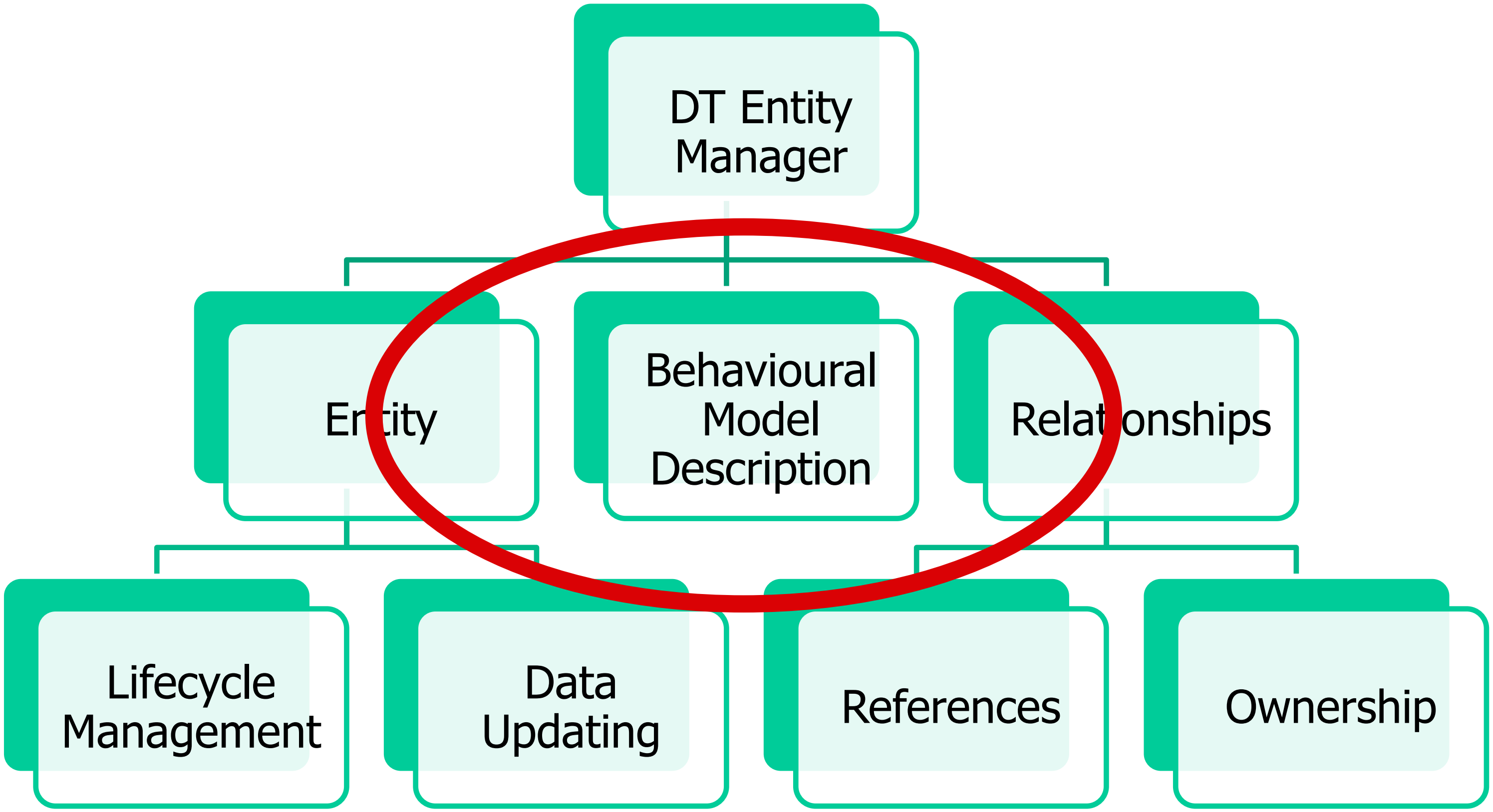


# DT Layer: Digital Twin Entity Mgmt

- The DT Entity Manager records the entity lifecycle and visualizes and controls various elements of the DT network, including:
  - Topology management
  - Model management
  - Security management

- At this level, the main components that can be identified include:
  - An activity ***monitoring service*** that is able to track tasks and functions within the DT
  - A **data extraction service**, which is able to analyze and visualize data both from the monitoring activities and from the data repository
  - **A management service**, which tracks the different agents within the DT according to their privilege level

# DT Layer: Behavioural Model Description



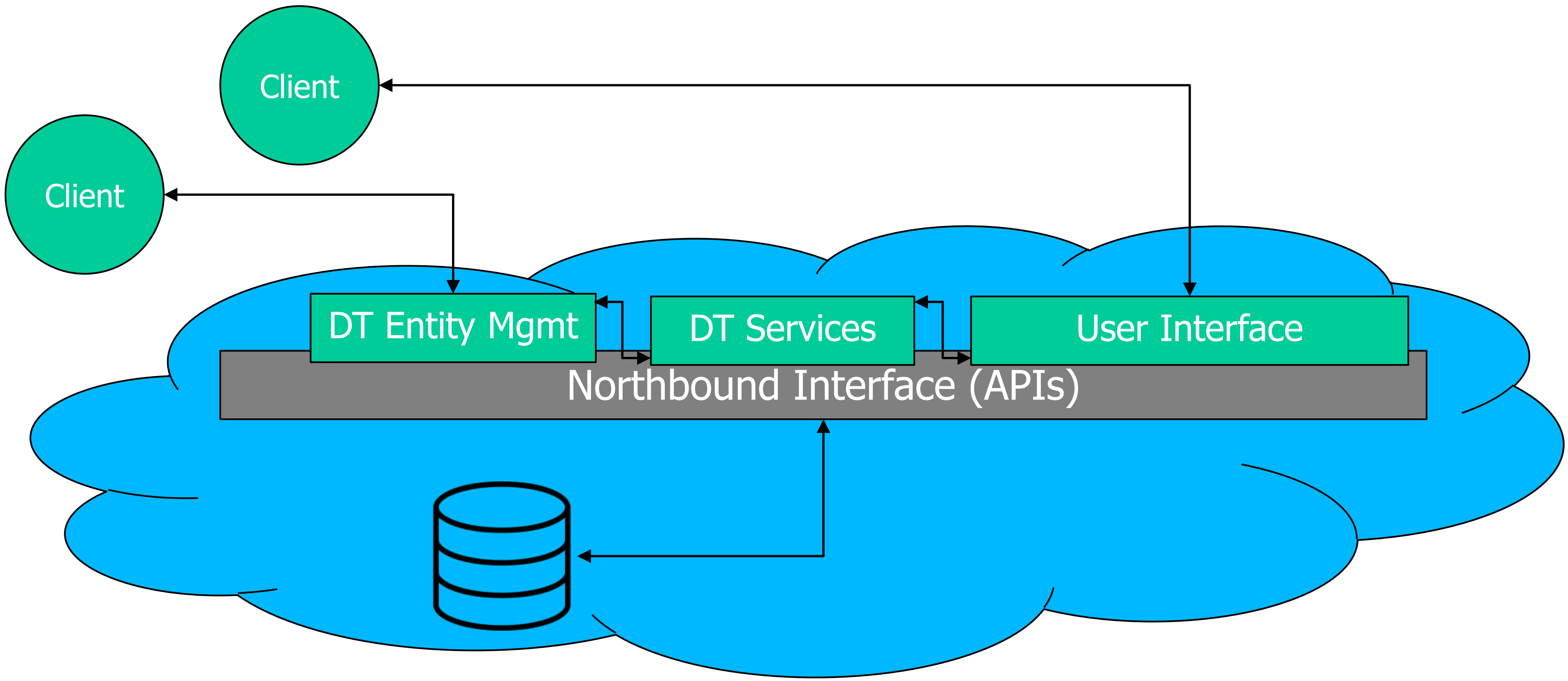
# Entities Behavioural Model

- A behavioral model denotes a representation of how a physical asset or system operates, behaves, and responds to various inputs and conditions within the framework of a digital twin environment

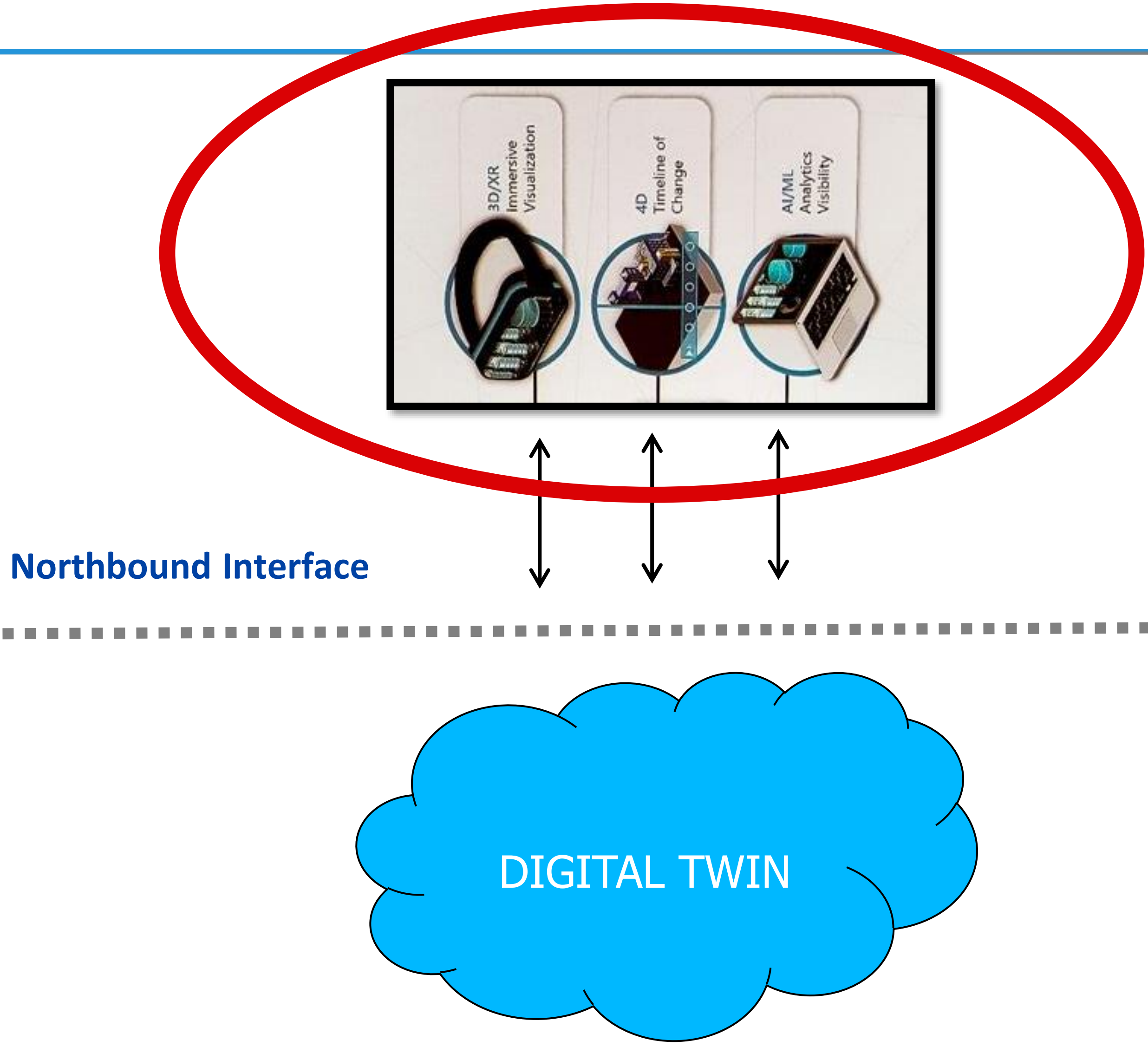
- Two main approaches are possible:
  - **Physics-Based Modeling**
    - Relies on physics-based equations and principles relevant to the asset or system being represented (these can include mechanical, electrical, thermal, or fluid dynamics models)
  - **Data-Driven Modeling**
    - Utilizes historical data from sensors and real-world observations to create predictive models that estimate future behavior

# BW DT and App Layers: the Northbound Interface

The Northbound interface specification in digital twins defines how information flows from the digital twin platform to higher-level applications and user interfaces, enabling data visualization, analytics, and decision-making, and ensuring seamless integration with external systems and stakeholders



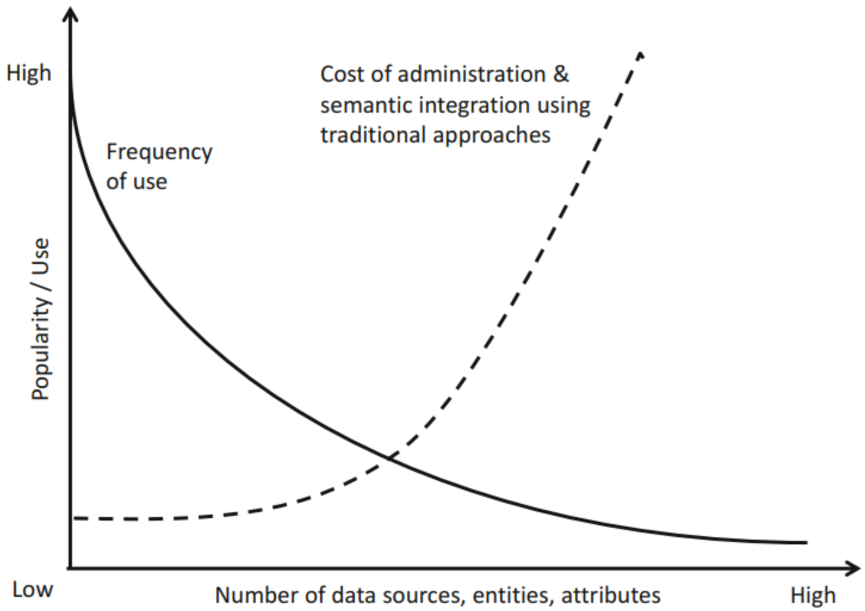
# Application Layer



# Data Spaces technology

# Big Data and The Long Tail of Data

- Rapid Data Expansion: we are witnessing a rapid proliferation of data in today's digital landscape
- Diverse Data Ecosystem: the data environment is becoming increasingly diverse, encompassing various types and origins of data
- Usability Challenges: the growing diversity of data can present usability challenges, as it may lead to difficulties in effectively harnessing and integrating this heterogeneous information

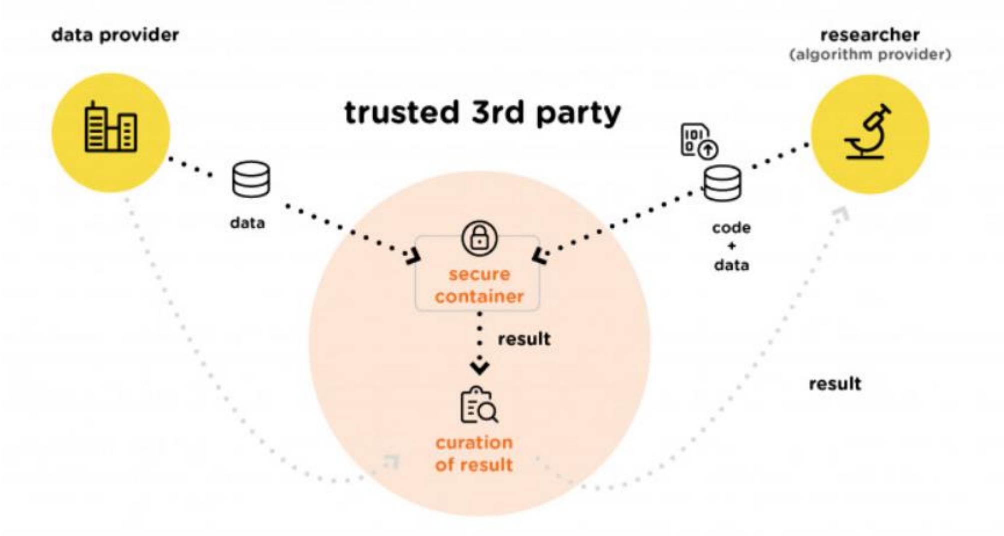



**Pareto principle:**

For many outcomes, roughly 80% of consequences comes from **20% of causes** → the "vital few"

# Traditional approach to Data Exchange/Sharing

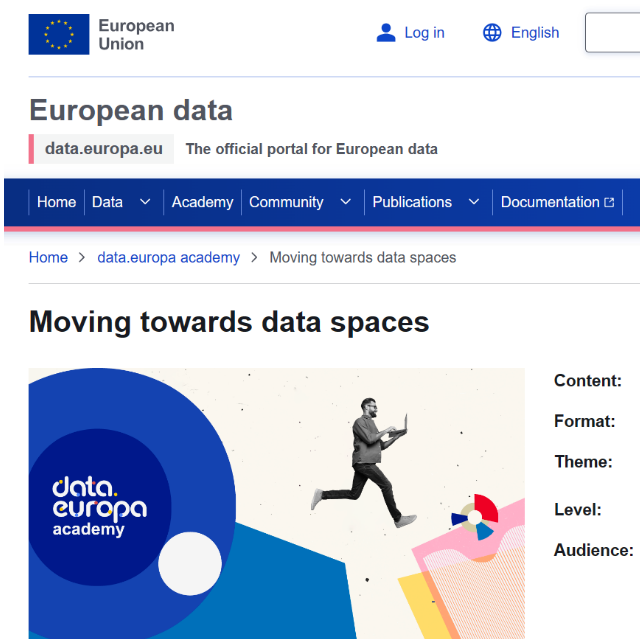
- Data exchange - and data sharing - typically occur through centralized systems or intermediaries
- Organizations and/or individuals have limited control over their own data, once it is shared
- Trust is in third parties, who are in charge of data management and security




- This potentially compromises data sovereignty

# European Strategy for Data

- The European strategy for data aims at creating a single market for data that will ensure Europe’s global competitiveness and data sovereignty

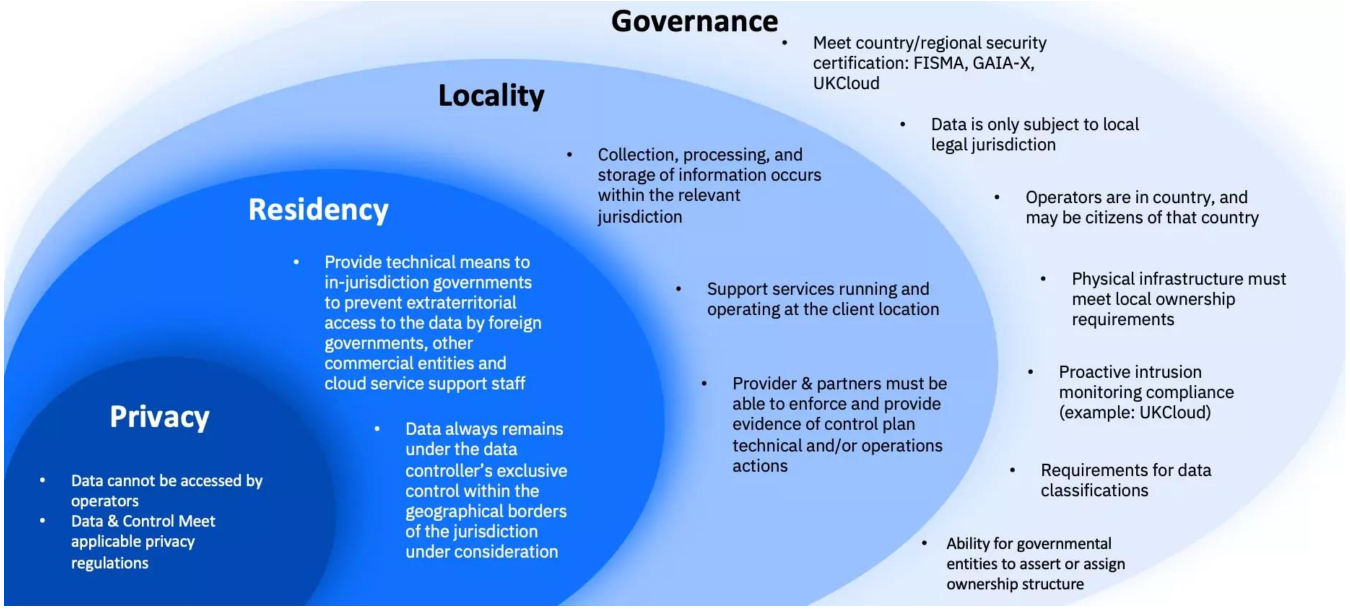




- Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control

# *The road to Data Sovereignty*

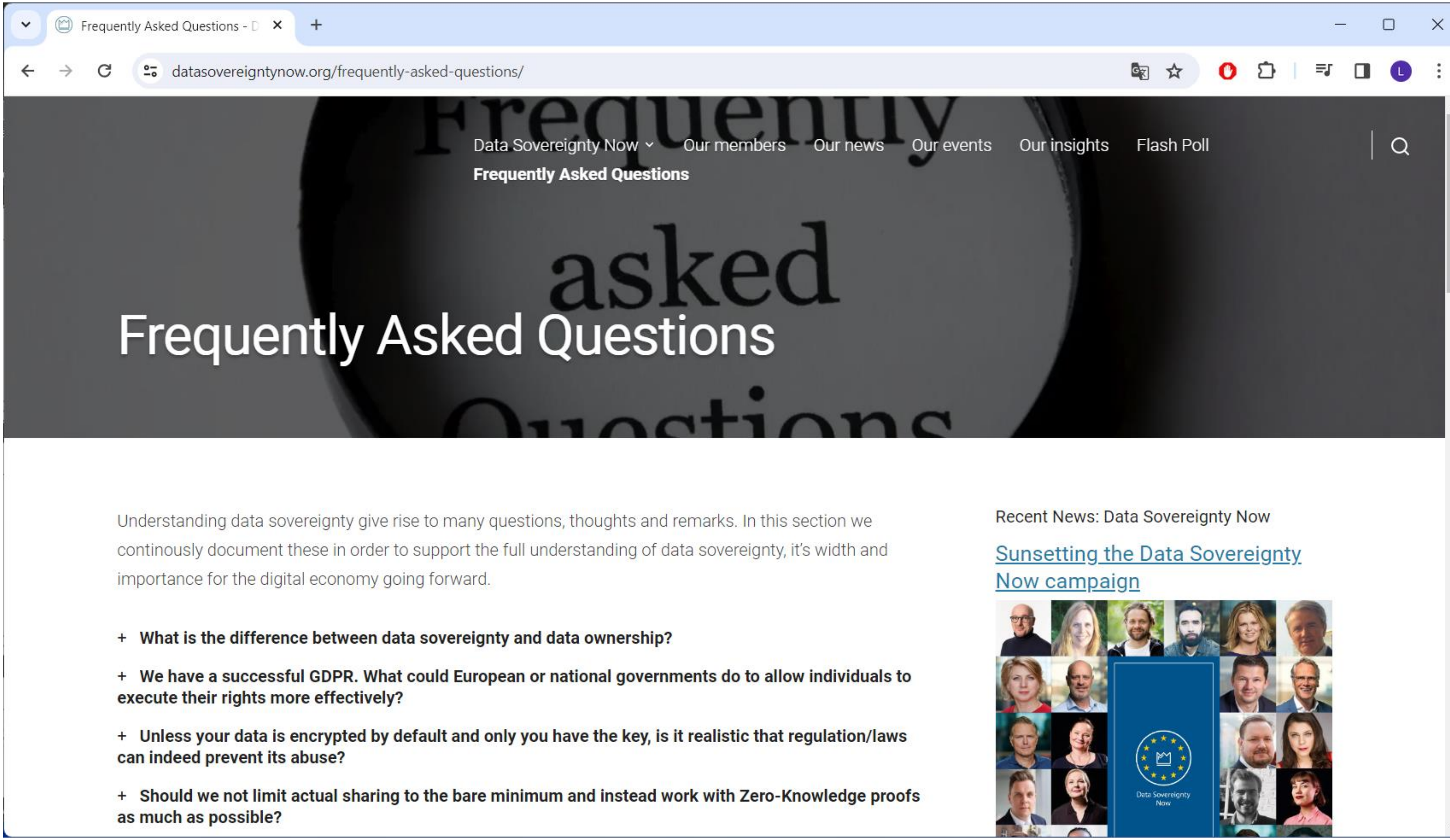
- Data sovereignty is the principle that asserts a nation's legal jurisdiction over data generated and stored within its borders, ensuring control and regulatory authority to safeguard data privacy and security

- It emphasizes the need to protect data from **foreign** or **unauthorized** access




[Data Sovereignty at the Edge - IBM Blog]

# Key Concepts



# FAQ (1/2)

- **What is the difference between data sovereignty and data ownership?**
  - Data sovereignty is the right to self-determination over data
  - In an ideal world the data owner – whether a citizen or a company – has control or ‘self-determination’ over their data
  - Data sovereignty is an instrument based on a fixed set of agreements (technical, functional, operational and legal) that reinforces the rights of data owners and puts them in control of their data

- **How can we ensure data security and privacy in the context of data sovereignty?**
  - Data security and privacy are design principles, and they too will be covered by the still-to-be-agreed standards for the soft infrastructure

# *FAQ (2/2)*

- **Consent can give us control about data, but giving consent is often too much effort (think of cookies) and we will be tricked into giving consent. So what alternatives are there to gain sovereignty in addition to more consent?**
  - An alternative to giving consent is a ‘soft’ infrastructure: central agreements between public-sector and private-sector organisations to regulate access to data
  - Individuals and organisations that conform to such agreements can share data with each other effortlessly, and have the practical tools to control who is allowed to access their data and under which circumstances

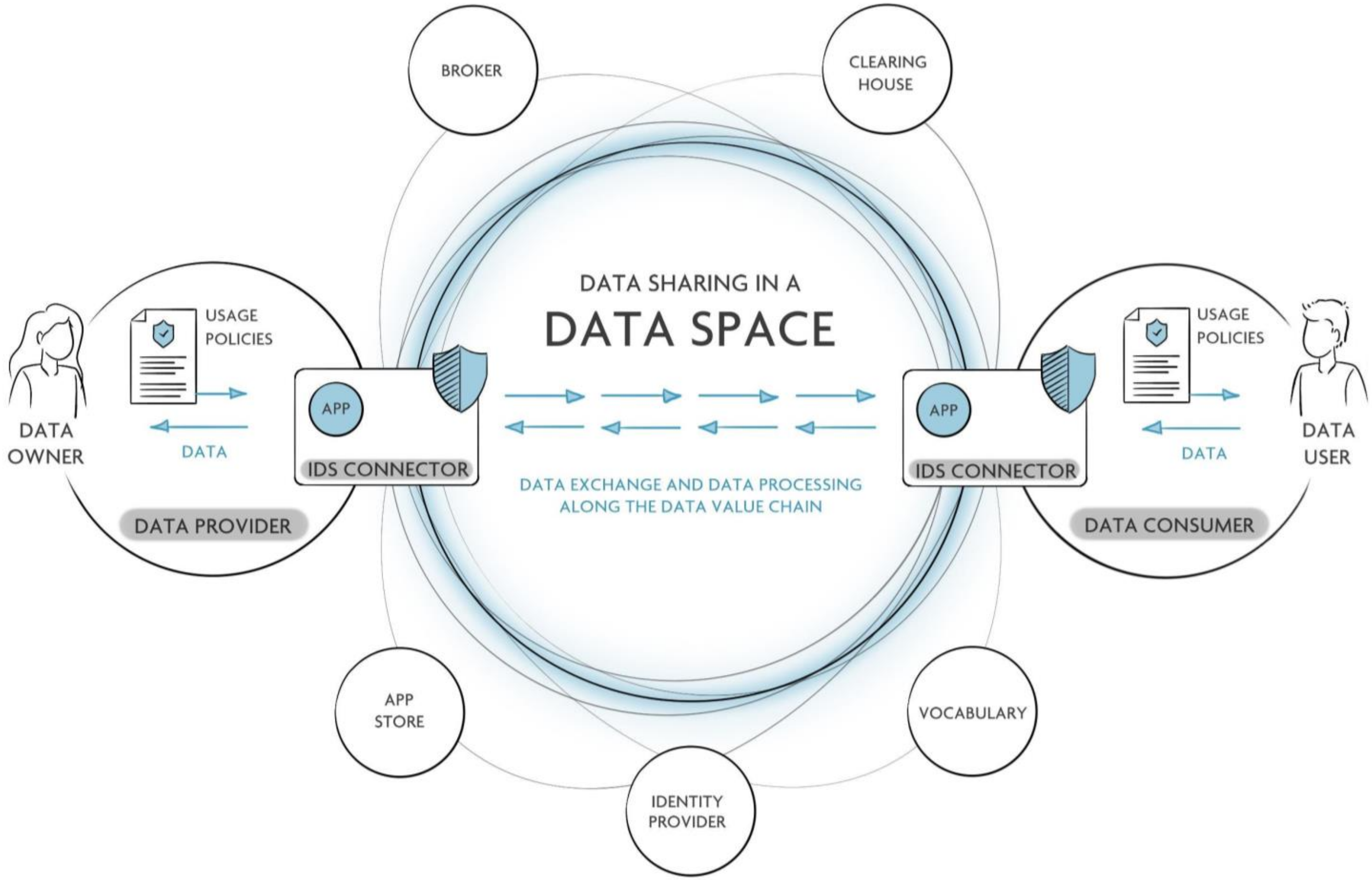
# The Data Space solution

- A data space solution creates a seamless ecosystem, where:
  - Data owners securely manage their information
  - Data providers offer valuable assets
  - Connectors facilitate seamless interactions
  - Consumers benefit from easy access to curated data

- Data Spaces foster efficient data sharing and collaboration

- Ultimately, they enable the Data Value Chain

# *IDSA view of Data Spaces*

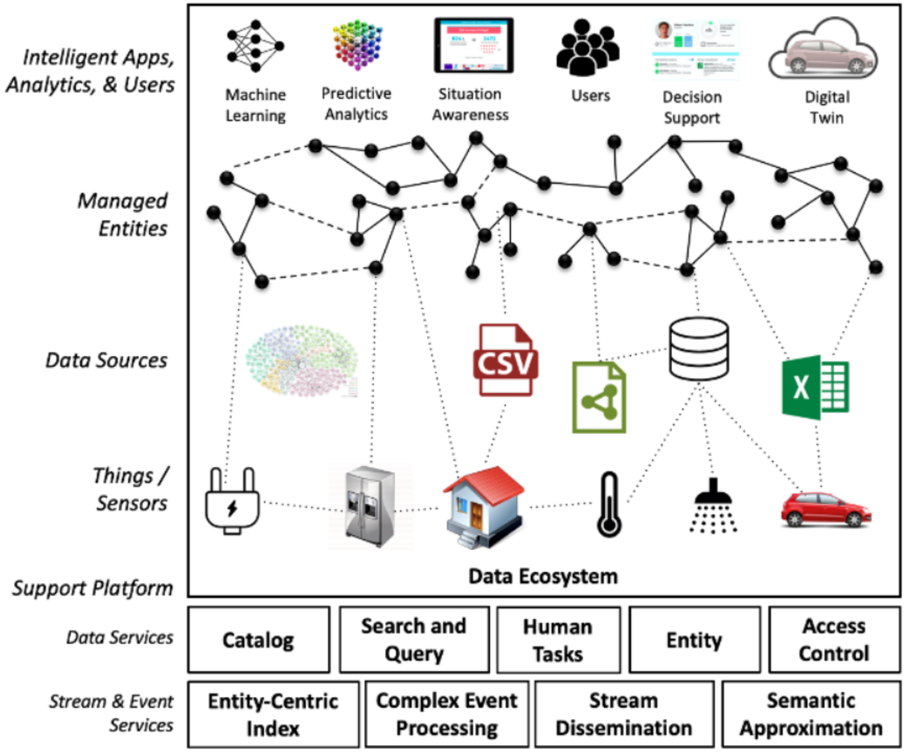





[Home - International Data Spaces]

# Data Spaces are not Datasets

- A dataspace represents a modern perspective on data management
- It acknowledges the complexities of large-scale integration scenarios, where numerous data sources are involved




- Within dataspace environments, various datasets coexist, yet they may not necessarily be completely unified or uniform in terms of their schemas and meanings

# Data Spaces are not Databases – 1/2

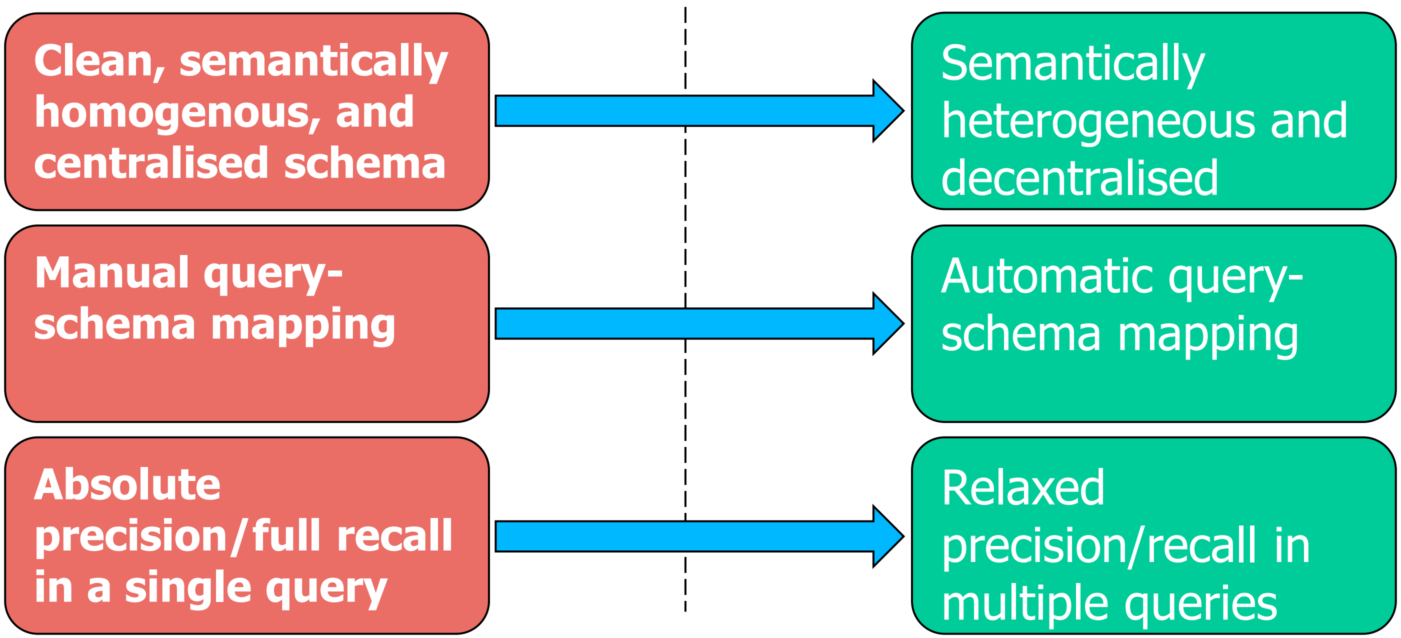
- **Schema:**
  - Databases follow a schema-first approach, requiring a structured schema before data entry
  - Data spaces allow for data-first entry and may even operate without a fixed schema
- **Control:**
  - Database management systems (DBMS) provide complete control over data
  - Data Spaces offer partial control, often allowing data to evolve more organically
- **Leadership:**
  - Databases typically follow a top-down leadership approach
  - Data Spaces may adopt a more flexible top-down or bottom-up leadership style
- **Query:**
  - Database queries aim for exact results
  - Data Spaces often involve approximate or flexible querying

# Data Spaces are not Databases – 2/2

- **Integration:**
  - Databases usually require upfront, comprehensive data integration
  - Data Spaces favor incremental integration as needed
- **Architecture:**
  - Databases tend to have a centralized architecture
  - Data Spaces can be decentralized, with data distributed across various sources
- **Real-time data processing:**
  - Real-time data processing is typically not applicable to traditional databases
  - Real-time data processing  is typically a significant aspect of Data Spaces, due to their dynamic nature

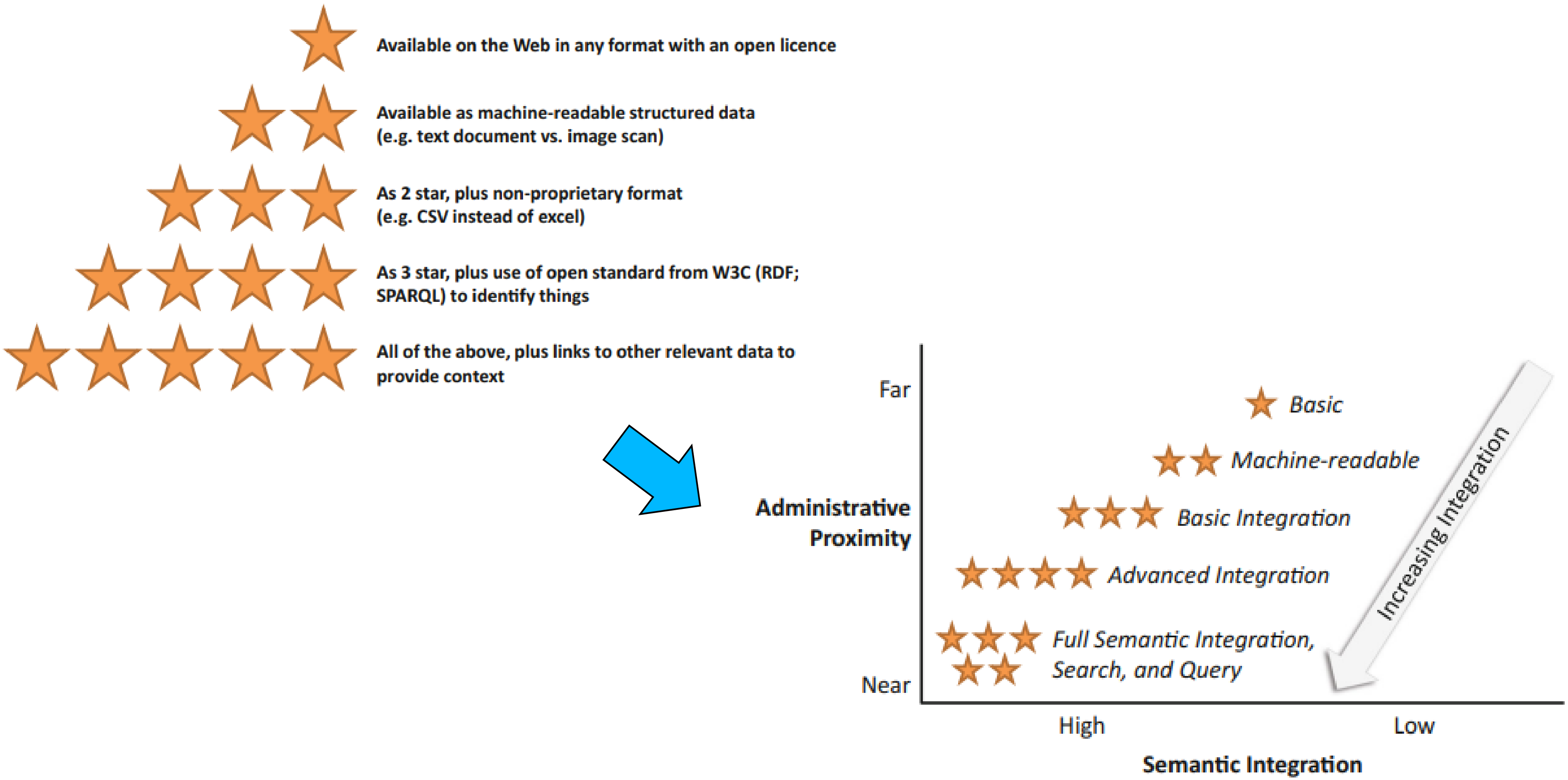
# *Approximate, Best-Effort, and "Good Enough"*

- The information approach of Approximate, Best Effort, and "Good Enough" recognizes that in many cases perfect accuracy is not necessary
- Focus is on providing reasonably accurate results quickly, which makes it well suited for the flexible and diverse nature of data in Data Spaces



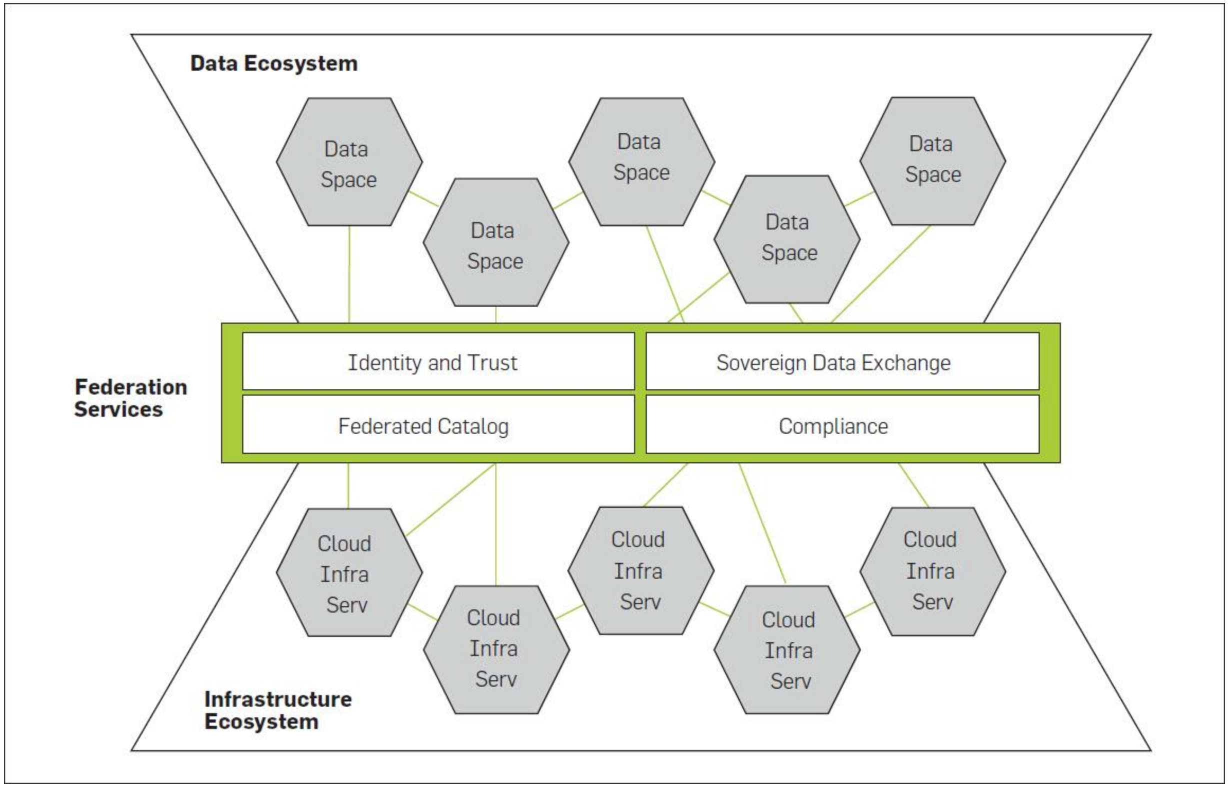
# Pay as-you-go fashion

When tighter semantic integration is required, it can be achieved in an incremental pay-as-you-go fashion by detailed mappings among the required data sources



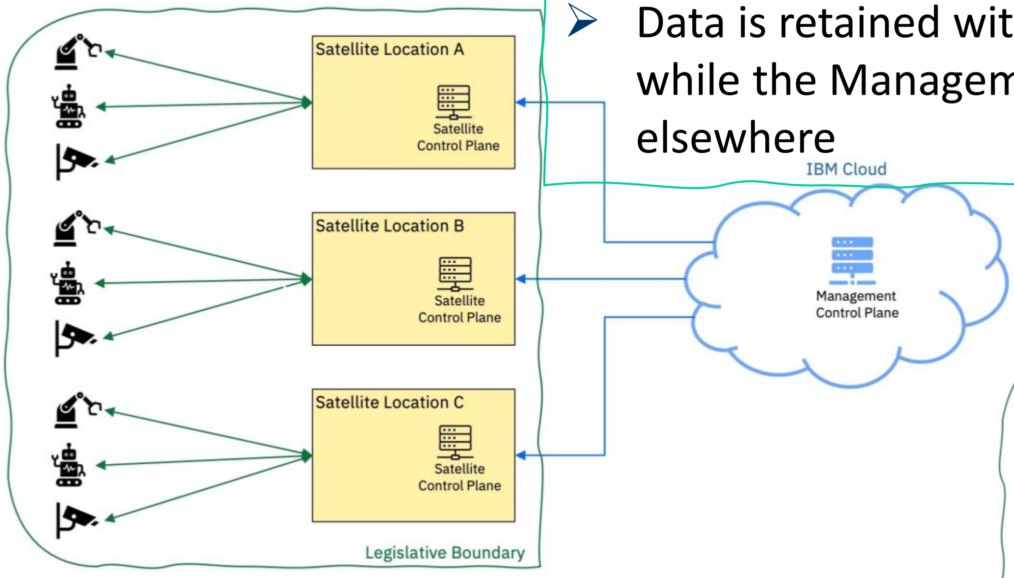
# Federated Data Spaces

Federation in Data Spaces refers to the collaborative network of interconnected data sources, each retaining control and sovereignty over its data while enabling seamless and secure data sharing among participating entities

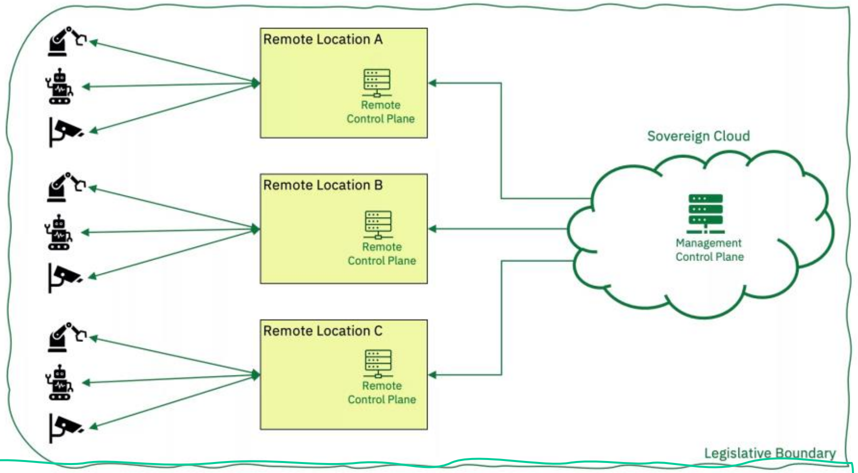



[https://cacm.acm.org/magazines/2022/4/259403-a-federated-infrastructure-for-european-data-spaces/fulltext]

# Sovereign Cloud



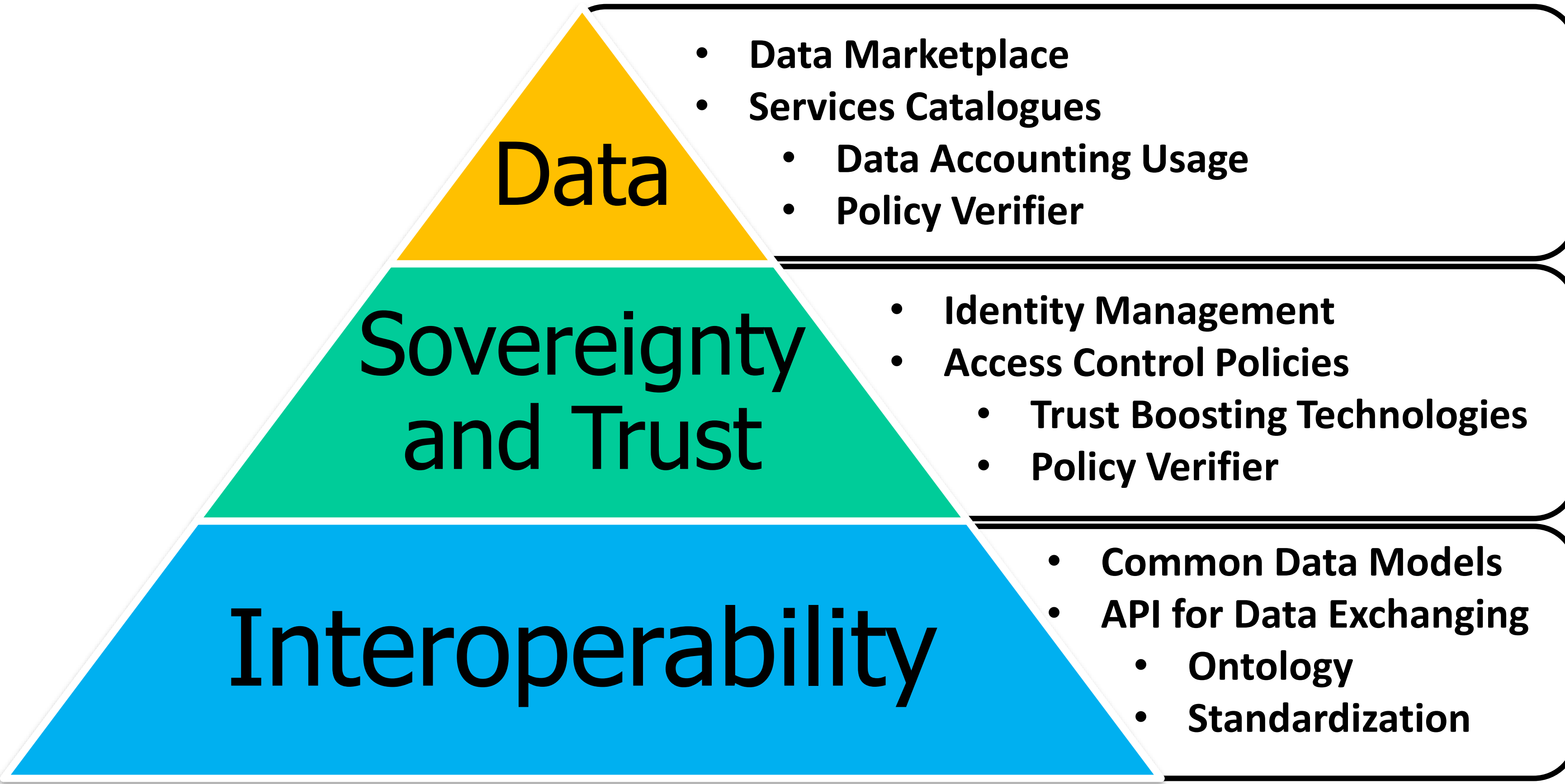

- Data is retained within the legislative boundaries, while the Management Control plane can reside elsewhere




- Data is stored locally within the legislative boundary, while the Management Control remains within the same legislative boundary

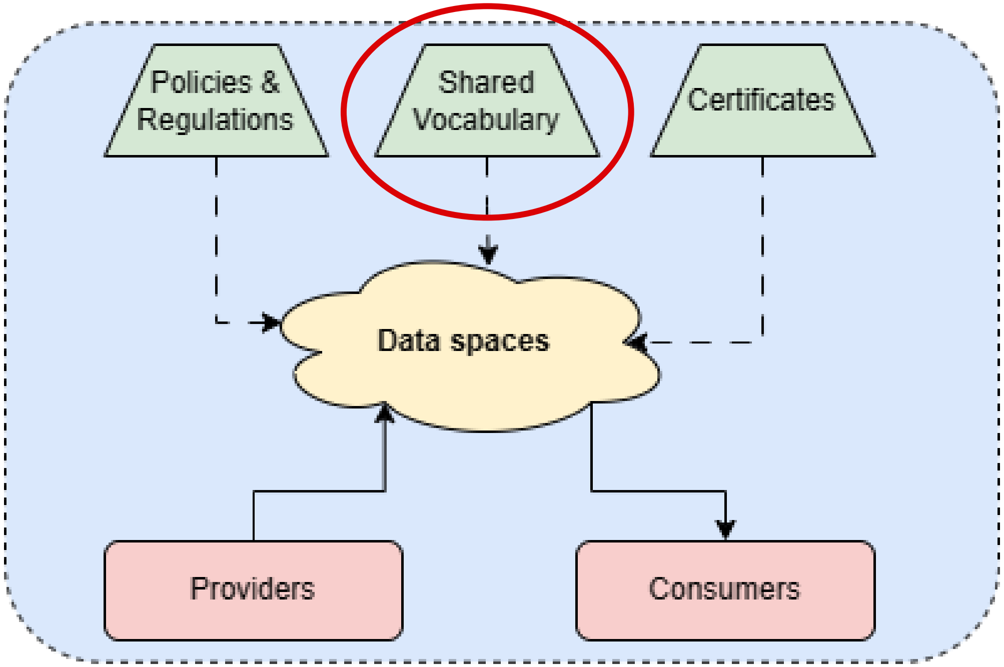
[Data Sovereignty at the Edge - IBM Blog]

# *Building blocks of Data Spaces technology*



# Data Spaces Interoperability

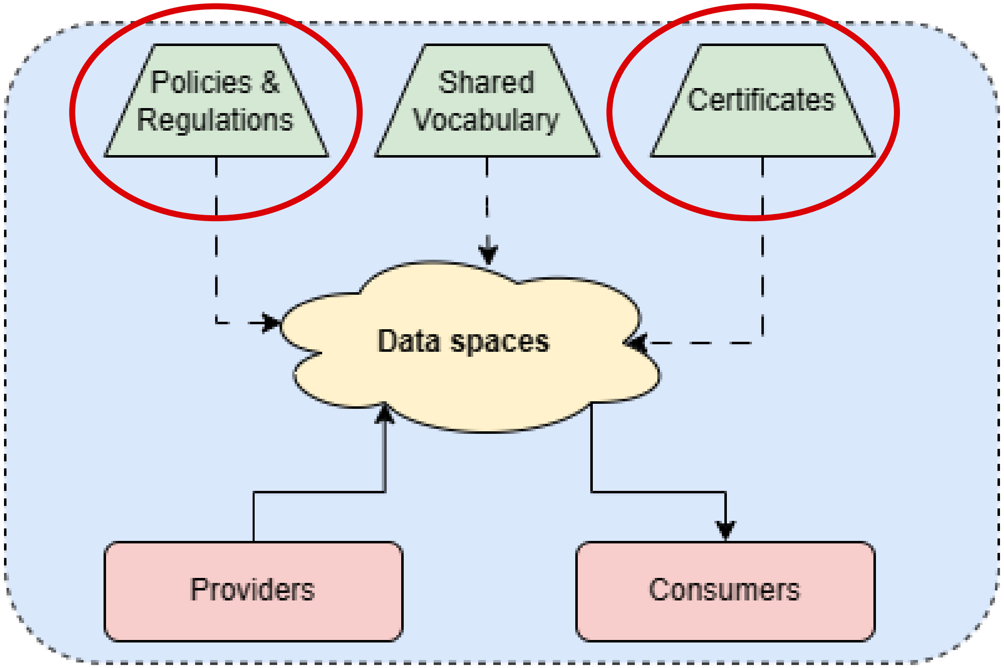
Data spaces achieve interoperability through the use of a shared vocabulary, enabling different data sources and systems to communicate and exchange information seamlessly




This common language ensures that data from various origins can be understood, integrated, and utilized effectively within the data space ecosystem

# Data Spaces Identity and Trust

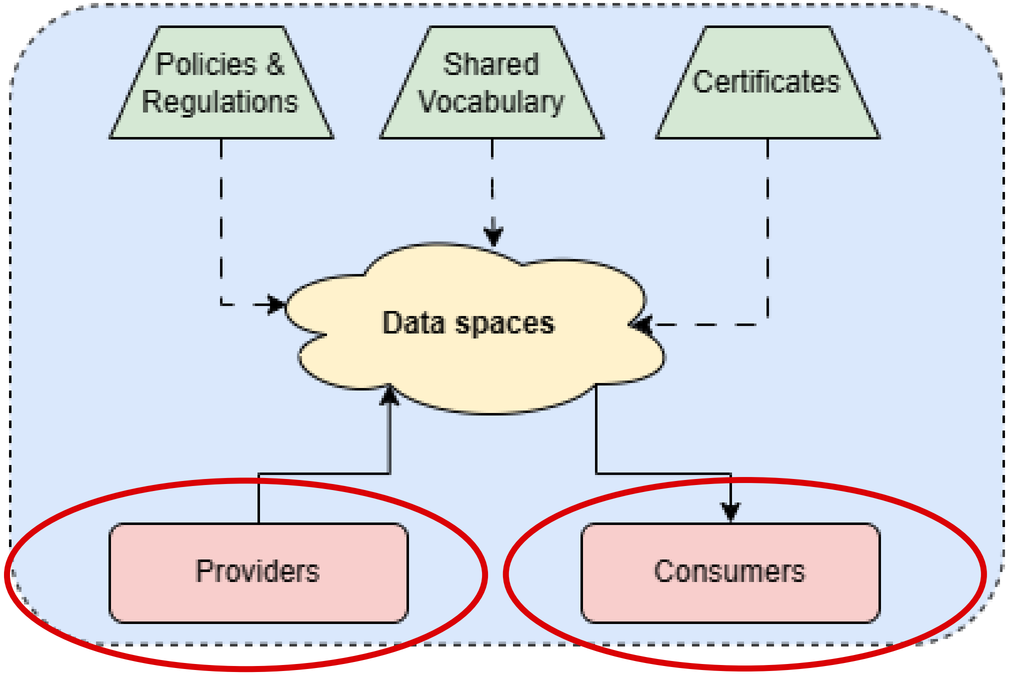
Data spaces establish identity and trust by implementing **policies and regulations** that govern data access and usage, ensuring data integrity and security




Additionally, the **certification** of computing nodes reinforces trust in the network infrastructure, assuring users of the reliability and authenticity of data transactions within the data space environment

# Data Value Chain in Data Spaces

Providers offer valuable data and services within the data space




Consumers can confidently access and utilize these offerings, underpinned by trust in the reliability and security of the data space platform

INTERNATIONAL DATA SPACES ASSOCIATION

# Data Spaces initiatives: IDSA

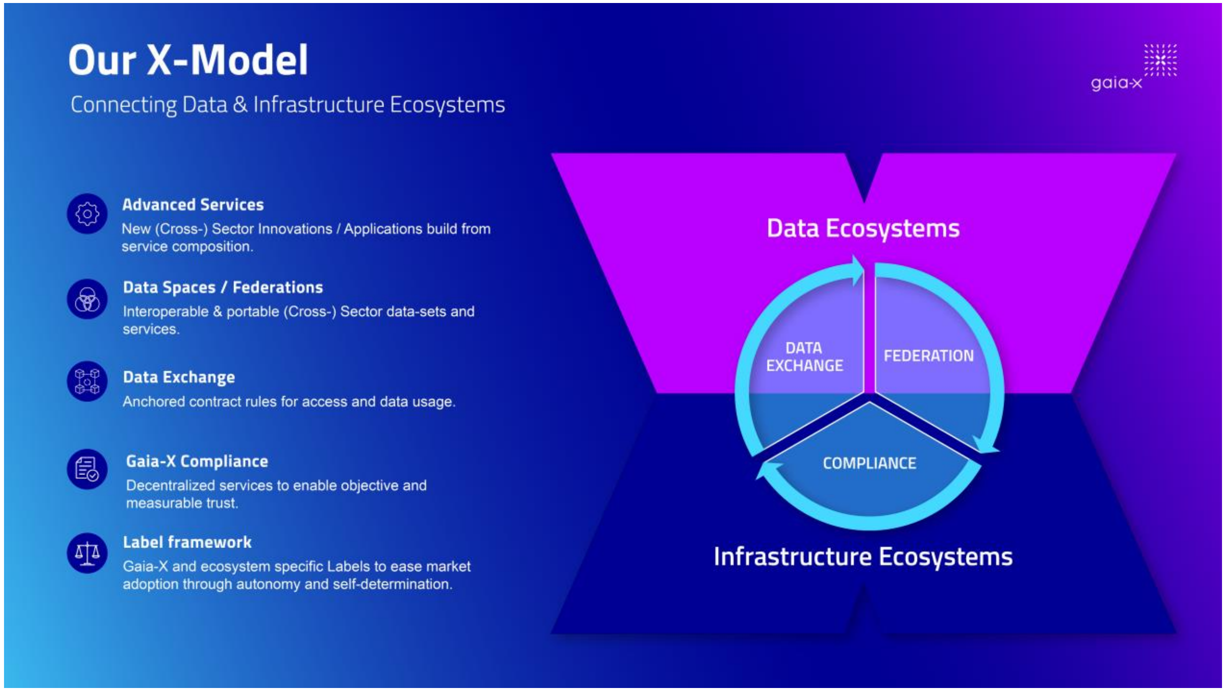
- The International Data Spaces Association (IDSA) is a global organization dedicated to promoting data sovereignty and secure data exchange

- It facilitates the development and implementation of standards and protocols that enable trusted and interoperable data sharing across international boundaries, fostering innovation and collaboration in the digital economy

- Two interesting things:
  - Minimum Viable Data Space Example with IDSA: [https://github.com/International-Data-Spaces-Association/IDS-Deployment-Scenarios/blob/main/Deployment-Scenarios/minimum-viable-data-space-top-ix.md]
  - A Minimum Viable Dataspace with Eclipse Dataspace Components utilizing Intel Software Guard Extensions: [https://github.com/International-Data-Spaces-Association/IDS-Deployment-Scenarios/blob/main/Deployment-Scenarios/minimum-viable-dataspace-with%20EDC-utilizing-Intel-Software-Guard-Extensions.md#a-minimum-viable-dataspace-with-eclipse-dataspace-components-utilizing-intel-software-guard-extensions]

# Data Spaces initiatives: GAIA-X

- GAIA-X is an initiative aimed at creating a secure, federated system that fosters the digital sovereignty of Europe
- It establishes common standards for data infrastructure and services, ensuring that data is stored and processed in ways that comply with European values and regulations, thus promoting transparency, openness, and trust in digital ecosystems.



# Data Spaces initiatives: FIWARE

- FIWARE is an open-source platform that provides a set of APIs and components for the development of smart solutions

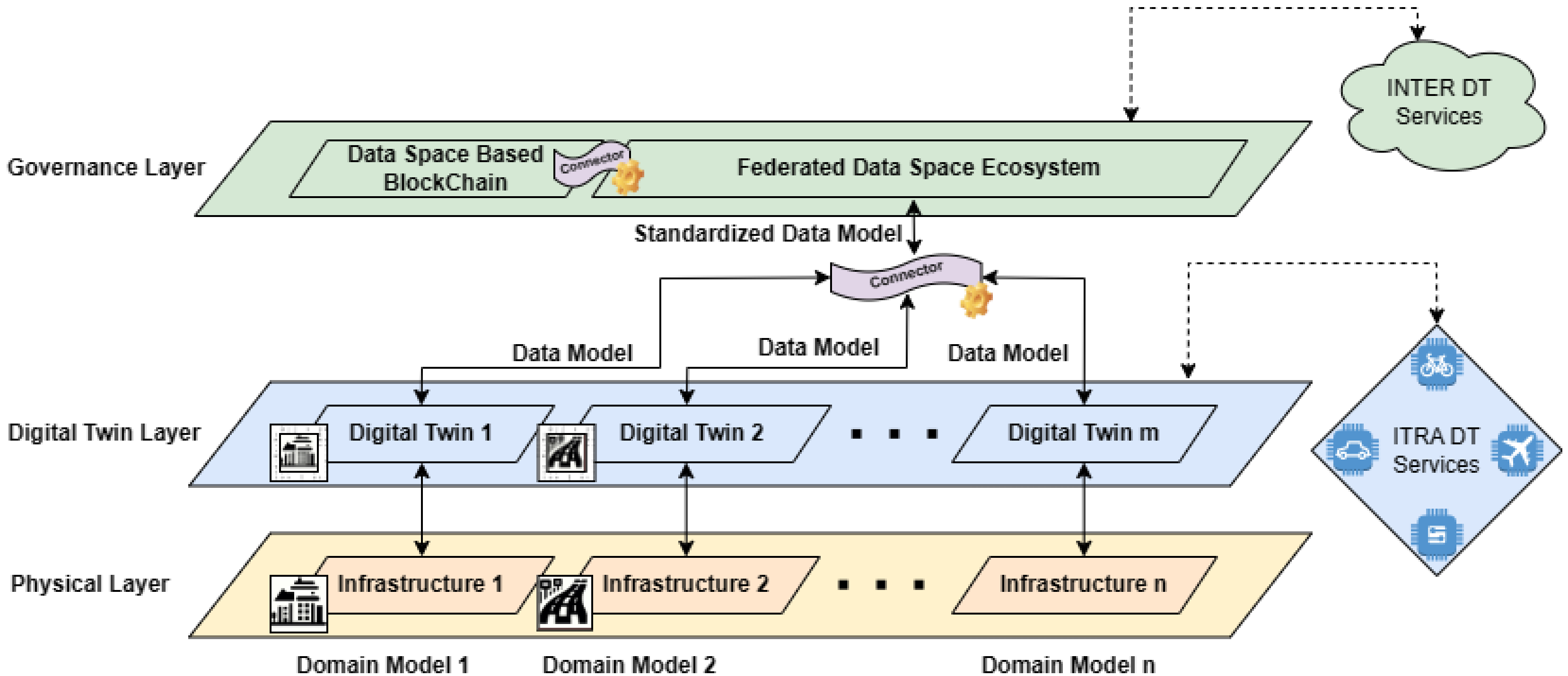
- It facilitates the management and processing of vast amounts of data in these environments, enabling interoperability, data sharing, and integration across different systems and platforms, which are essential components in the creation and operation of data spaces

- Interesting Links:
  - Smart Data Models repo: [https://www.fiware.org/smart-data-models/]
  - Tools and solutions catalogue: [https://www.fiware.org/catalogue/]

# An enabling DT/DS technology

# Digital Twins and Data Spaces

- Digital Twins and Data Spaces are closely linked
- DT/DS technologies enable the creation of services within a data space ecosystem, which effectively utilize the capabilities of digital twin entities



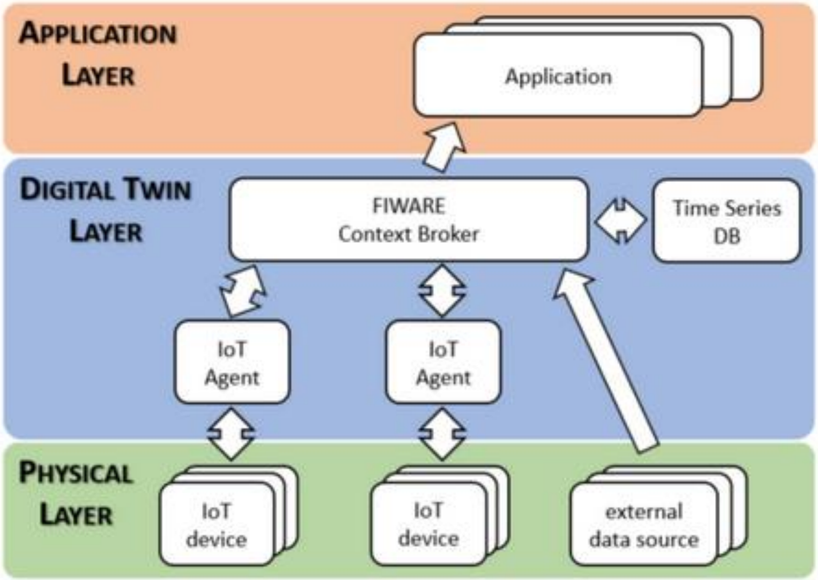
# FIWARE DT/DS solutions

**Context Broker:**

- Key component which facilitates the management of real-time context data
- Essential for creating and maintaining digital twins in IoT and smart city applications

**IoT Agents:**

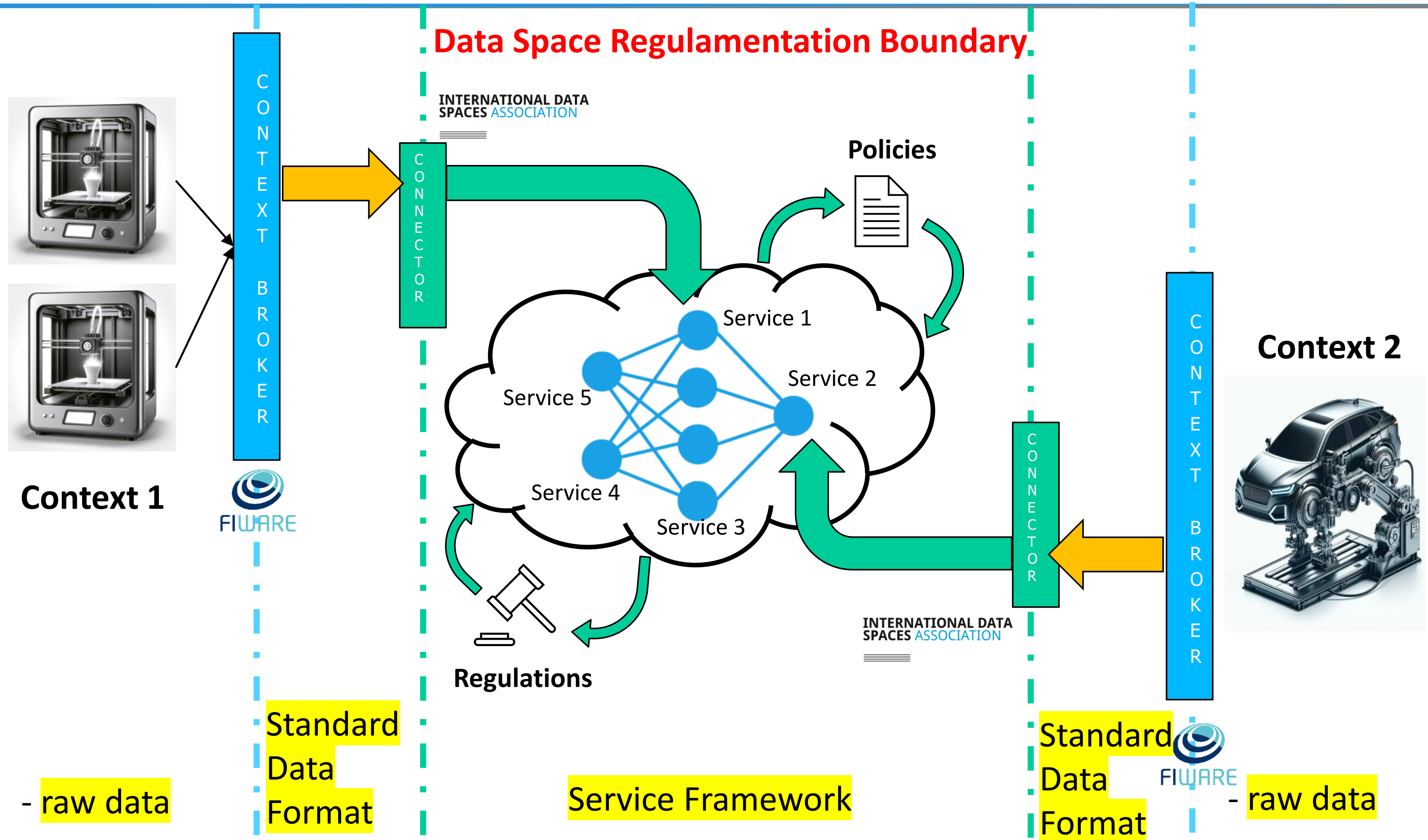
- Manufacturer-agnostic interfaces which enable seamless integration and communication between various IoT devices and platforms
- Favour interoperability and flexibility in IoT ecosystems




**Smart Data Models:**

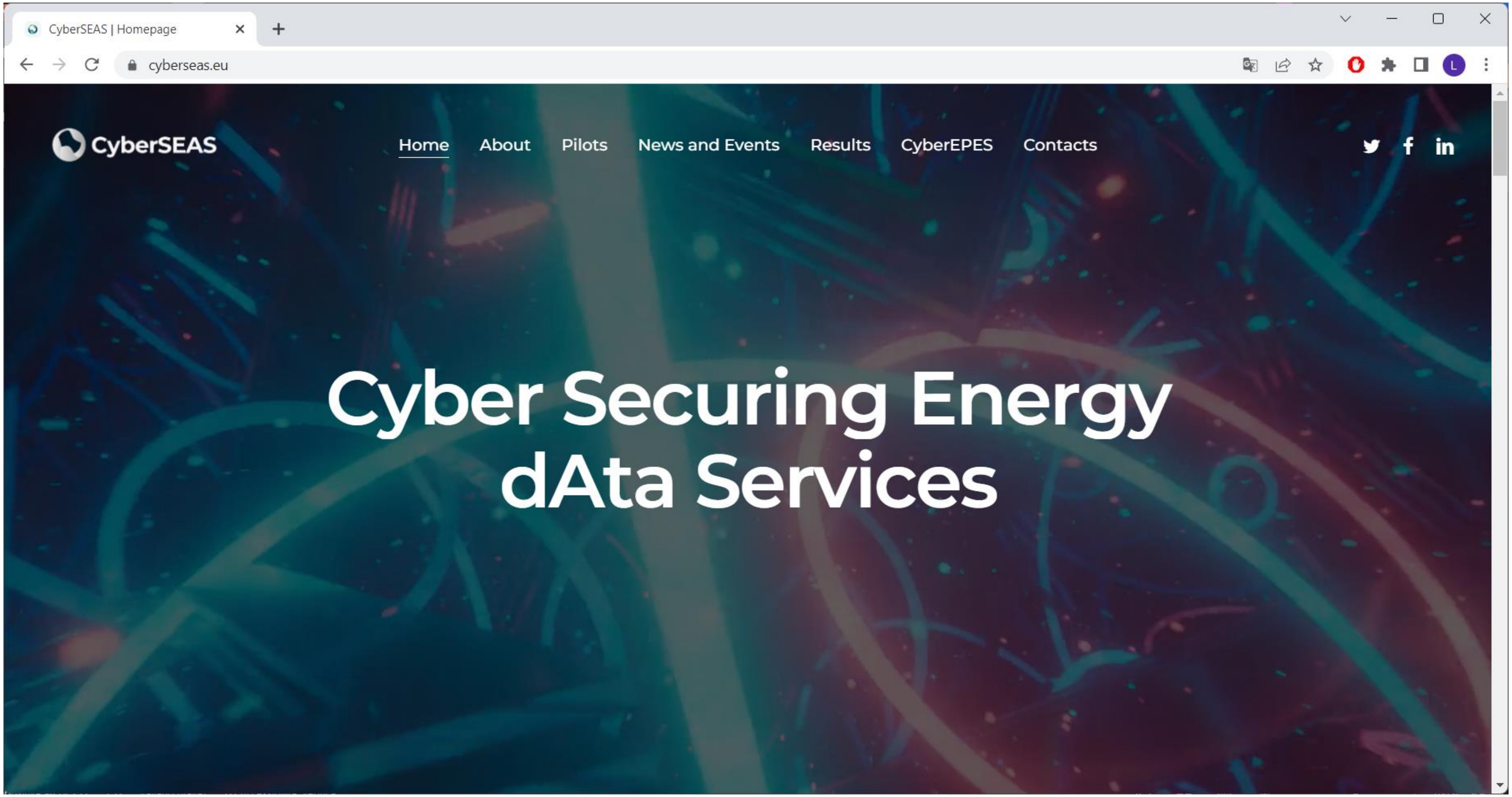
- Offer standardized data representations
- Promote compatibility and consistency in IoT applications and ecosystems

# FIWARE-based DT/DS setup



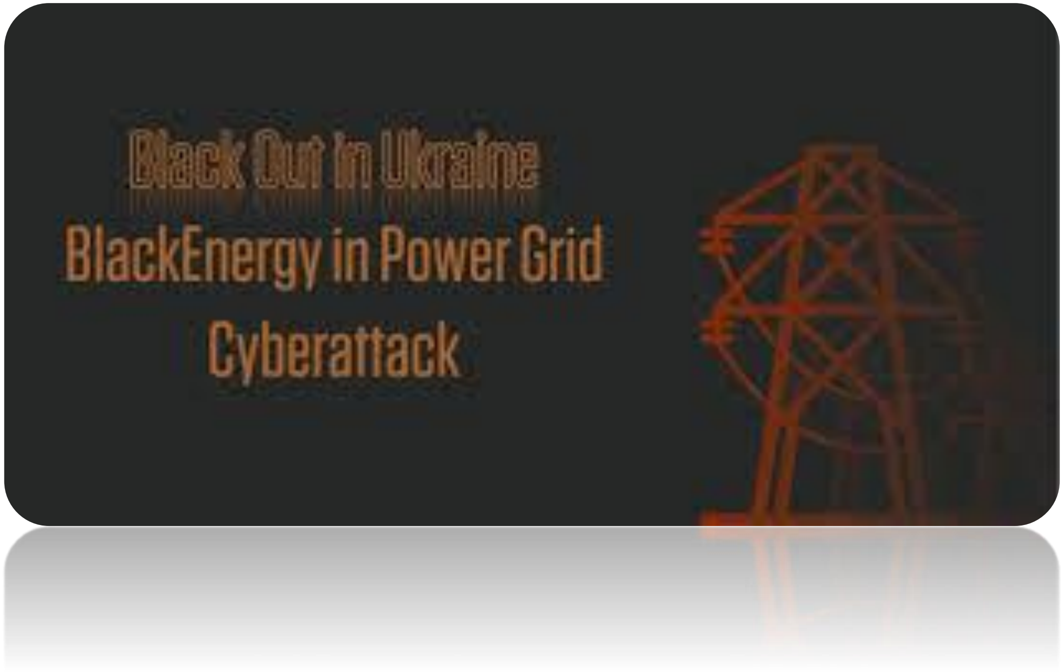
# Case study: Smart Grid

# *The CyberSEAS project*



# *Focus #1: high-impact cyber-attacks*

- Attacks, which:
  - Have the **highest potential of disrupting the business continuity** of critical elements in the energy distribution, but also
  - Most importantly, result in **major safety incidents**, with loss of lives and substantial damage to infrastructure (including cascading effects) and **critical privacy breaches**



# *Focus #2: renewable sources and legacy systems*

- Security issues resulting from:
  - The **increasing use of decentralized renewable energy sources**
  - The cohesistence of new devices and large proportions of **legacy systems** in extended energy supply chains involving a variety of diverse operators and consumers

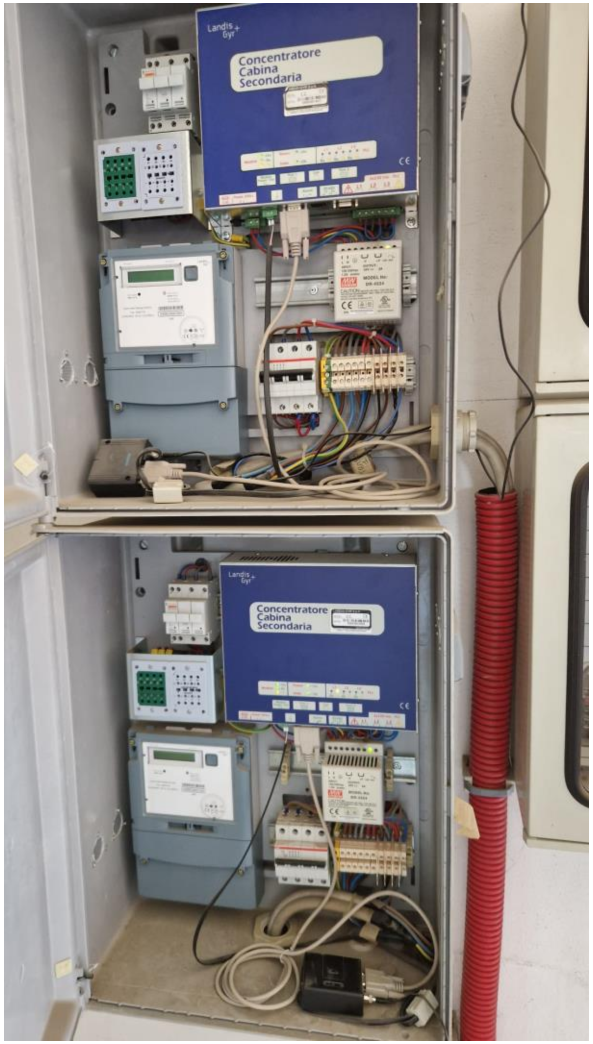
# *Focus #3: citizens' data and  Energy data space*

- Attacks targeting:
  - **The confidentiality of citizens'** data
  - **The privacy and the integrity of the Energy data space** in general

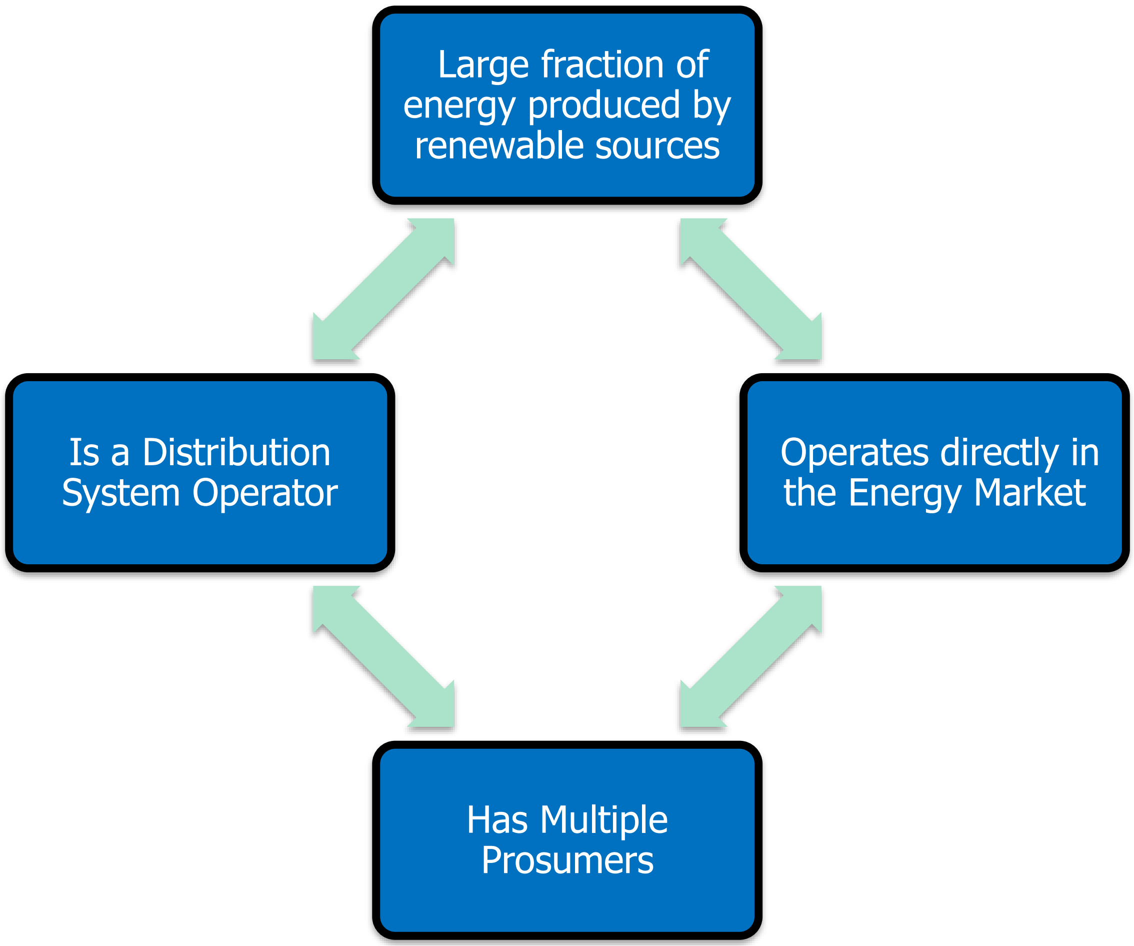
# *The Italian Pilot Smart Grid*

BERCHIDDA & BENETUTTI
ENERGY COMMUNITY


# Berchidda & Benetutti Smart Grid

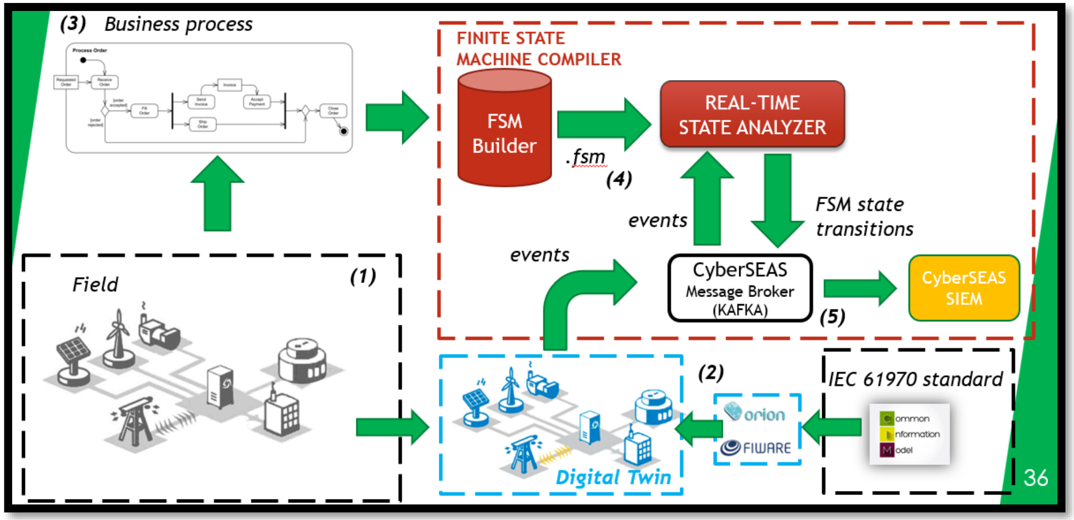




# Berchidda & Benetutti Smart Grid Characteristics



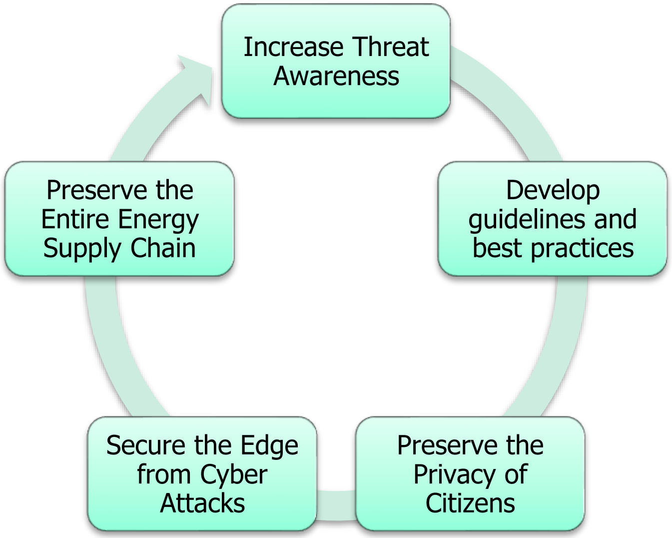
# Digital Twin Monitoring

- To monitor the smart grid, we have constructed a digital twin of the infrastructure
- The behavioral model is based on the business process specification of the power grid
- The structural model of the digital twin is based on the IEC61970 Standard and adapted via FIWARE Smart data models
- The solution is fully compliant to the data space view of interoperability and ontology-based interactions

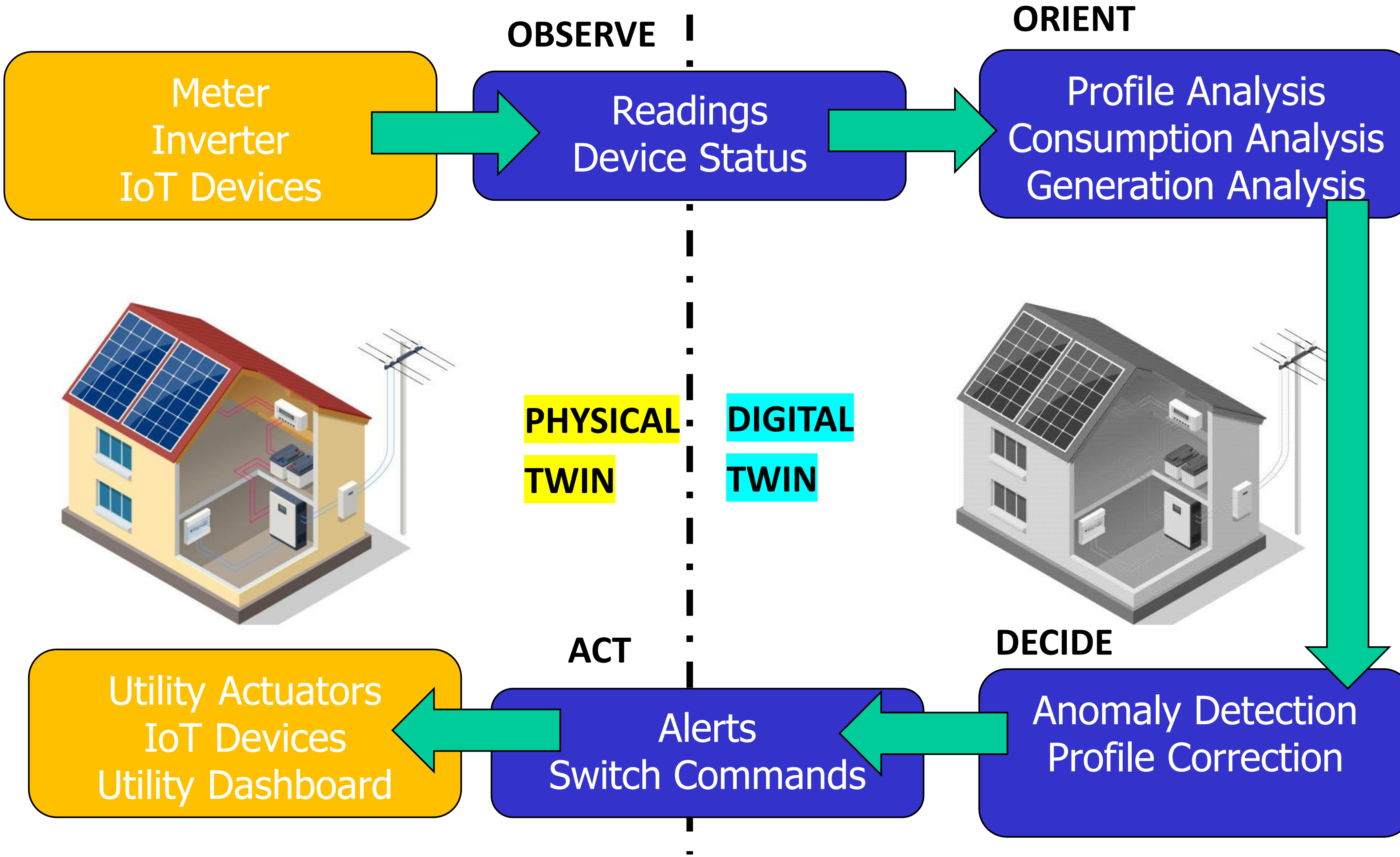


# *Prosumer-centric approach*

- Prosumers – i.e. individuals who both produce and consume energy – are increasingly vulnerable to cyberattacks
- **The interconnected nature of energy systems** can be exploited, posing threats both to energy assets and to personal data
- **Lack of robust cybersecurity guidelines** and **threat awareness** is an important factor to be taken into account

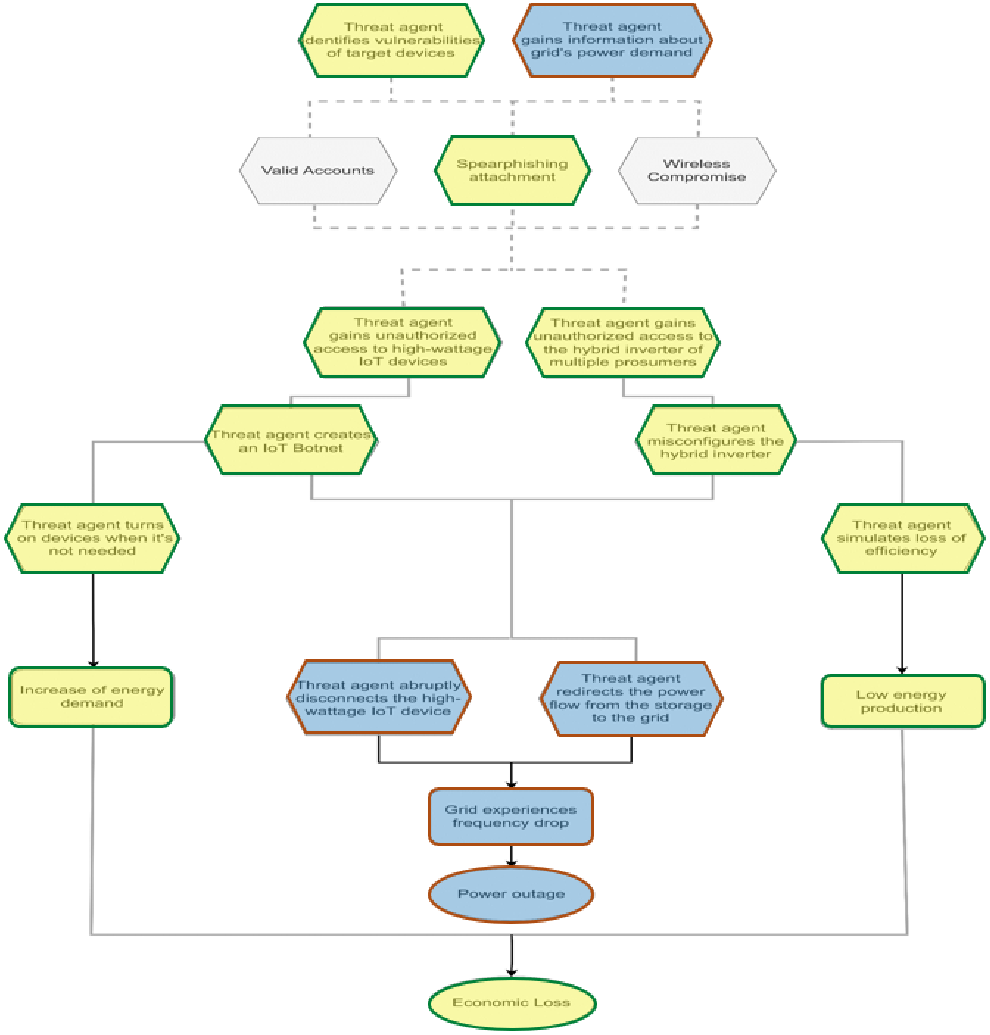


# *The OODA Loop in Smart Grid Monitoring*

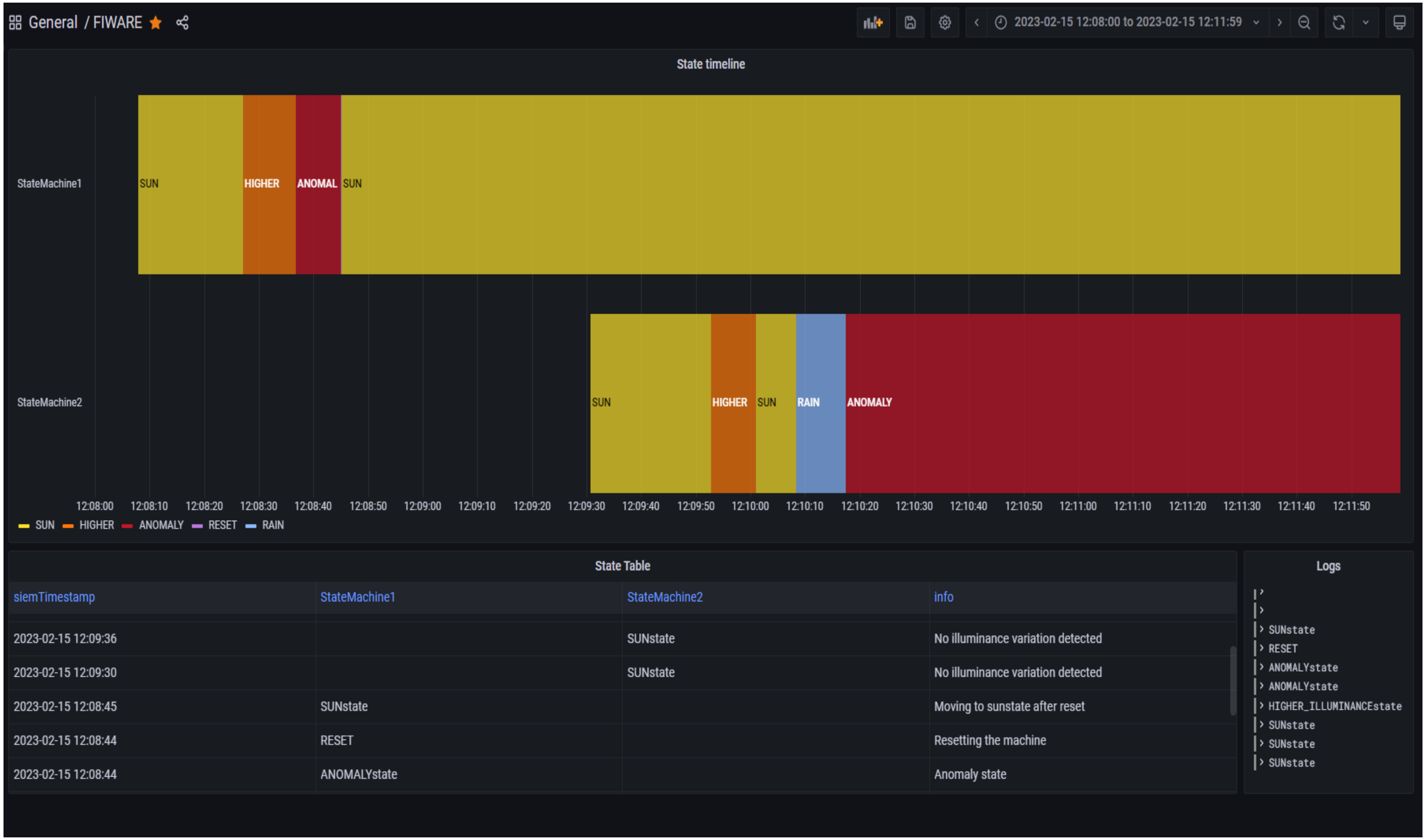


# Attack Scenario

- Threat agents start to identify vulnerabilities in the target devices
- A malicious user gains access to multiple prosumer networks via spearphishing attachments
- The malicious user manages to gain unauthorized access to the hybrid inverter of multiple prosumers
- The threat agent starts misconfiguring the hybrid inverter
- Through misconfiguration, the threat agent simulates loss of efficiency from renewable sources

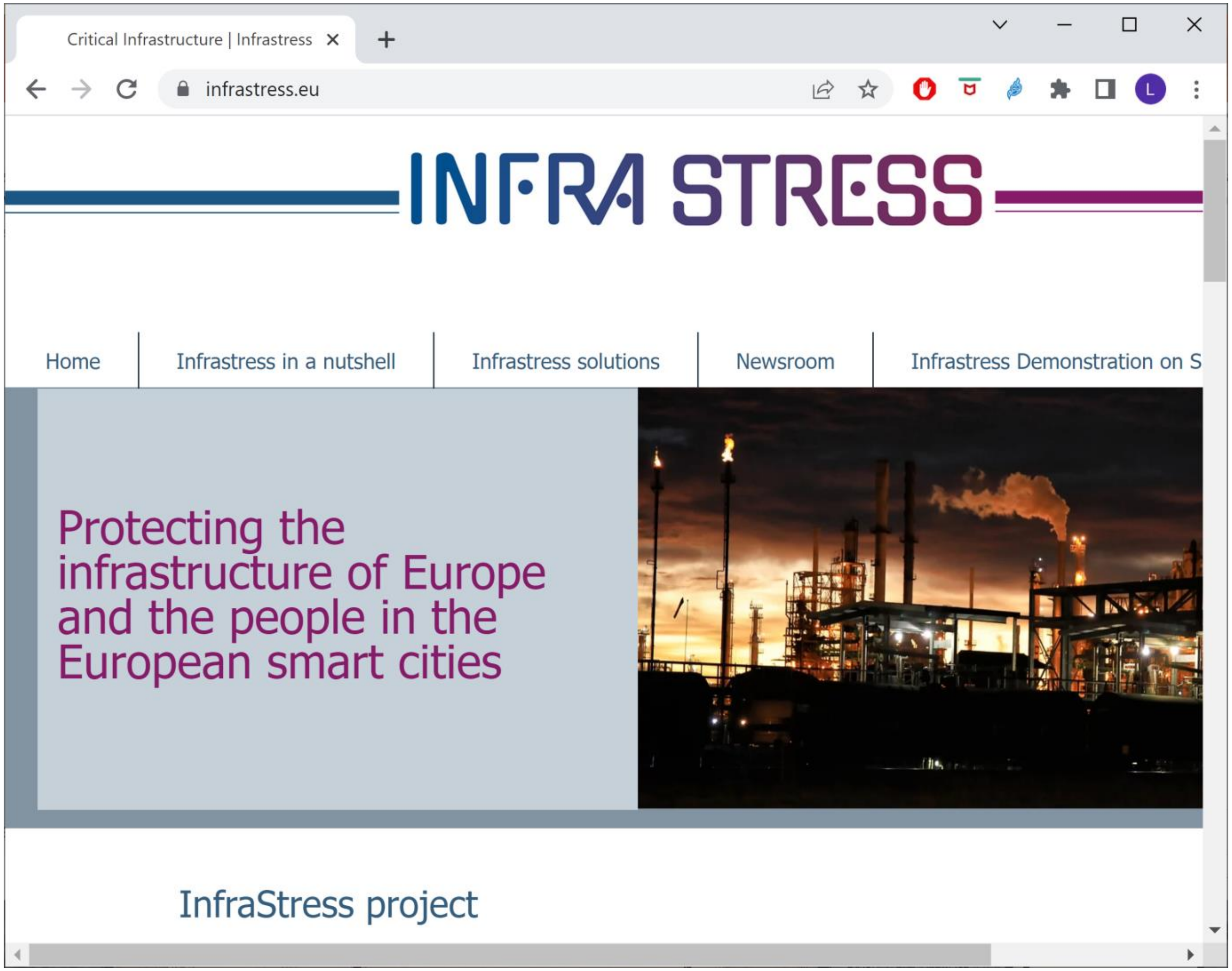


# Anomaly Detection in Energy Production

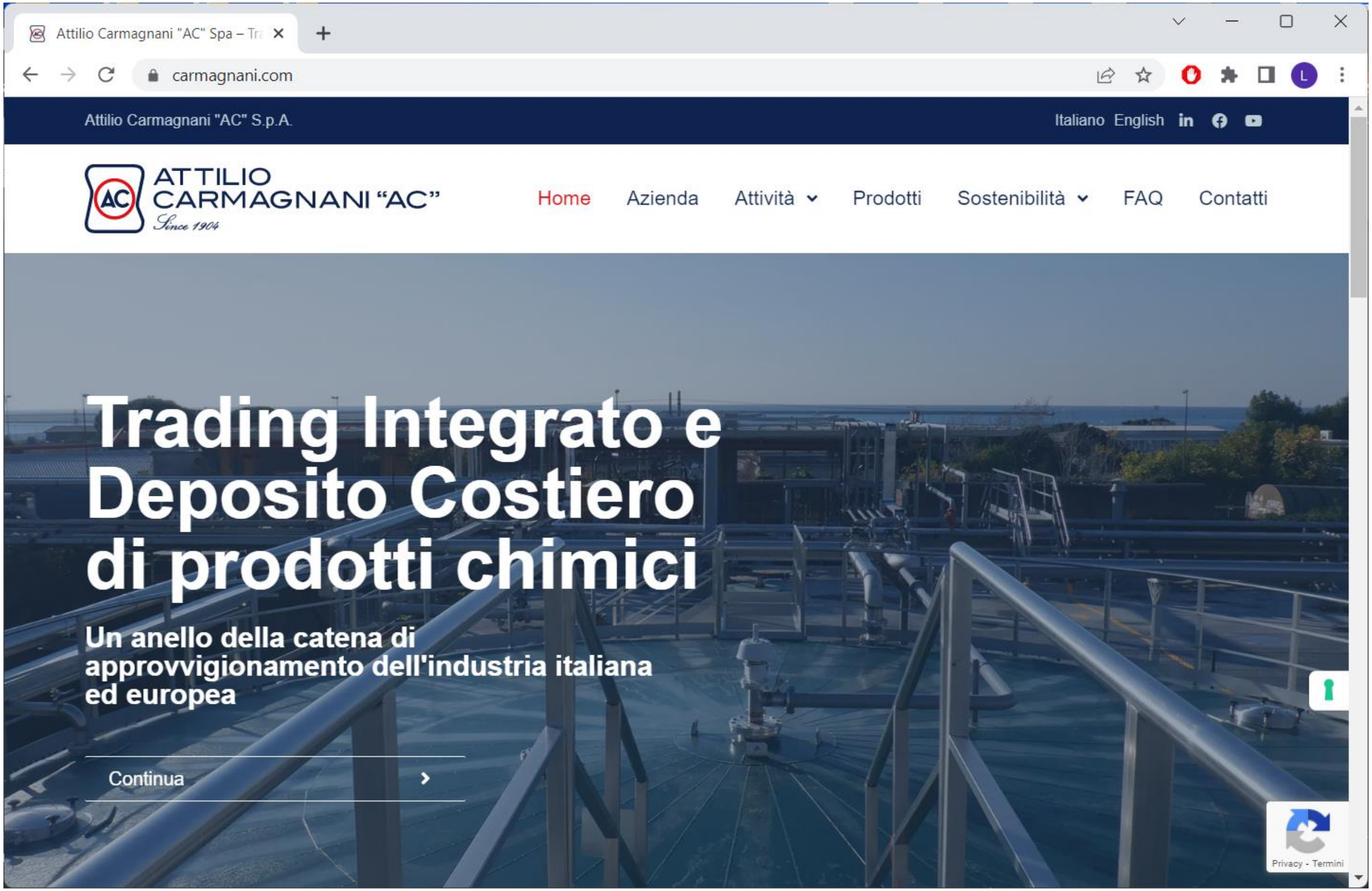


# Case study:
# Sensitive Industrial Plant

# The InfraStress project



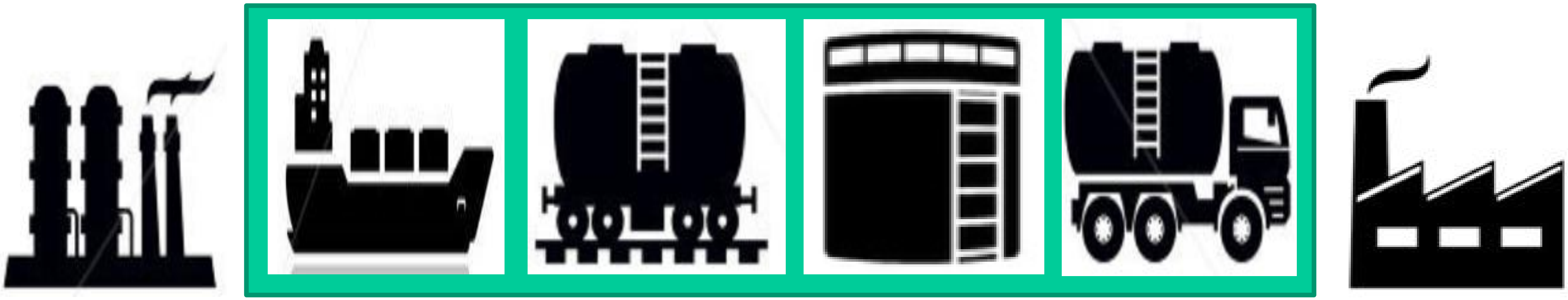
# ATTILIO CARMAGNANI



# THE COMPANY


ATTILIO CARMAGNANI - GENOVA
Stabilimento Raccordato - Genova - Cornigliano
Sala N. 1. per preparazione spedizioni

# Chemicals supply chain



2018

46 vessels

73 trains

139.795 Tons

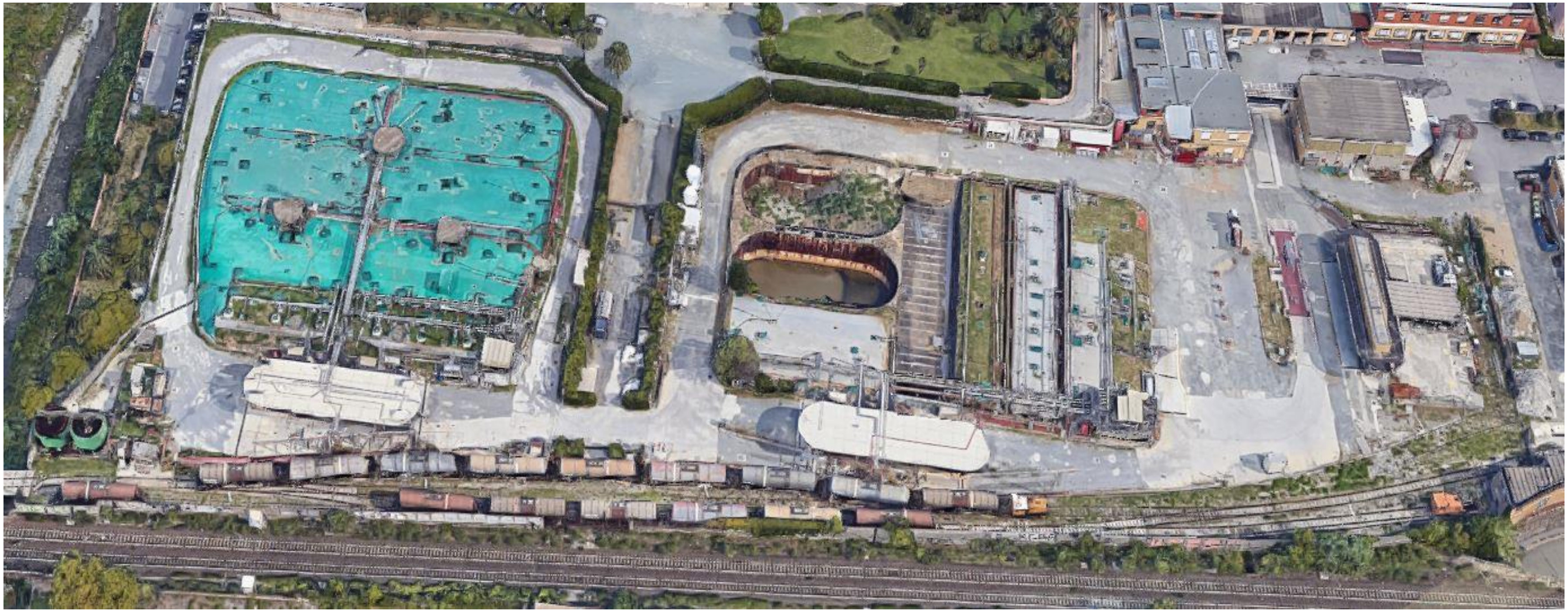
3.303 trucks

# The terminal

30.000 square meters
31 semi-buried or underground tanks
total capacity 27.504 cubic meters

5 tanks * 3000 mc
4 tanks * 1000 mc
6 tanks * 700 mc
2 tanks * 400 mc
6 tanks * 300 mc
8 tanks * 120 mc

# *The terminal*

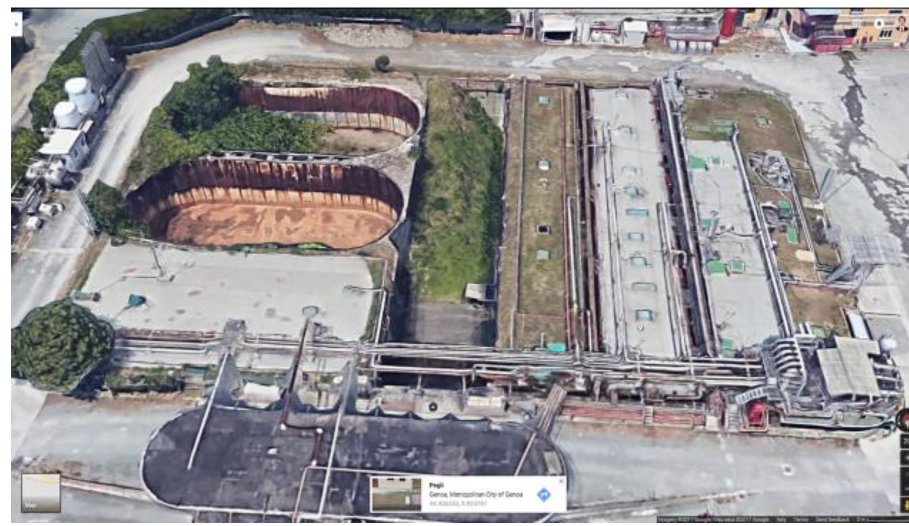


# *Critical activities*

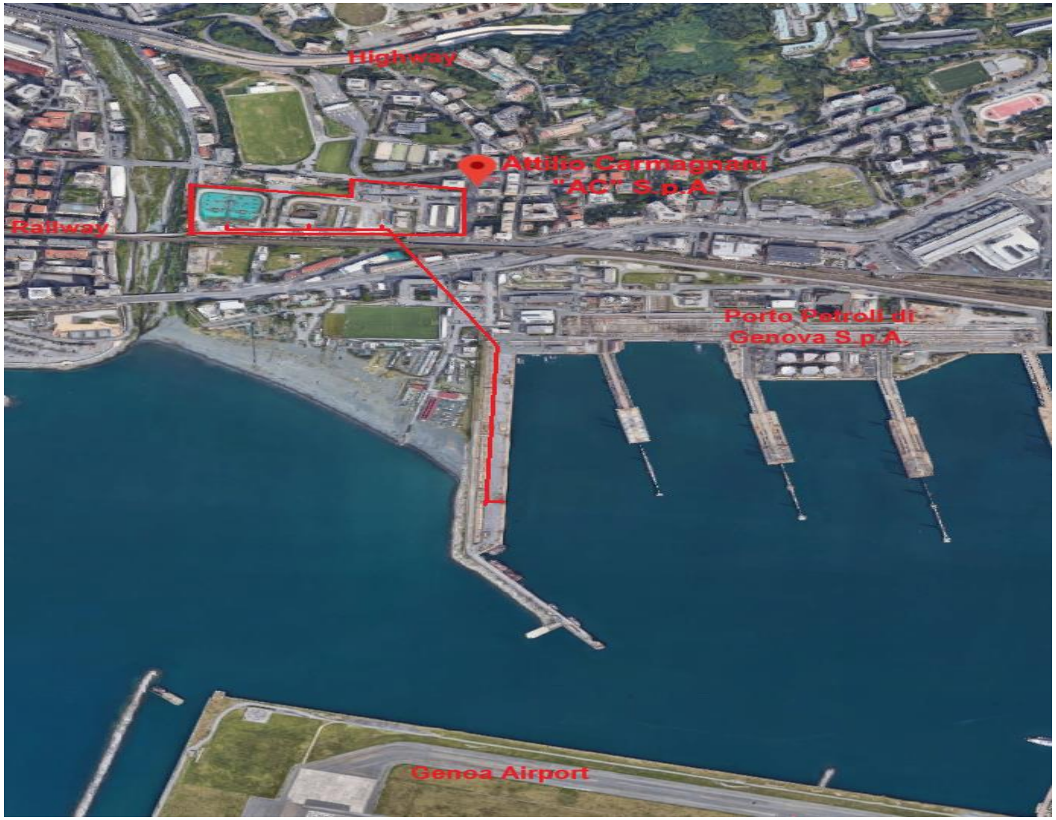

# *Threats and vulnerabilities*

| Substance | Hazard classes |
|---|---|
| Carmasol 100 (Solvent naphta C9) | E2/P5c |
| Carmasol 150/ Carmasol 150ULN (Solvent naphta C10) | E2 |
| Xylene/Orthoxylene | P5c |
| Pseudocumene | E2/P5c |
| Cyclohexanone | P5c |
| Vinyl acetate(VAM) | P5c |

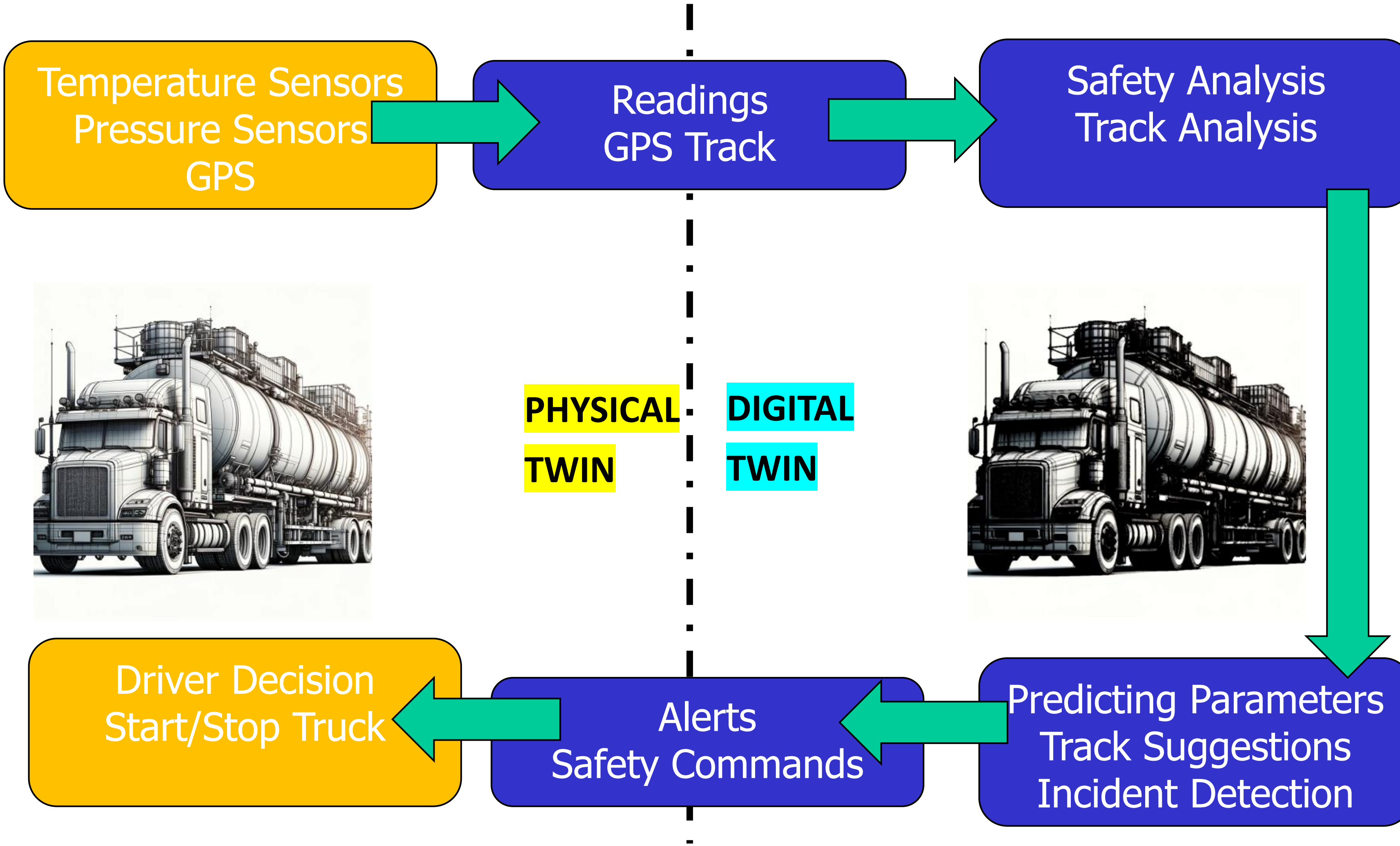
15 May 1987 8:30



# The surrounding environment

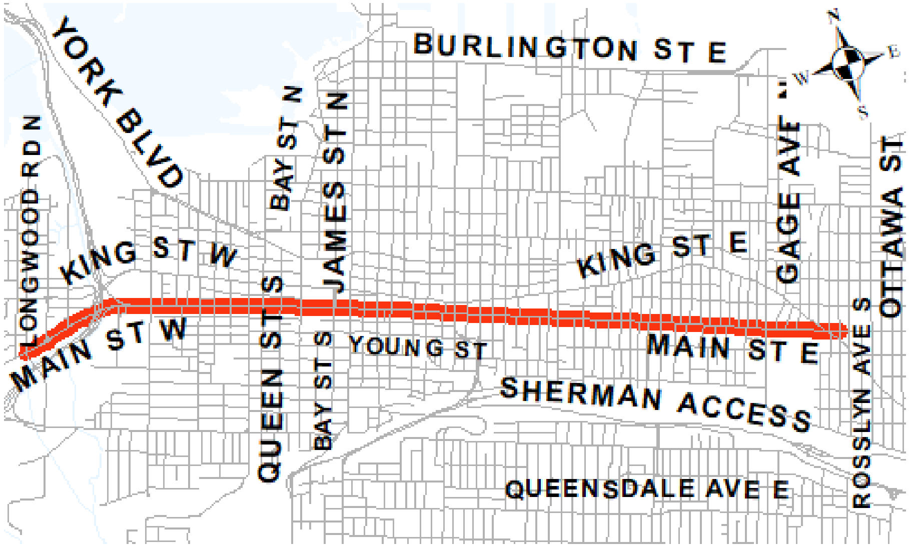



# The OODA Loop in the Chemical Supply Chain Monitoring

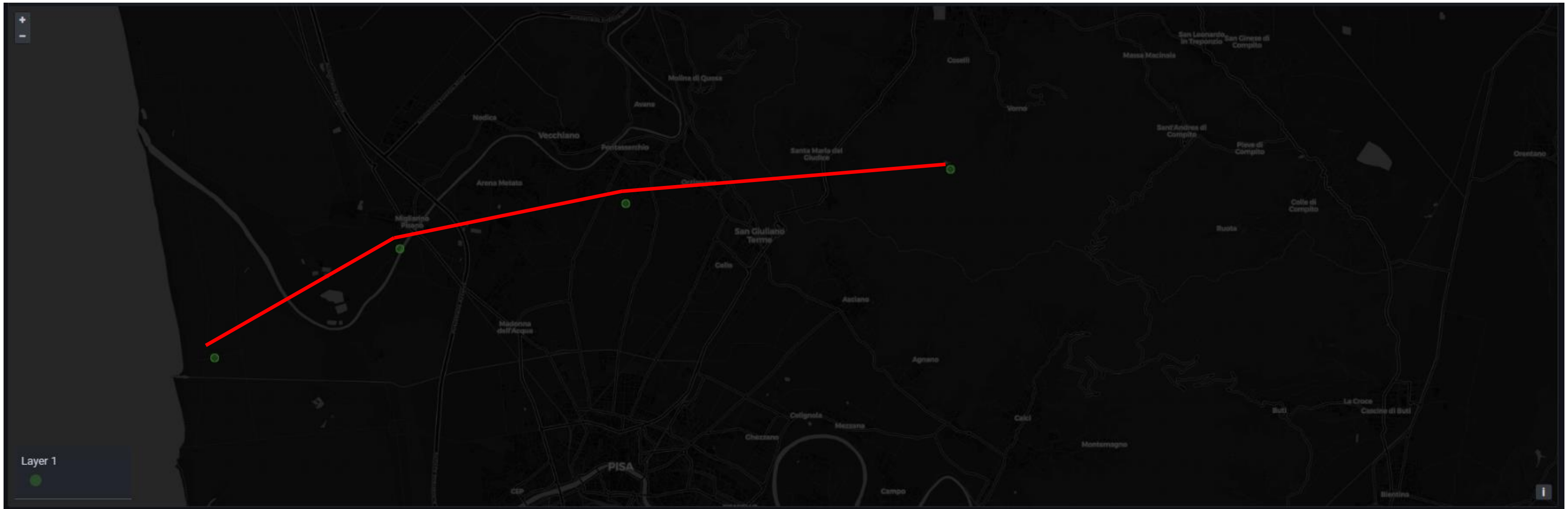


# Attack Scenario

- Threat agents start by conducting thorough surveillance of the target company
- A malicious user targets employees of the trucking company with spearphishing attacks
- With successful phishing, the attackers gain access to the trucking company's fleet management system
- The threat agent manipulates the route information within the fleet management system, redirecting the truck to an unauthorized location



# Route Hijacking Detection



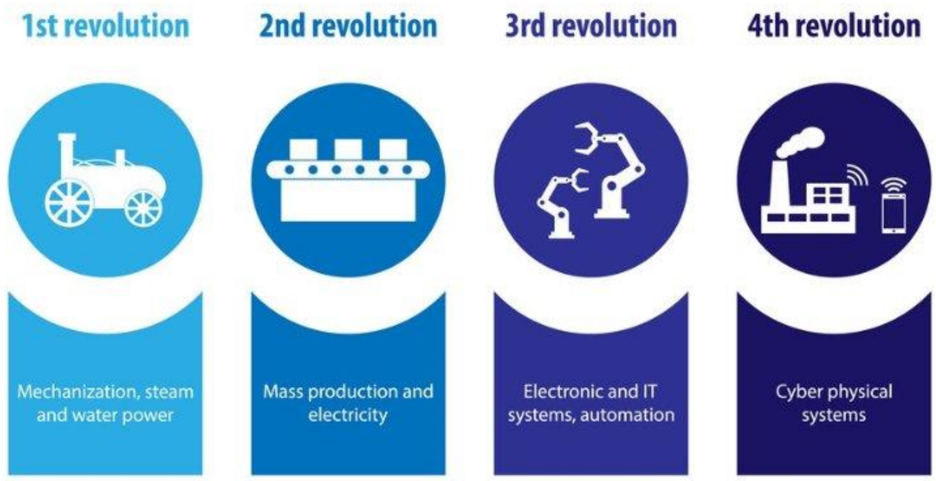

Truck A

| timestamp | latitude | longitude | temperature_C | pressure_bar | speed_kmh |
|---|---|---|---|---|---|
| 2023-12-10 09:00:00 | 43.8 | 10.5 | 20 | 1 | 50 |
| 2023-12-10 09:01:00 | 43.8 | 10.5 | 20 | 1.10 | 52 |
| 2023-12-10 09:02:00 | 43.8 | 10.5 | 21 | 1.10 | 53 |
| 2023-12-10 09:03:00 | 43.8 | 10.5 | 21 | 1.10 | 54 |
| 2023-12-10 09:04:00 | 43.8 | 10.5 | 22 | 1.10 | 55 |
| 2023-12-10 09:05:00 | 43.8 | 10.5 | 22 | 1.20 | 56 |

# Case study:
# Flexible Manufacturing System

# *Smart Manufacturing and Flexible Manufacturing Systems (FMS)*

- Manufacturing as we knew it is a memory from the past that will never come back
- The current (and the future) scenario is a global competition arena
- Companies must react quickly and in an economically feasible fashion to market requirements that change continuously and at an amazingly fast pace




https://www.iotcentral.io/blog/the-evolution-of-industry-4-0

# *Problem Statement*

- While volumes have increased, **margins have dropped**

  **The Airbus example:**

  Airbus has an average 100 billion euros throughput in cash flow going out of their factories

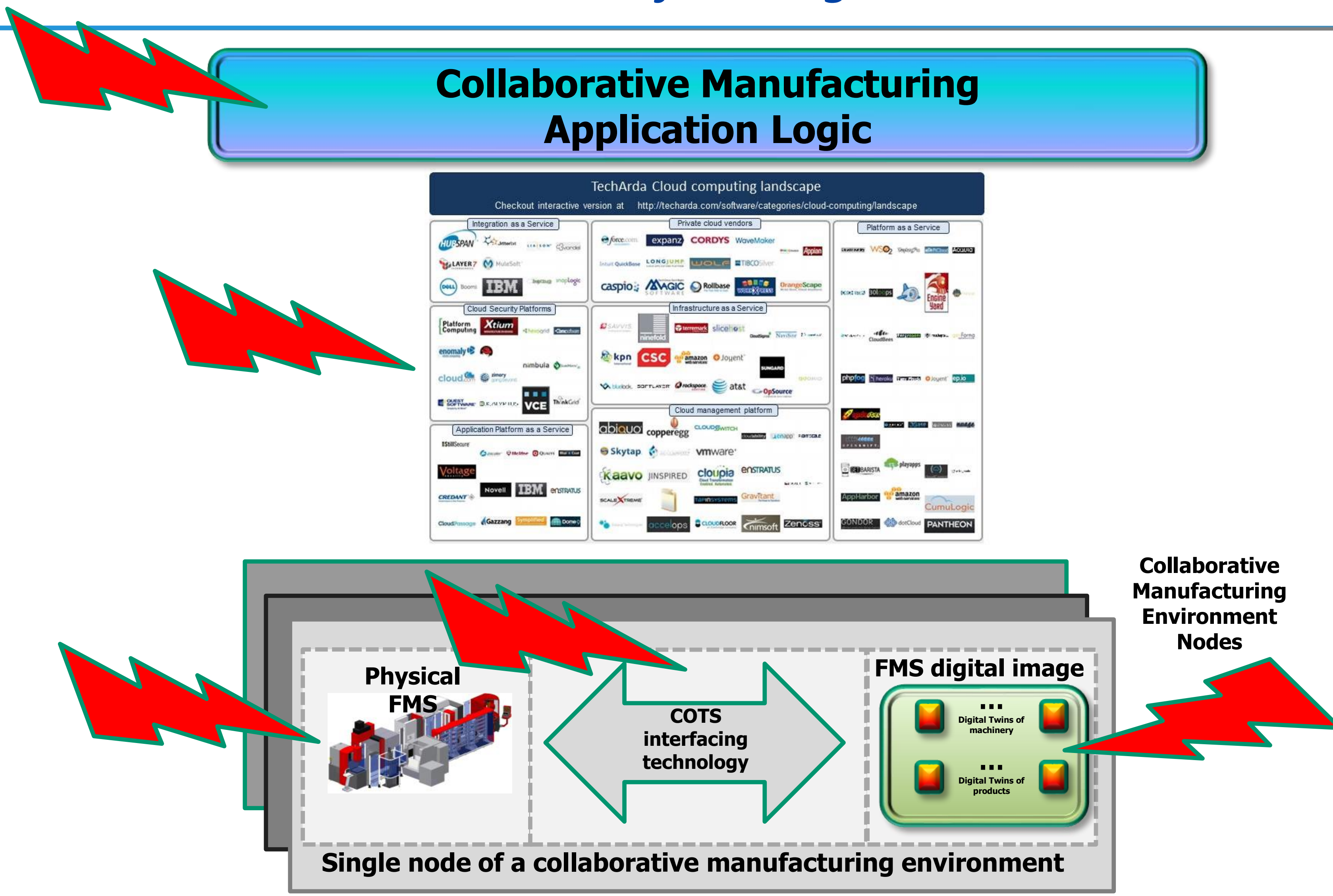
  **Their net profit margin is 6.27% (source: https://www.macrotrends.net/stocks/charts/EADSY/airbus-group/profit-margins)**

→ It is key that production plants be managed efficiently:

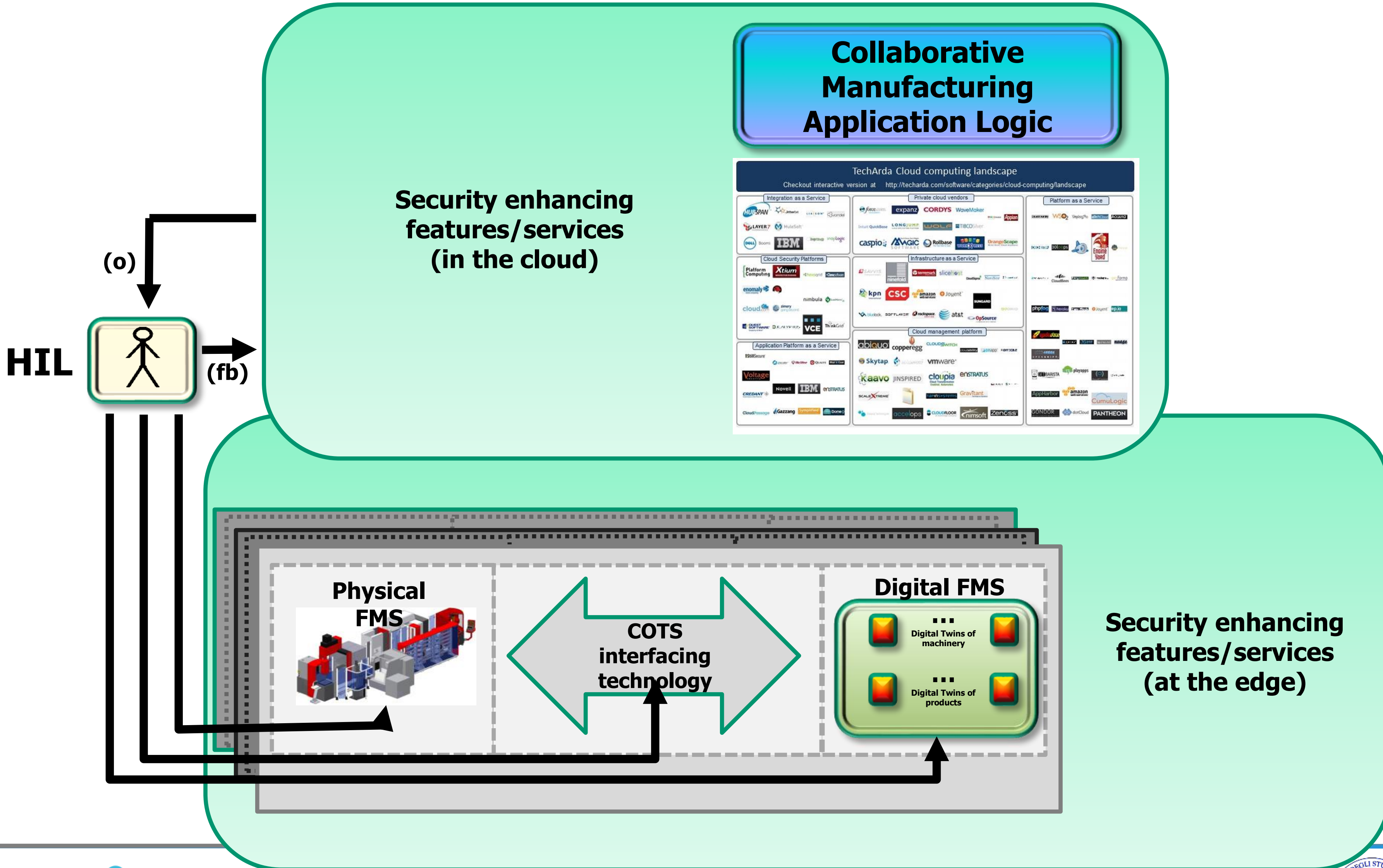
- Quickly apply changes in product design
- Handle increasingly smaller lot sizes
- Ensure that distribution meets challenging reliability and timeliness requirements

**Obviously enough, this is not possible if the ICT infrastructure on which the operation of the FMS relies upon is not able to survive** (faults and) **attacks**

# Conceptual architecture (and attack surface) of a Collaborative Manufacturing Environment

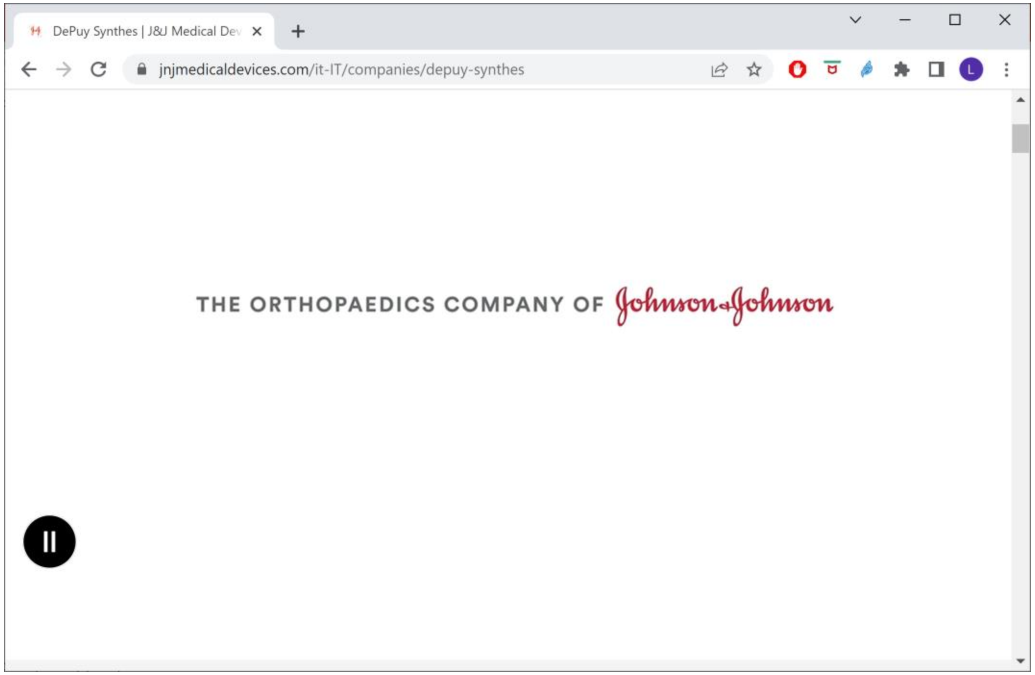


# *Securing a Collaborative Manufacturing Environment*



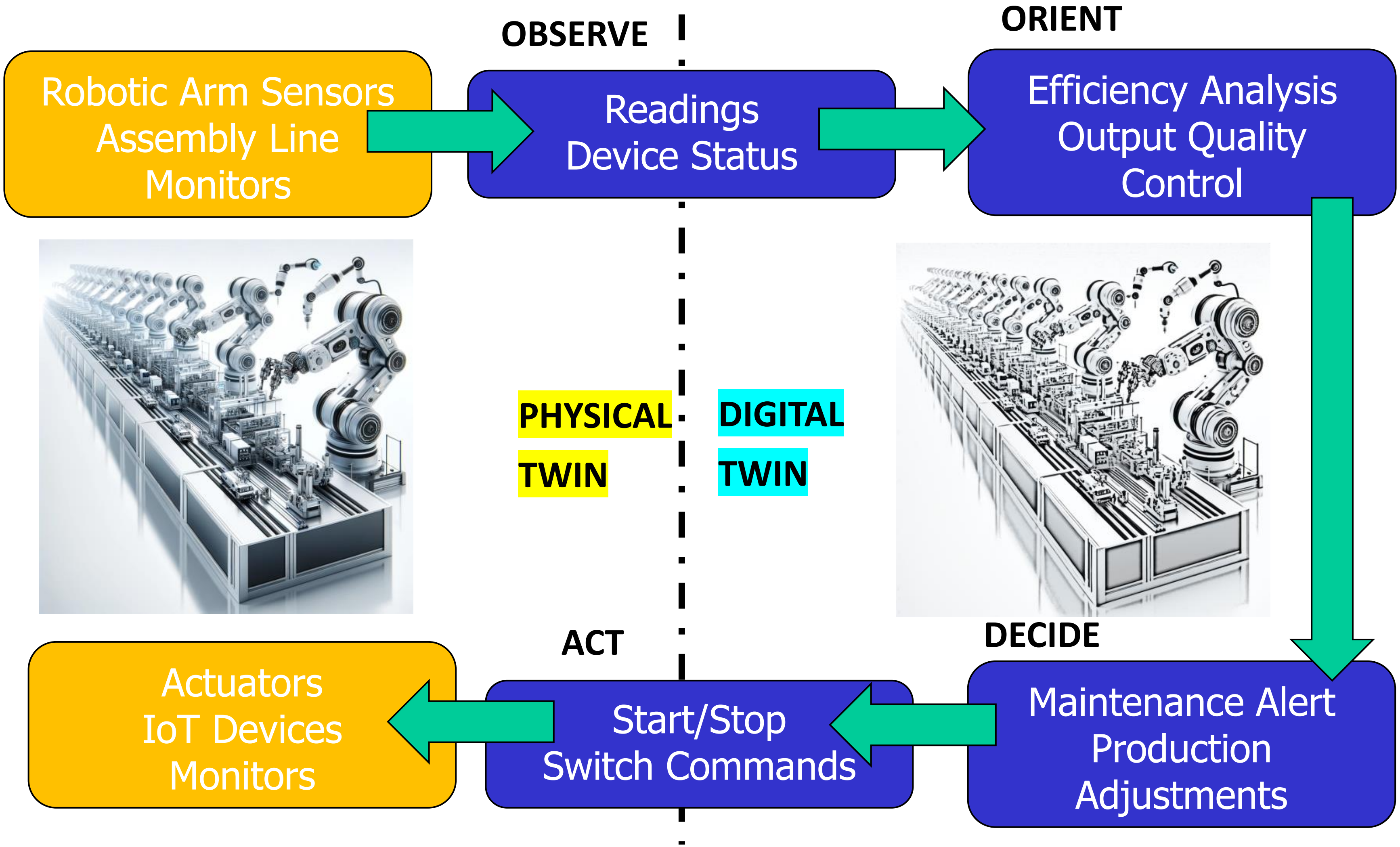
# *A major challenge (and opportunity): re-using legacy systems*

- In Septemer 2018 DePuy was recognized as one of the nine Industry 4.0 Lighthouse projects/companies




- A major motivation behind this decision was that **they use legacy technology to build Digital Twins**

# The OODA Loop in Flexible Manufacturing Systems



# *Attack Scenario*

- Threat agents begin their operation with extensive reconnaissance of the target manufacturing firm
- A malicious user targets employees of the firm with spearphishing attacks
- Threat actors gain unauthorized access to the Manufacturing Execution System (MES)
- Once inside the system, agents introduce subtle alterations to the manufacturing process parameters
- These could include changes to robotic arm movements, temperature settings, or equipment calibration data, with the intention of sabotaging production quality or safety

# 3D Printers Sabotage

# Hands-on Preview

# *What you will do*

- **You will learn the fundamentals of FIWARE**: Gain an understanding of FIWARE architecture, components, and applications
- **You will build a digital twin using FIWARE**: Engage in a step-by-step process to create a functional digital twin, utilizing the FIWARE platform
- **You will develop a security testbed for monitoring**: Implement security measures and monitoring protocols within your digital twin setup
- **You will engage in interactive learning and problem-solving**: Collaborate, discuss, and solve challenges during the practical session, thus enhancing your understanding and skills

# Prepare Your Environment

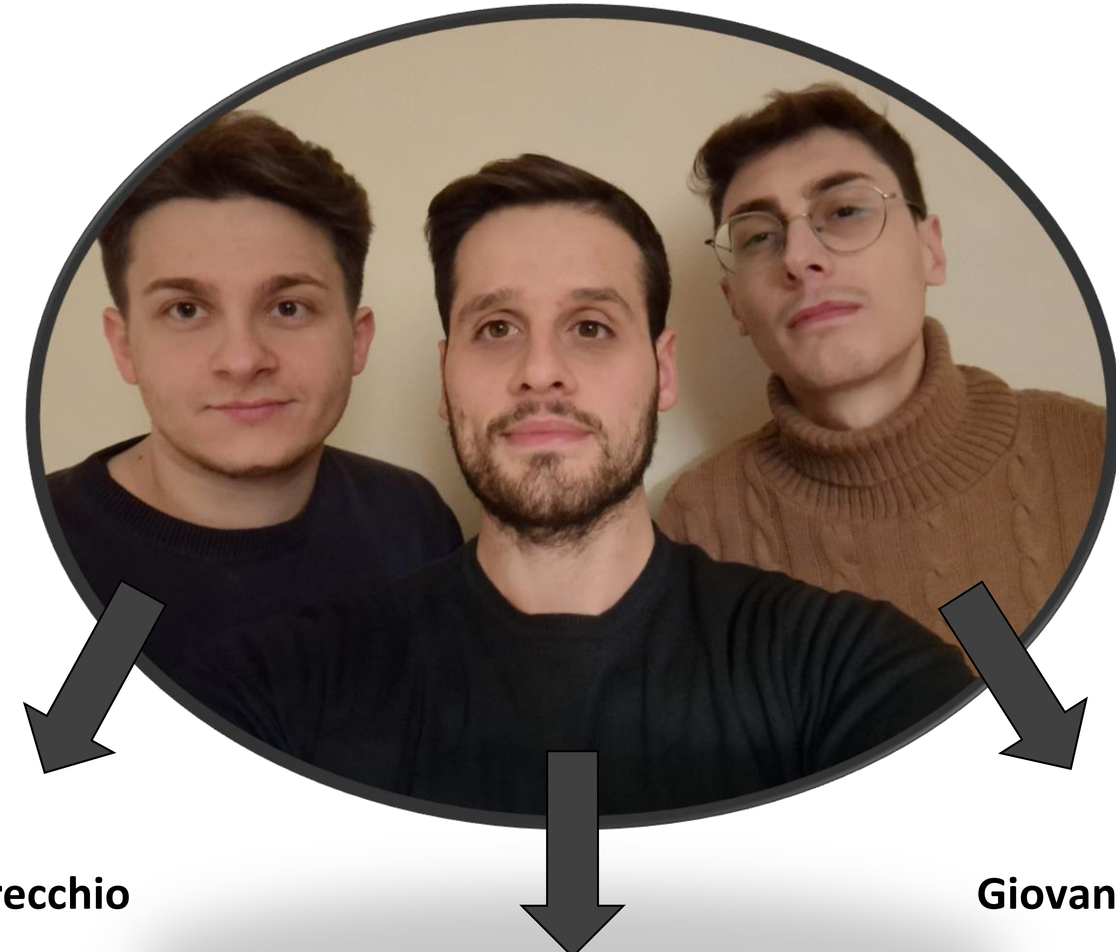
- To prepare for a productive session, before Friday:
  1. scan the QR code and download the GitHub repository provided below:

  2. Go to the Project Folder and Run:

  docker compose build OR docker-compose build

  <u>It may take a while!</u>

# *Do You Need Assistance?*



**Alessandro De Crecchio**

**Alfredo Petruolo**

**Giovanni Maria Cristiano**

# Acknowledgements and contacts

# FP7 projects – 1/2

http://www.intersection-project.eu/

http://www.inspire-strep.eu

http://www.inspire-inco.eu/

http://www.streamproject.eu/

https://srt-15.unine.ch/home.html

# FP7 projects – 2/2

http://www.massif-project.eu

http://www.sawsoc.eu/

http://leanbigdata.eu/

# *H2020 projects – 1/2*

http://www.konfido.eu

https://www.compact-project.eu

https://www.serecaproject.eu/

https://www.securecloudproject.eu/

# H2020 projects – 2/2

https://www.infrastress.eu/ INFRA STRESS

# Horizon Europe projects

https://encrypt-project.eu/

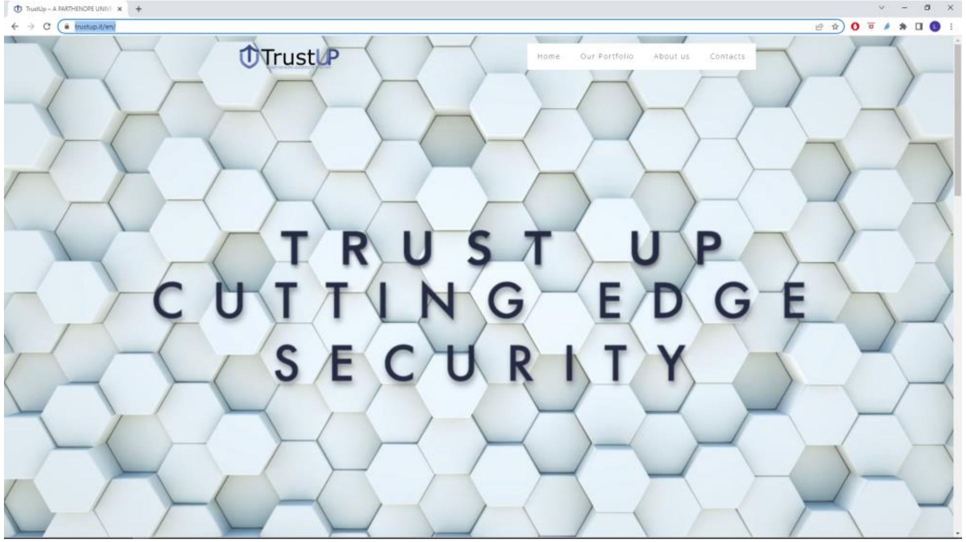
https://certify-project.eu/

# Contact Info


**Luigi Romano**

**e-mail:**
**luigi.romano@uniparthenope.it**
**Cell: +39-333-3016817**
**Tel: +39-081-5476700**


The **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S** (FITNESS) research group
**fitnesslab.eu**




*https://www.trustup.it/en/*

# References and More Details

# Sources and pointers – Data Spaces

1. https://digital-strategy.ec.europa.eu/en/policies/strategy-data
2. EUR-Lex - 52020DC0066 - EN - EUR-Lex (europa.eu)
3. https://dataspaces.info/common-european-data-spaces/#page-content
4. https://datasovereigntynow.org/frequently-asked-questions/
5. https://internationaldataspaces.org/
6. https://gaia-x.eu/
7. https://catena-x.net/en/
8. https://www.fiware.org/
9. https://www.fiware.org/smart-data-models/
10. Data Spaces Book

# *Sources and pointers – Digital Twin*

1. ECSO Technical paper (ecs-org.eu)
2. bim-digitwin-ru.pdf (siemens.com)
3. SimulationAndDigitalTwin (siemens.com)
4. What is a digital twin? | IBM
5. https://www.fiware.org/wp-content/uploads/FF_PositionPaper_FIWARE4DigitalTwins.pdf
6. https://www.oodaloop.com/archive/2022/02/23/the-worlds-largest-digital-twin-modeling-and-simulation-project/
7. https://dataspaces.info/intelligent-systems-and-applications/#page-content
8. https://www.computer.org/publications/tech-news/trends/digital-twin-use-cases
9. https://www.digitaltwinconsortium.org/
10. How Digital Twins Could Protect Manufacturers From Cyberattacks | NIST