Industrial IoT security: approaches and challenges

M. Repetto

CNR - Institute for Applied Mathematics and Information Technologies
“E. Magenes” (IMATI)

Outline

- Cyber-Physical Systems
  - evolving paradigms and security challenges
- Digital Twins
  - modelling physical systems and cyber-security processes
- Service chains
  - from digital to hybrid interconnectedness of multiple business and technological domains
- Key take-aways
  - research and methodological hints

Cyber-Physical Systems (CPS)

- *"the next generation embedded ICT systems that are interconnected and collaborating providing citizens and businesses with a wide range of innovative applications and services"*

  •EC Horizon 2020

- *"the evolution of embedded systems into smart objects that will be joined together to create highly distributed systems, bringing a wealth of opportunities and innovations in technology, applications and business models"*

  •ISTAG

- *"embedded intelligent ICT systems that are interconnected, interdependent, collaborative, and autonomous. They provide computing and communication, monitoring/control of physical components/processes in various applications"*

  • ECSEL Joint Undertaking

Cyber-Physical Systems (CPS)

Physical surrounding

Internet of Things

+

Communication networks

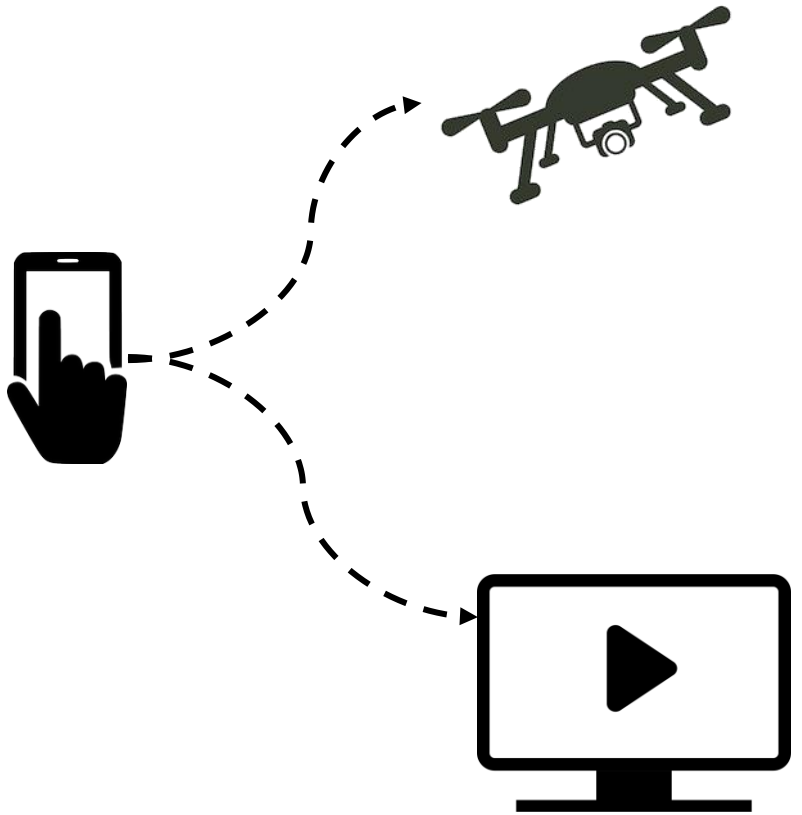
+

Internet of services

= *Smart services*

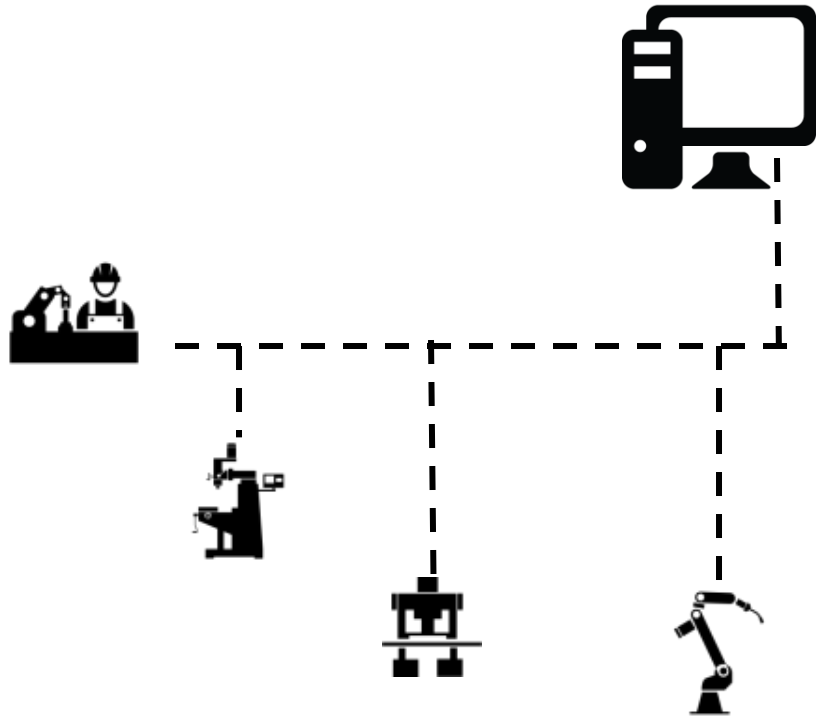
Evolving paradigms…

- **Remote control**
  - “hardwired” connection/discovery
  - closed world
  - single function or business process
- Application:
  - video control, device control
- Protocols:
  - UPnP, DLNA



Evolving paradigms…

- **Internet of Things**
  - Internet-enabled devices
  - closed world
  - sensors and actuators
- Application:
  - manufacturing, autonomous driving, SCADA systems
- Protocols:
  - M2M, MQTT, CoAP, SOAP

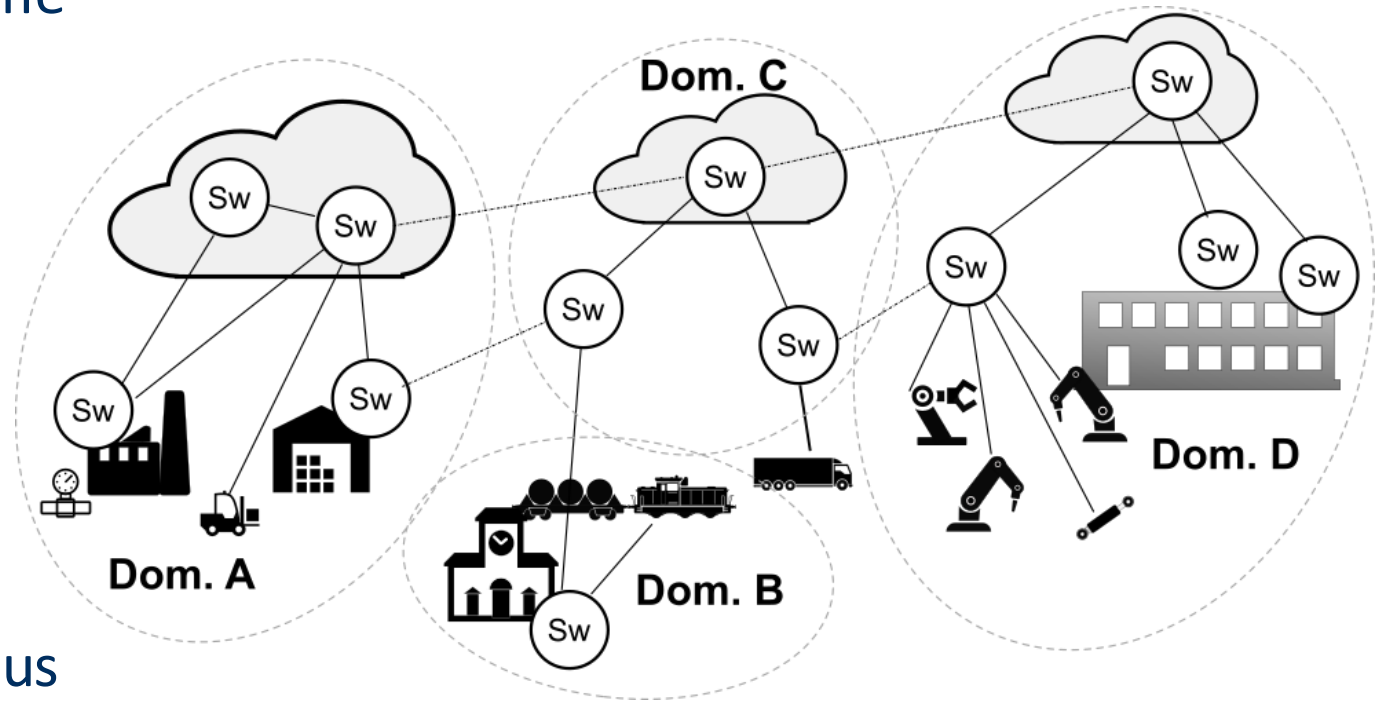


Evolving paradigms…

- Cloudlets: Small-scale IoT environments
  - devices in close physical or logical proximity to process data more efficiently
  - smart meter devices, controller units, storage units, and analytics applications for network management and monitoring
  - the master terminals are equipped with programmable logic controller (PLC) based automation units
  - Message Queuing Telemetry Transport (MQTT)
  - Gateway units provide private networks for each cloudlet and implement additional privacy properties

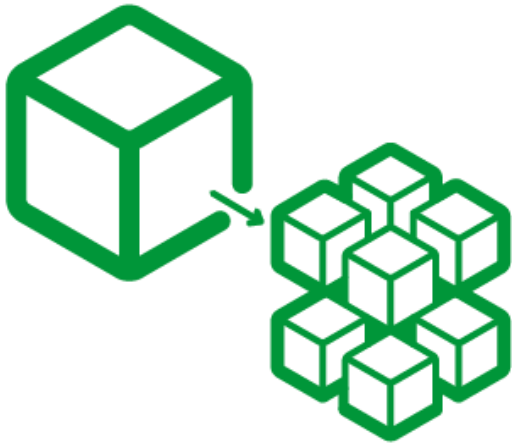
Evolving paradigms…

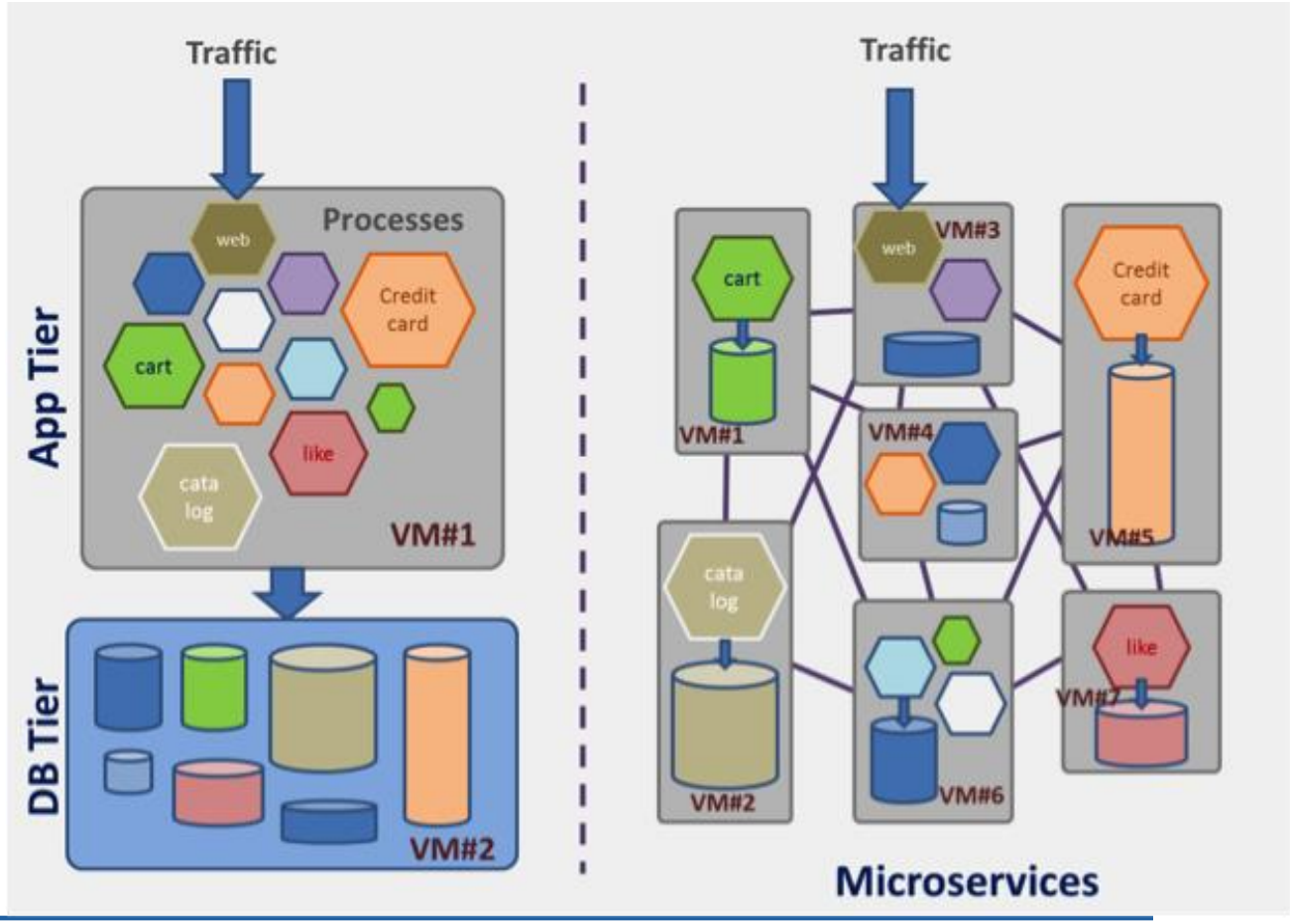
- **Cyber-Physical Systems**
  - dynamic composition and run-time evolution
  - “open” world
  - blurred system boundaries
  - uncertainty in the specifications
  - devices and software
  - business chains
- Application:
  - smart manufacturing, autonomous driving, smart cities, eHealth



Software paradigms for CPS

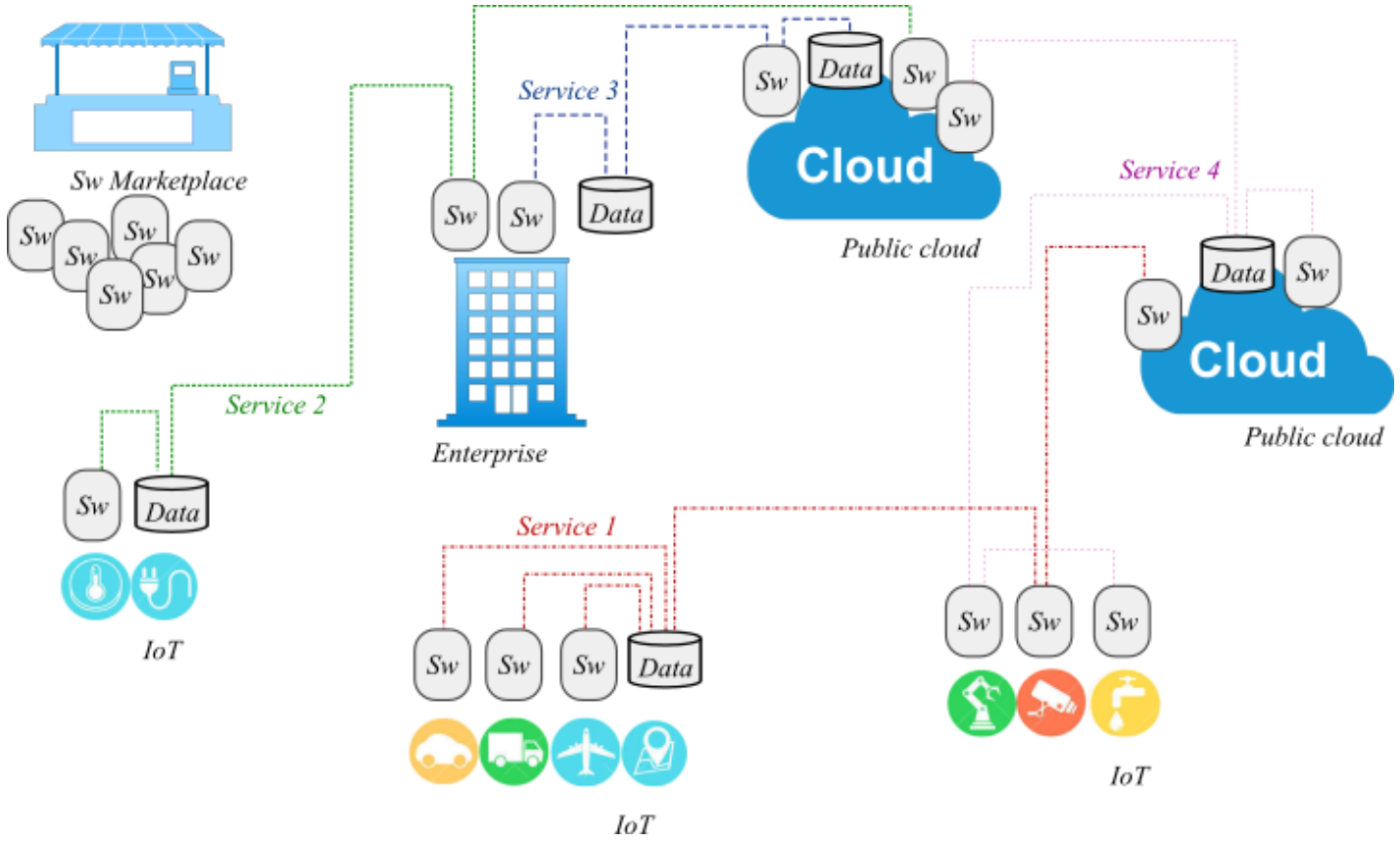
- From “code writing” to “service chaining and configuration”
- From monolithic applications to micro-services





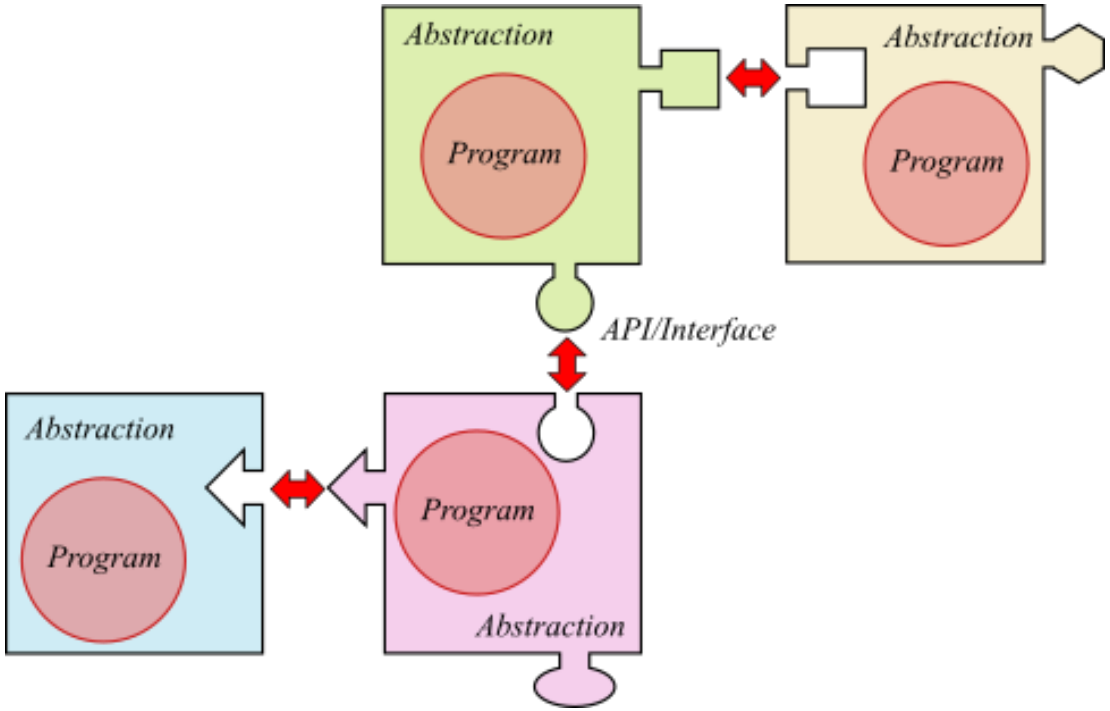
Software paradigms for CPS

- Composition of
  - pre-packaged software images
  - smart devices
- Elastic topologies
  - model-driven or data-driven
- Programmable infrastructure
  - cloud, SDN, IoT



Software paradigms for CPS

- Service model
  - description
  - capabilities (what the component does)
  - properties (configuration elements),
  - requirements (virtual resources, libraries, other components), and
  - management operations (e.g., install, start, stop, scale, monitor).
- Orchestration
  - deploy the service in the underlying virtualization infrastructure
  - perform life-cycle management actions.
- Examples: TOSCA, ETSI NFV, IETF SFC, FIWARE



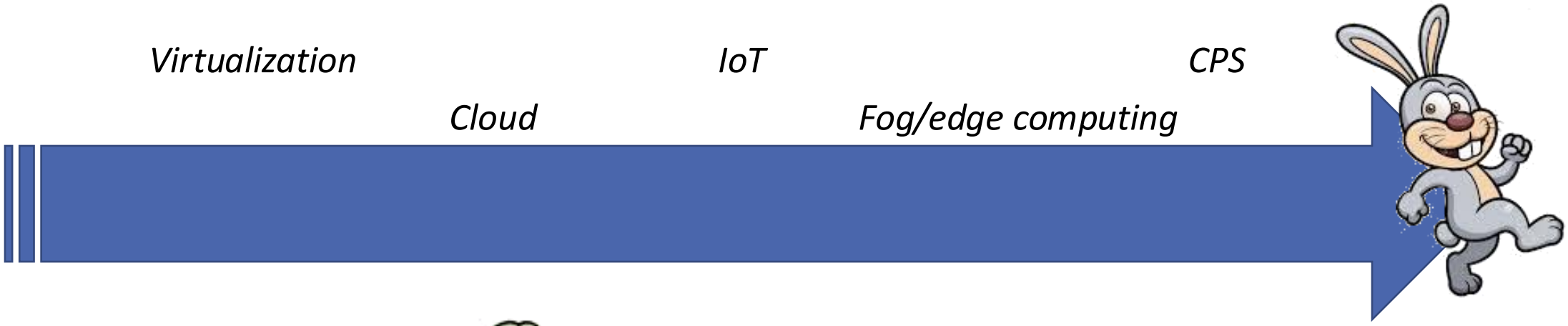
Challenges for CPS

- Heterogeneity:
  - “chaining” processes, software, and devices
  - feeding with relevant user’s data and context
- Agility:
  - digital services and business chains emerge and dissolve much faster than traditional value creating networks
- Autonomicity and dynamic composition
  - through service-oriented and everything-as-a-service models
- Multi-tenancy, multi-domain by nature

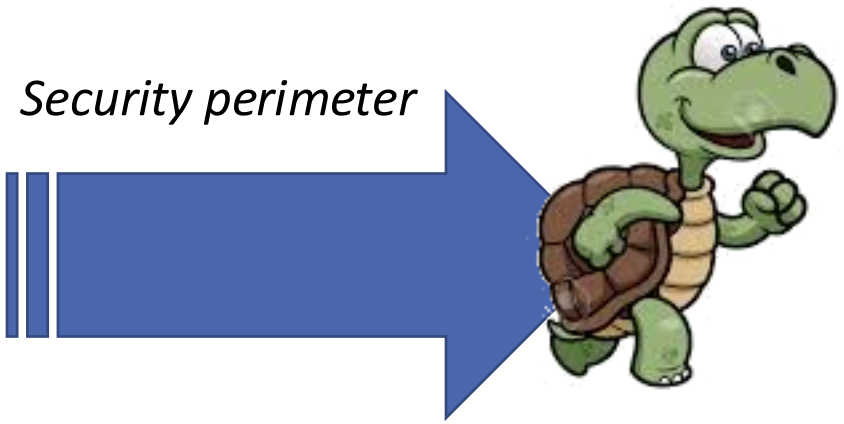
… and security?

Virtualization *IoT* *CPS*

Cloud *Fog/edge computing*



Security perimeter

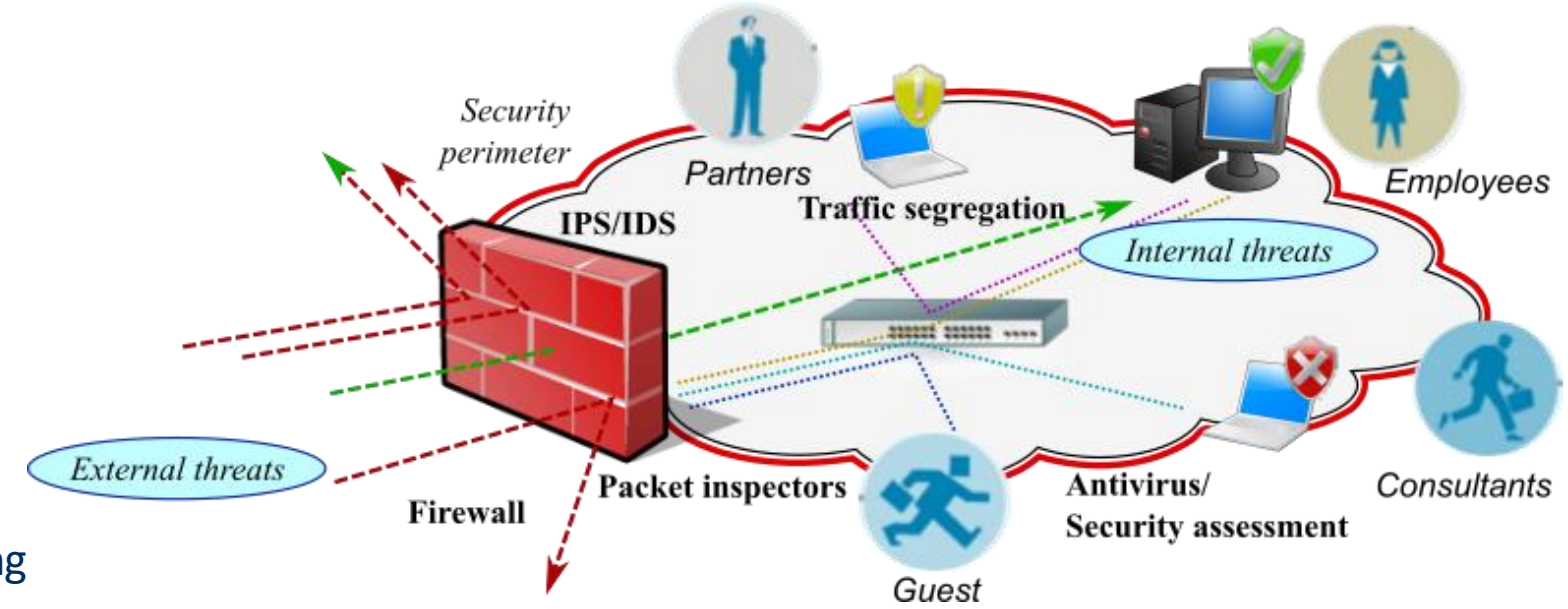


Well-known incidents

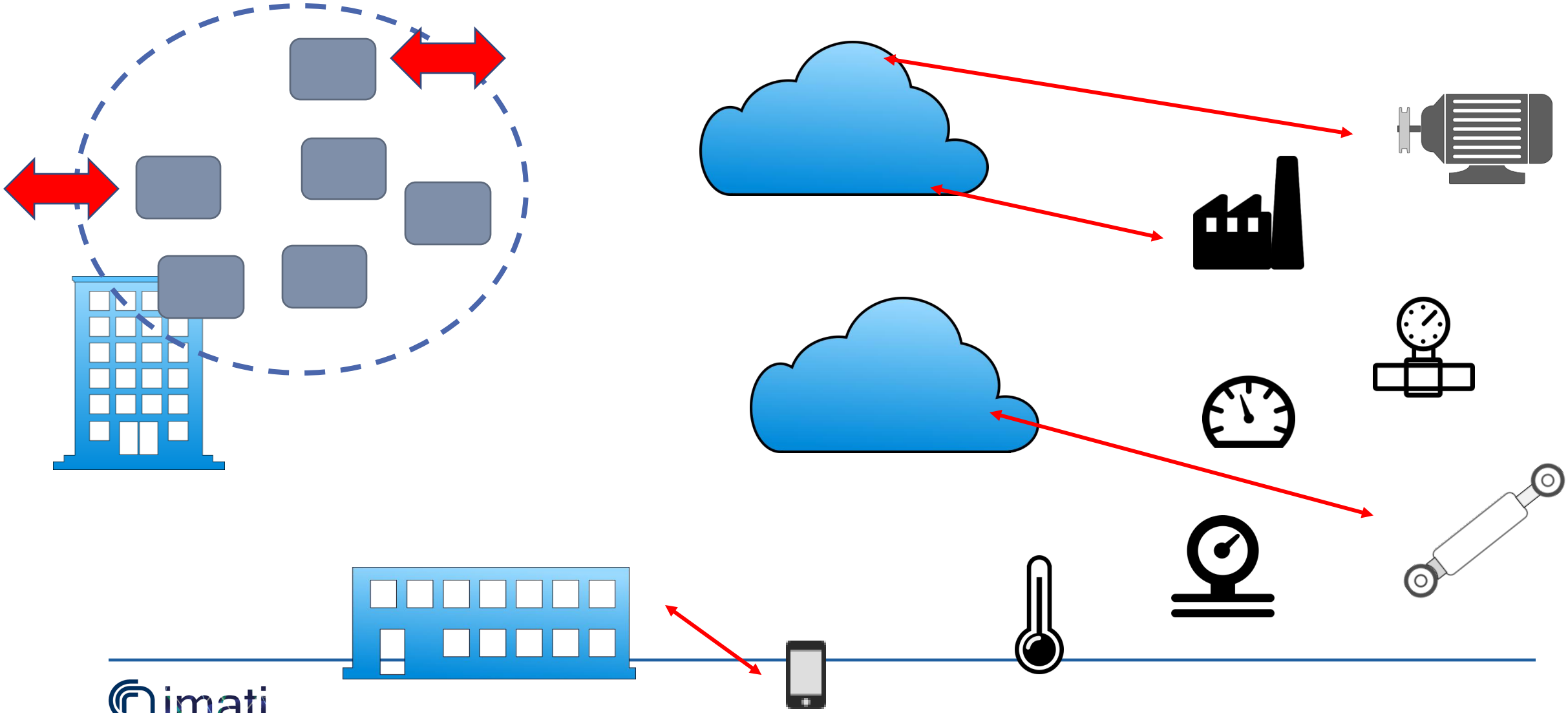
- North-eastern blackout, USA and Canada (2003)
  - 50 million people without electricity
  - Blaster worm spreading might have hindered the detection of inial small power outage
- Baku-Tbilisi-Ceyhan oil pipeline explosion, Turkey (2008)
  - control system accessed via internet-connected security cameras to raise the pressure
- STUXNET worm (2010),
- TRITON malware
- Shamoon Saudi Aramco spear-phishing attack (2012)
  - malware attack floored 30,000 workstations
  - 10 days to restore normal businesses
- Metcalf sniper attack, California (2013)
  - physical attack to substation (communication cable cut, 17 transformers shooted)
- German steel factory attack (2014)
  - spear-phishing e-mail and social engineering
  - blast furnace not being able to be turned off in a regulated fashion caused massive damage to the system
- Ukrainian power grid attack (2015, 2016)
  - utility computers: large-scale blackout (~6 hours), 230,000 people (2015)
  - substation: false control signals to operate the network circuit breakers (2016)
- Saudi Arabia petrochemical plant (2017)
  - manipulate emergency shutdown system
- Venezuela blackouts (2019)
- US grid reconnaissance (suspected) (2019)
- Russian US malware (claimed) (2019)

The “security perimeter” model

- Shortcomings:
  - rigidity
    - network partitioning
    - hw/sw security appliances
    - routing/switching policies
  - market segmentation
    - network packets bounced across security appliances
      - for analysis, inspection, mitigation, and processing
    - redundant inspection/analysis
    - limited scope security service



The security perimeter model and CPS

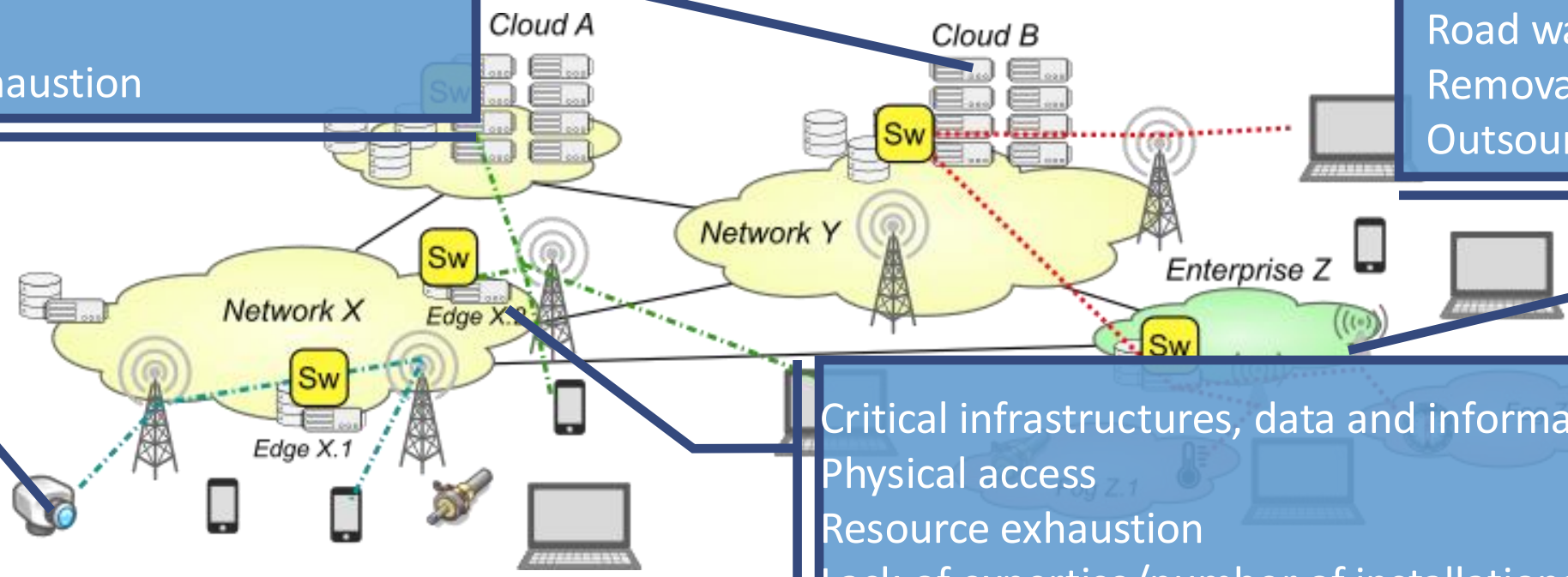


Security threats in CPS

Broader range of attack models
Increased attack surface
Multi-tenancy
Lack of hardware acceleration
Lack of trusted platform modules

Public Internet connection (LTE, WiFi)
Weak security mechanisms by design
Poor configuration
Tampering
Resource exhaustion

Personal and portable devices, multihoming
Road warriors
Removable storage
Outsourcing



Critical infrastructures, data and information leakage
Physical access
Resource exhaustion
Lack of expertise/number of installations
Dynamic service composition (NFV, MEC)
Intrusion and privilege escalation

imati

Attacks

False Data Injection Attack (FDIA):

- poisons power system state estimation by injecting false data into meter measurements,

Denial-of-Service (DoS) attack:

- consumes the resources of a remote host or network until the system stops responding or crashes

Man-in-the-Middle (MITM) attack:

- intercepts and manipulates messages (ARP/DNS spoofing)

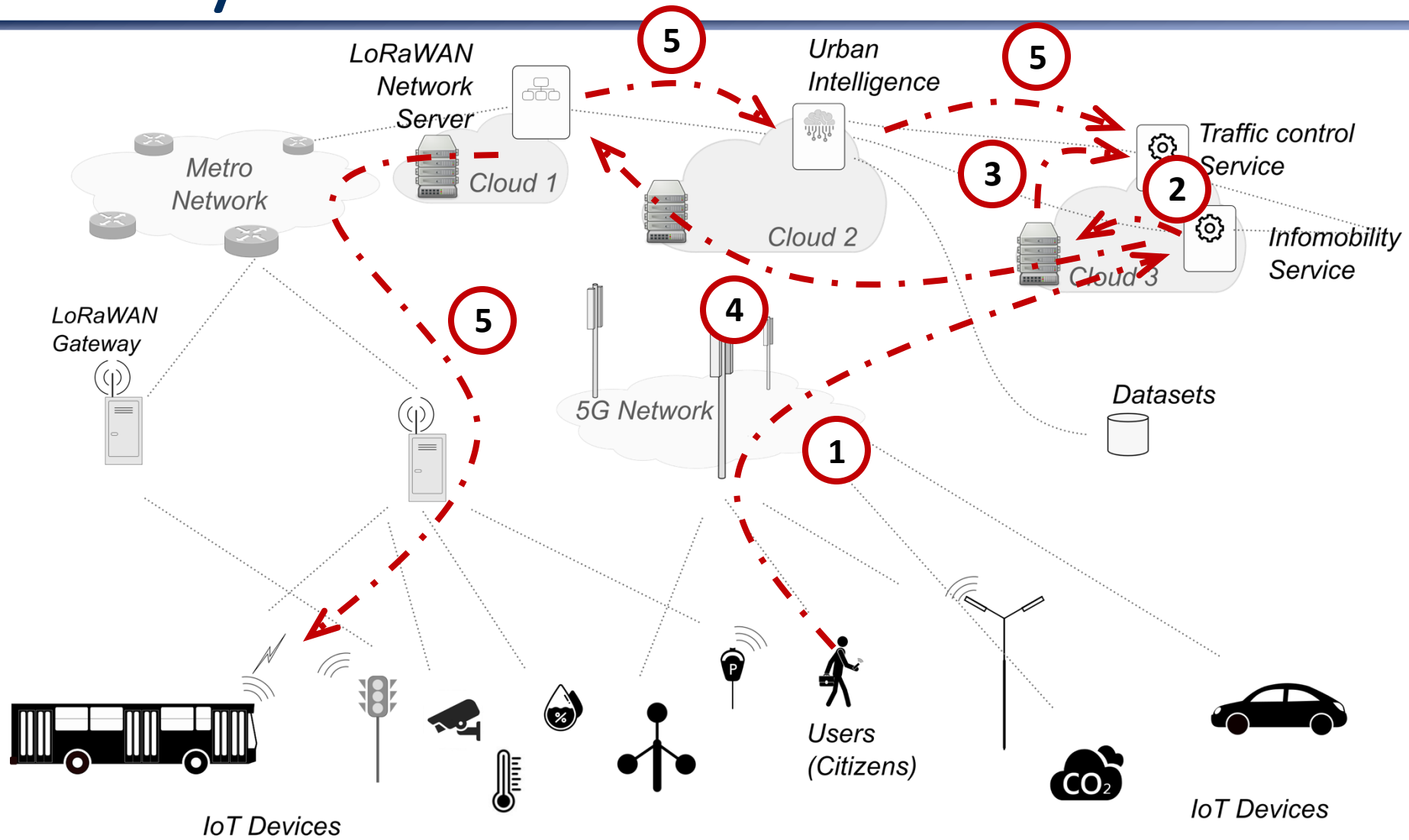
Replay attack:

- intercepting a system's usage pattern to mislead the receiver (destroys the
- correctness of authentication)

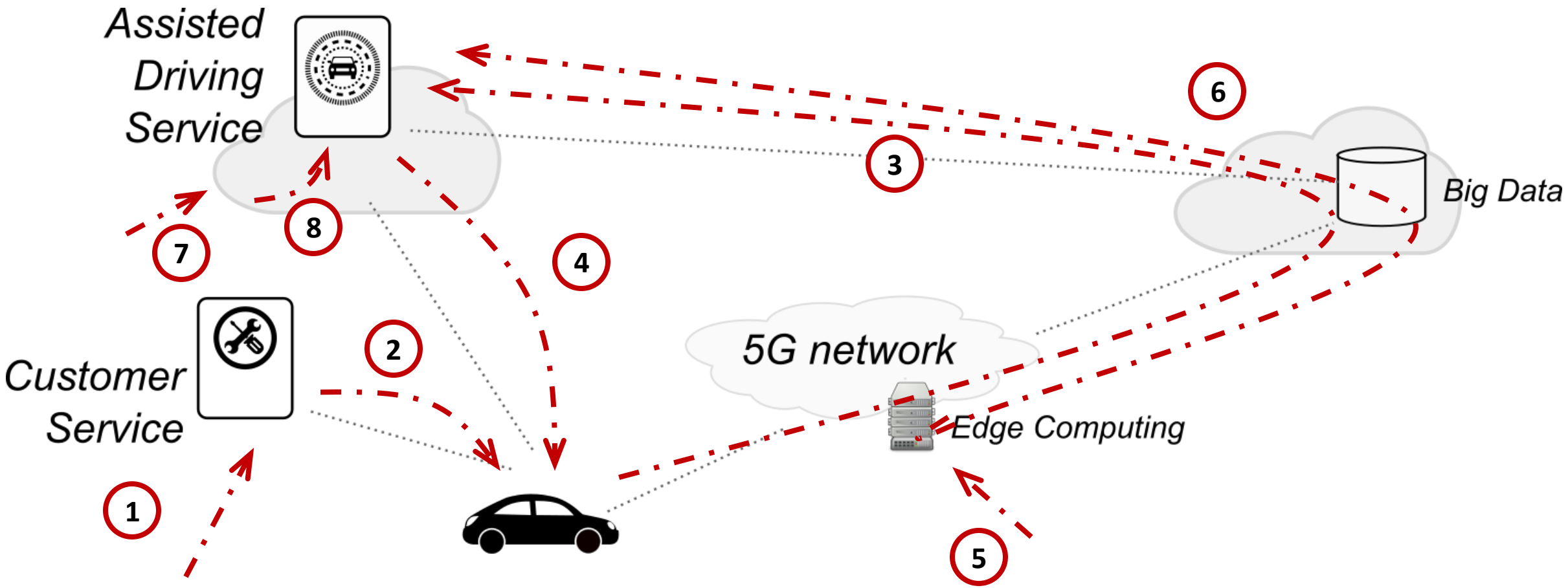
Other attacks:

- GPS Spoofing Attacks (GSA) targeting phasor measurement units
- Load-Altering Attacks (LAA) against demand response programs
- Delay Attacks that disrupt communication channels

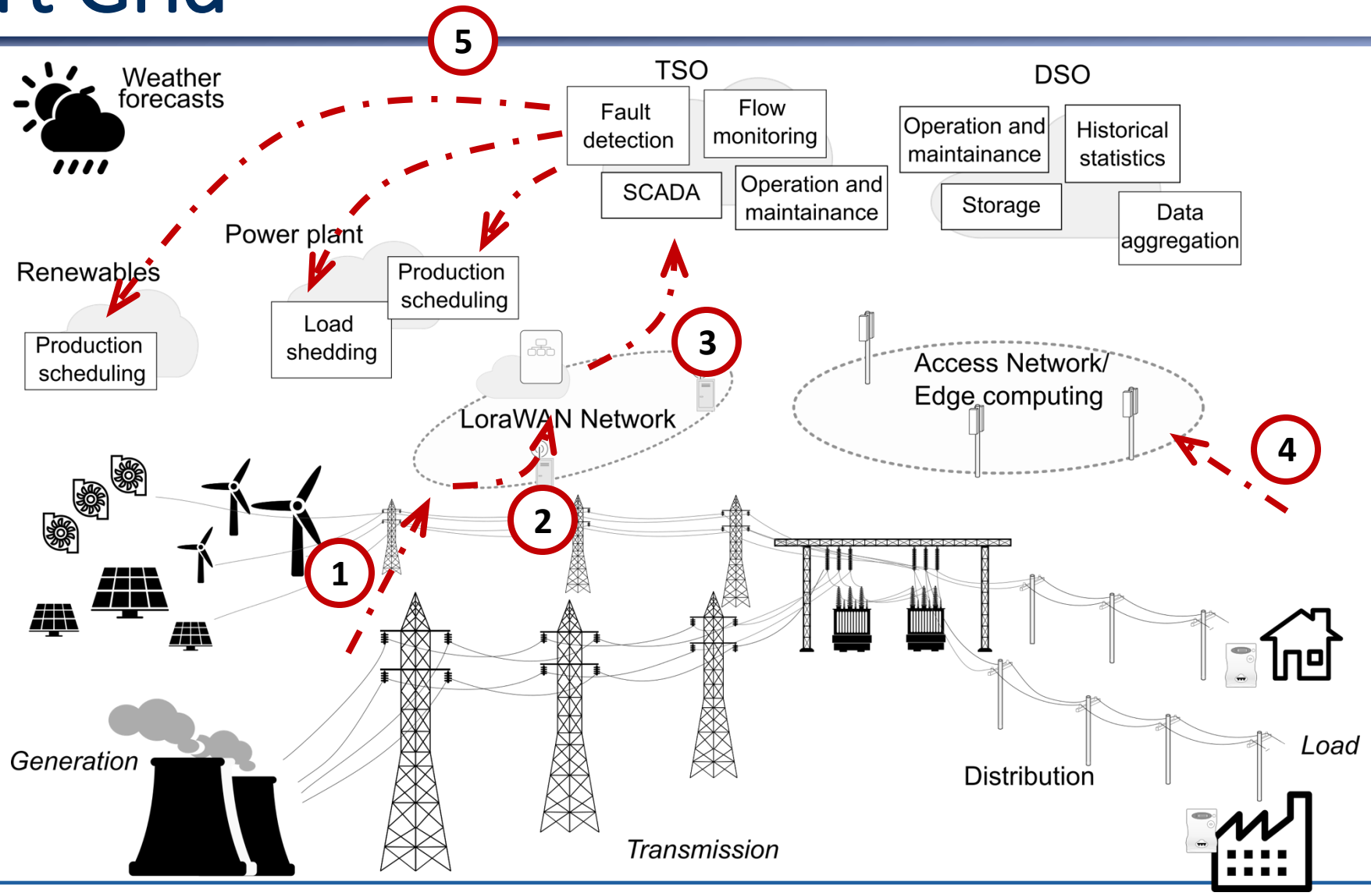
Smart City


LoRaWAN
Network
Server
Cloud 1
Metro
Network
Urban
Intelligence
Cloud 2
Traffic control
Service
Infomobility
Service
Cloud 3
LoRaWAN
Gateway
5G Network
Datasets
Users
(Citizens)
IoT Devices
IoT Devices
1
2
3
4
5
5
5

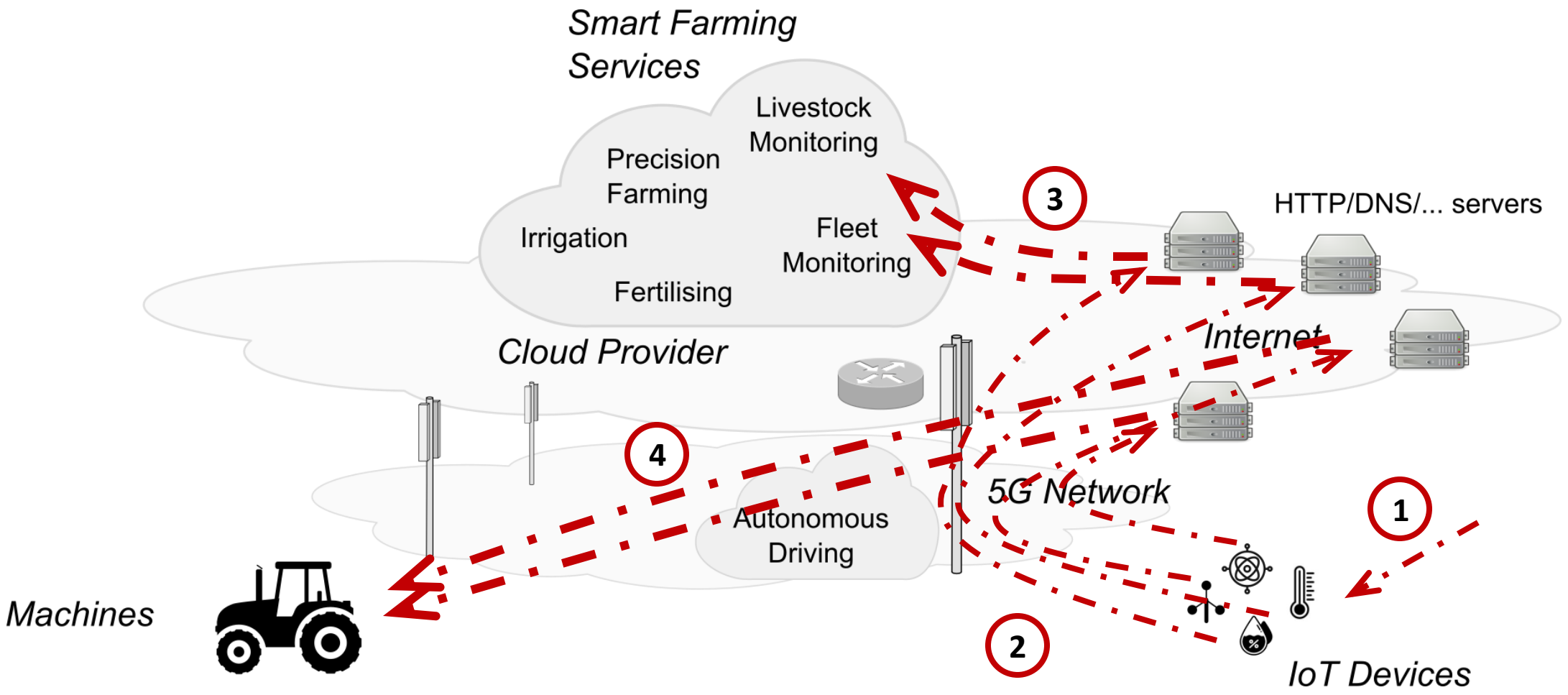
Automotive


Assisted
Driving
Service
Customer
Service
5G network
Edge Computing
Big Data
1
2
3
4
5
6
7
8

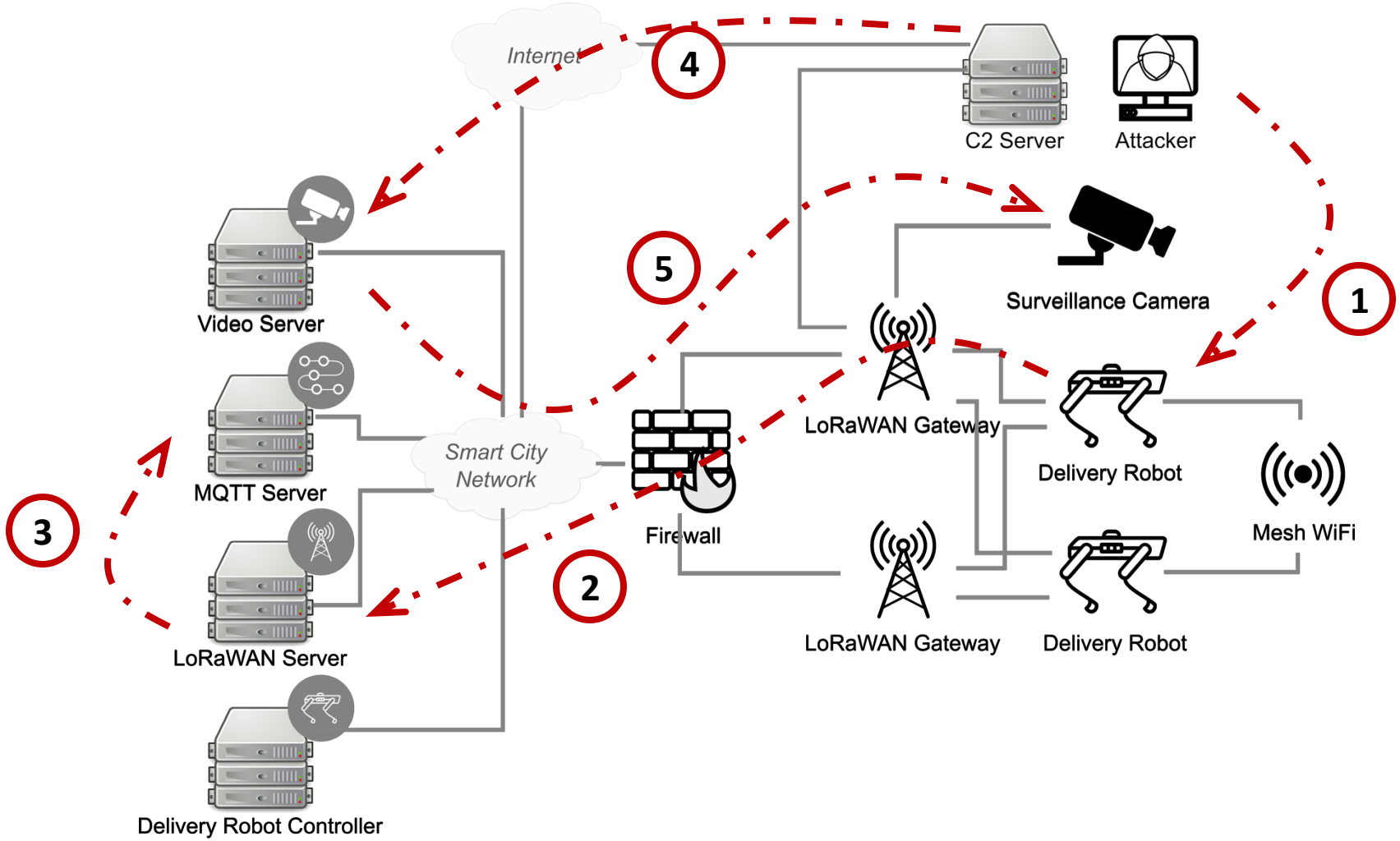
Smart Grid


5
Weather forecasts
TSO
Fault detection
Flow monitoring
SCADA
Operation and maintainance
DSO
Operation and maintainance
Historical statistics
Storage
Data aggregation
Power plant
Renewables
Production scheduling
Load shedding
Production scheduling
3
LoraWAN Network
Access Network/ Edge computing
4
2
1
Generation
Transmission
Distribution
Load

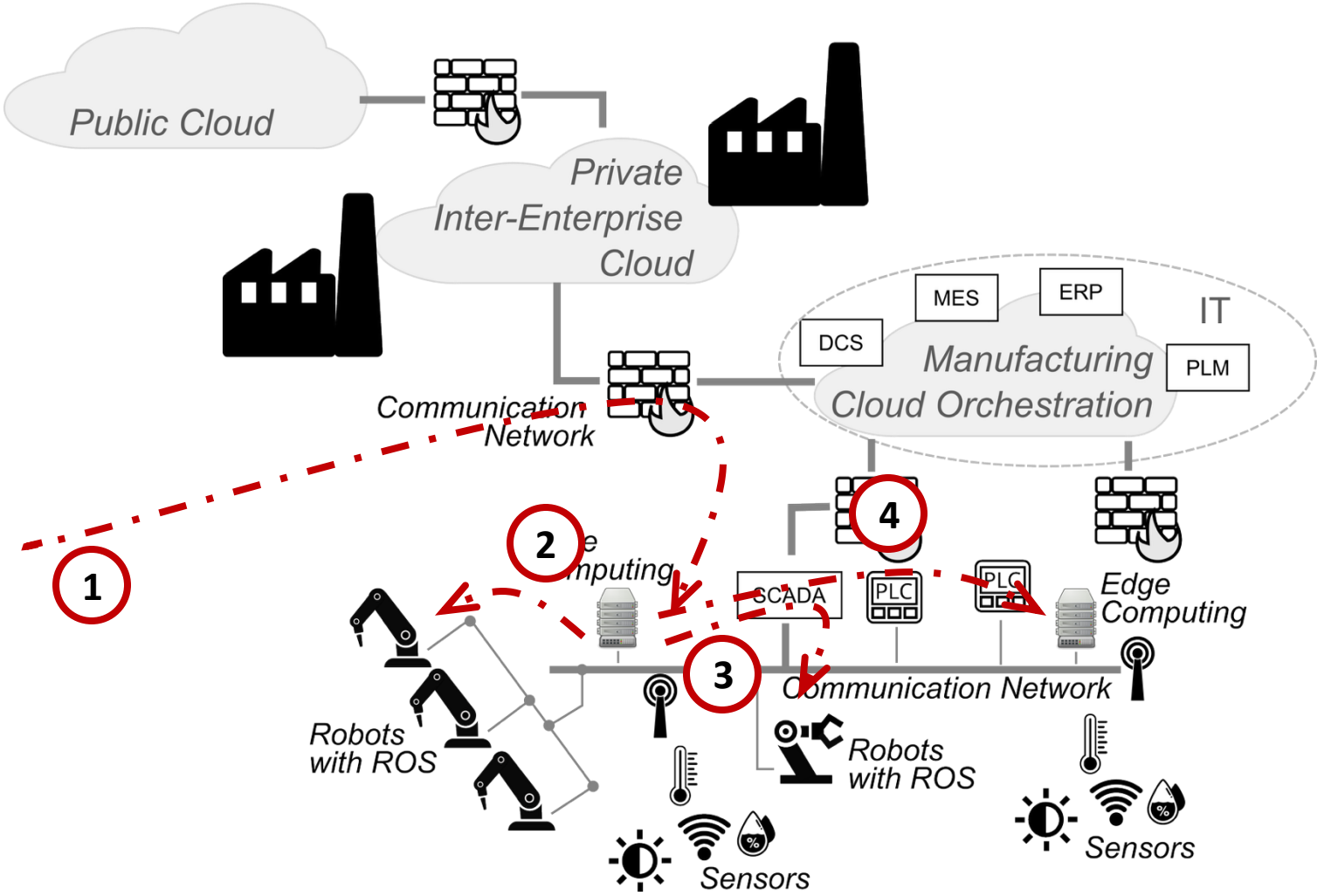
5G Verticals – Smart Farming



Delivery robots



Smart Manufacturing



Security challenges in CPS

- Growing complexity
  - human errors in design, implementation, configuration, and management
- Trustworthiness and reliability of the overall end-to-end service
  - integrity and dependability of the whole chain beyond identity management and access control
  - tracking the propagation of private data and sensitive information
  - weak links represent a privileged attack vector
- Dynamic composition
  - the chain topology and composition are usually unknown
  - difficulty to assess and certify trustworthiness for multi-domain and multi-tenancy services

Security challenges in CPS

- Service integrity
  - timely detect any attack or threat that may compromise the integrity, confidentiality, or availability of data and processes.
- Service trustworthiness
  - trust software developers, things, vendors, service providers, infrastructures, data sources, …
- Data sovereignty
  - know who, how, and where will process private data and sensitive information

Cyber-security for CPS

- What cyber-security framework for CPS?

Digital Twins

- John Vickers (NASA) ~2005
  - publicly used from 2010
- Replication of physical entities by “models”
  - individual components/units:
    - PLCs, historians, sensors, actuators data acquisition units, human machine interface (HMI) units
  - complete manufacturing systems
    - robot loading stations, conveyor belts, etc.

Digital Twins, Shadows, and Models

- **Digital Twin**
  - automated, bi-directional, real-time interaction with the physical system
- **Digital Shadow**
  - automated, mono-directional, real-time interaction
- **Digital Models**
  - manual integration between physical and digital entities

- *Digital Twin is a buzzword today!!!*

Operation mode

- Simulation
  - operated a virtual clone independently of the physical environment
- Replication
  - replaying the events from the physical environment

Digital Twins and security

- Why?
  - security testing, monitoring, intrusion detection and risk management are fundamental activities to carry out
  - testing in the production environment is not always feasible and typically not recommended
- What?
  - A digital twin replication model and corresponding security architecture can be used to allow data sharing and control of security-critical processes [Gehrmann and Gunnarsson, 2020]
  - A digital twin structure to be tested for potential vulnerabilities, updated continuously with cyber-threat intelligence [Atalay and Angin, 2020]
  - Cyber Digital Twin (CDT): a cybersecurity-oriented virtual replica of a system, network, or device that can be used, for example, to simulate potential cyber attacks and test security measures [Somma, 2023]
  - Captures and models the aspect of the enterprise's cybersecurity posture from a hackers' perspective and models hackers' movements [Hadar, 2020]
- How?
  - Derive the Digital Twin from system specification
  - Derive the Digital Twin from cost optimization [Bitton et al., 2018]

Security objectives for a CDT

- Security testing:
  - by connecting real devices in the virtual environment
  - non-invasive penetration testing
- Cybersecurity training:
  - help personnel train on cybersecurity issues and solutions
- Attack/intrusion/anomaly detection
  - simulation from real-time inputs
  - comparison between state of virtual replica with actual system
    - includes also the detection of SW/HW misconfigurations
- Selection of security controls
  - evaluate in advance the impact of specific security controls
- Cyber-threat intelligence (CTI) generation
  - based on the simulation of incident scenarios
- Diagnostic
  - investigate the causes of incidents

Applications

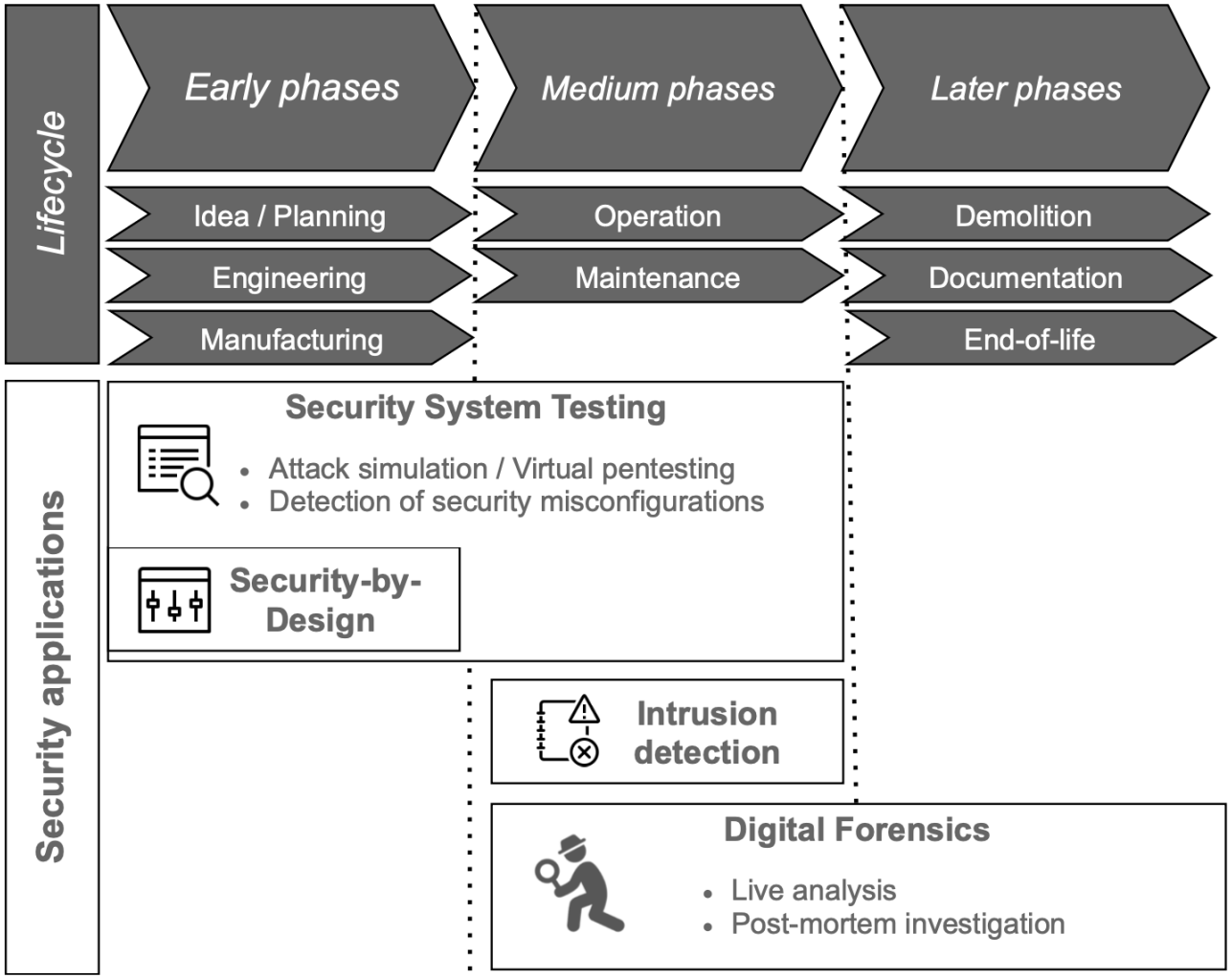
- **Improved patch management:**
  - explore the impact of applying a patch
  - no need to maintain an expensive secondary system
- **Continuous validation of security and other properties**
  - traditionally only tested in late development stages
  - more efficient automation of security tests as part of a more rigorous regression testing regime in the development life-cycle of the OT deployment, providing additional assurance to integrators and stakeholders alike.
  - undertake detailed assessments of potential of system vulnerabilities in anticipation of attacks on critical components of the system
  - investigate and evaluate potential attack vectors
  - understand and test the impact of configurations

Applications

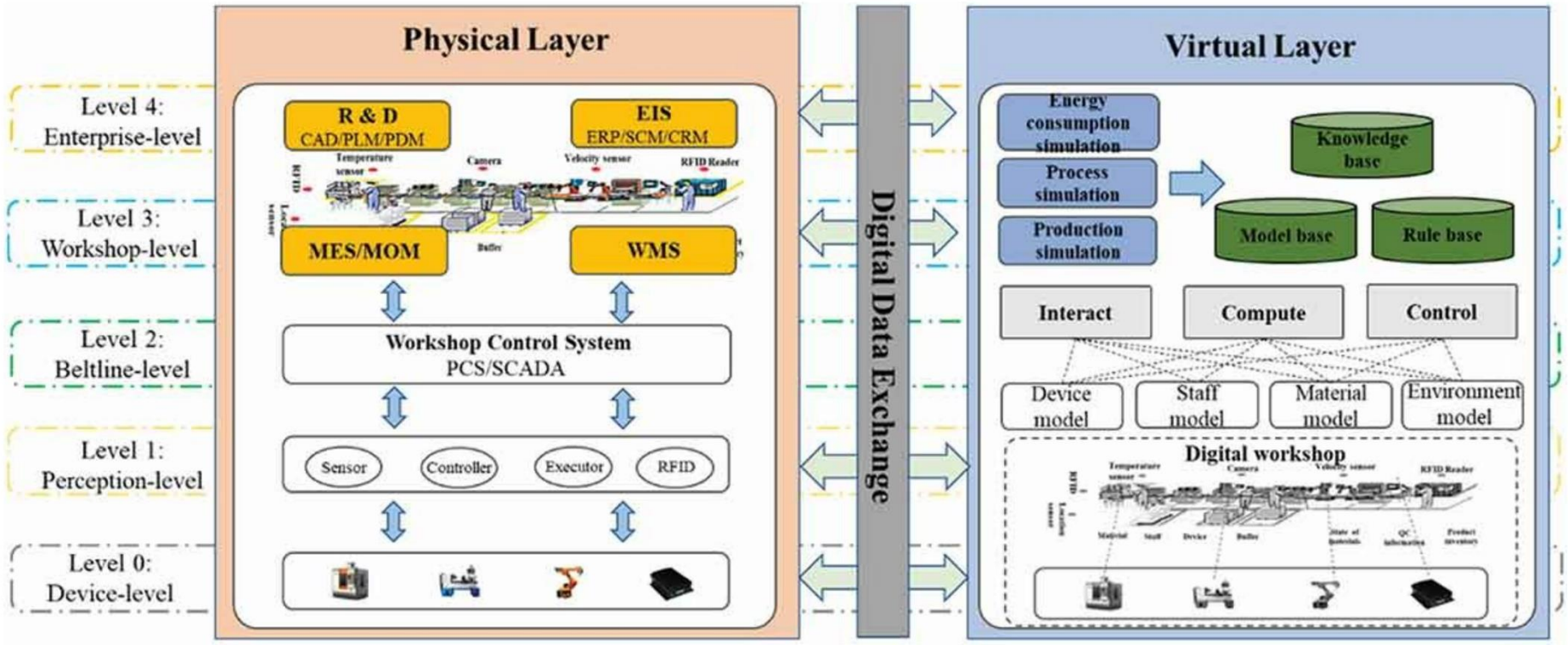
- **Improved risk management:**
  - evaluation of a new system component
  - reducing any potential threat to human safety, or that of the facility or environment.
- **Active Cyber Defence:**
  - understand the impact of any compromise to the system operation and its cyber defence profiles
  - reduce attack vectors and aid incident preparation
- **Advanced Training and Incident Response Capability:**
  - encourage and promote the cyber security practitioner skill development
- **Conformance checking**
  - compliance to reference (i.e., normative) process models through fitness metrics and specific parameters

Applications during lifecycle

- For some authors, a DT might even exist before the physical system
  - simulation only
  - *is this a "model" or a "twin"???*
- Security assessment
  - Active/passive scanning (target identification)
  - Vulnerability analysis
    - retrieved from public feeds
  - Exploitation (attacks)
  - Classification (CVE, CVSS)



DT architectures

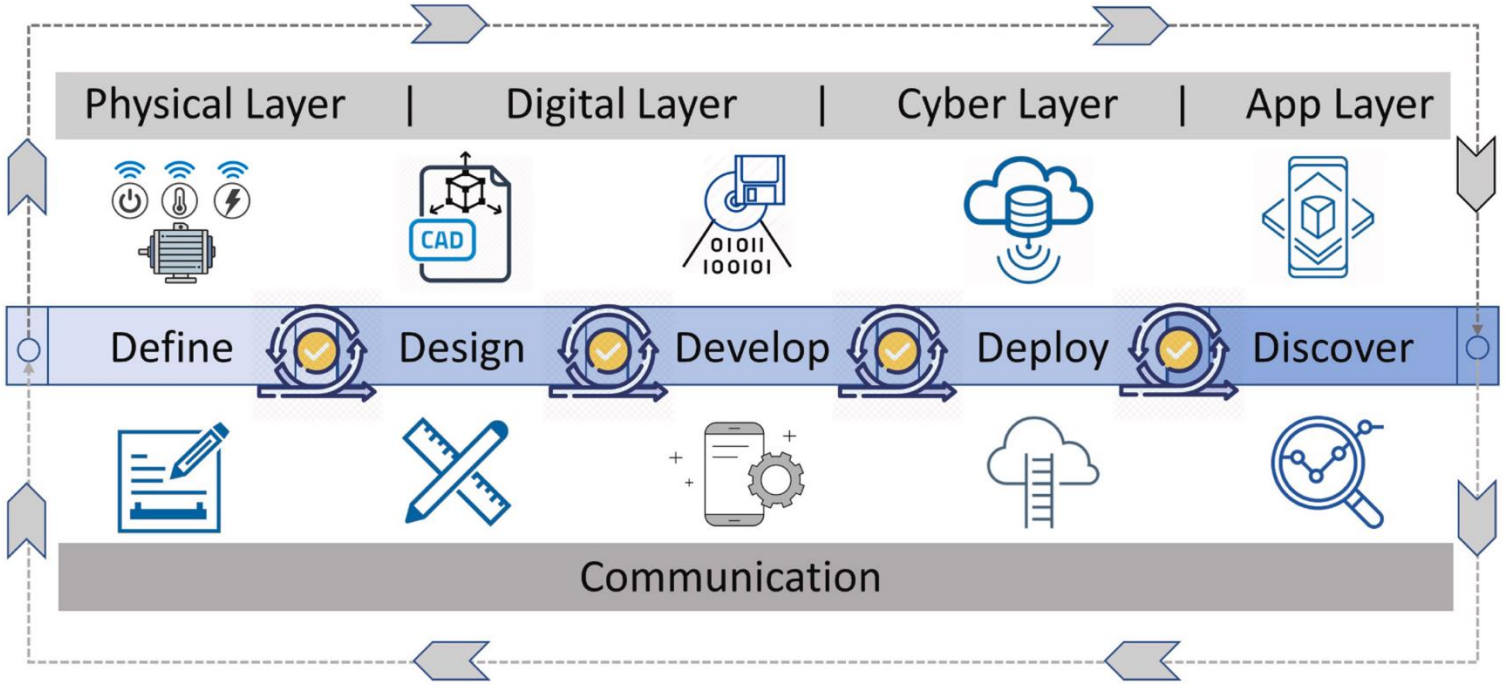


- **Three layers** [Barenji et al. 2021]
  - Physical, Digital, Communications

- Modelling functionalities inside the digital layer are predominant,
- Data and services are not taken into account

A. V. Barenji, X. Liu, H. Guo, and Z. Li, "A digital twin-driven approach towards smart manufacturing: reduced energy consumption for a robotic cell," International Journal of Computer Integrated Manufacturing, vol. 34, no. 7-8, pp. 844–859, 2021

DT architectures



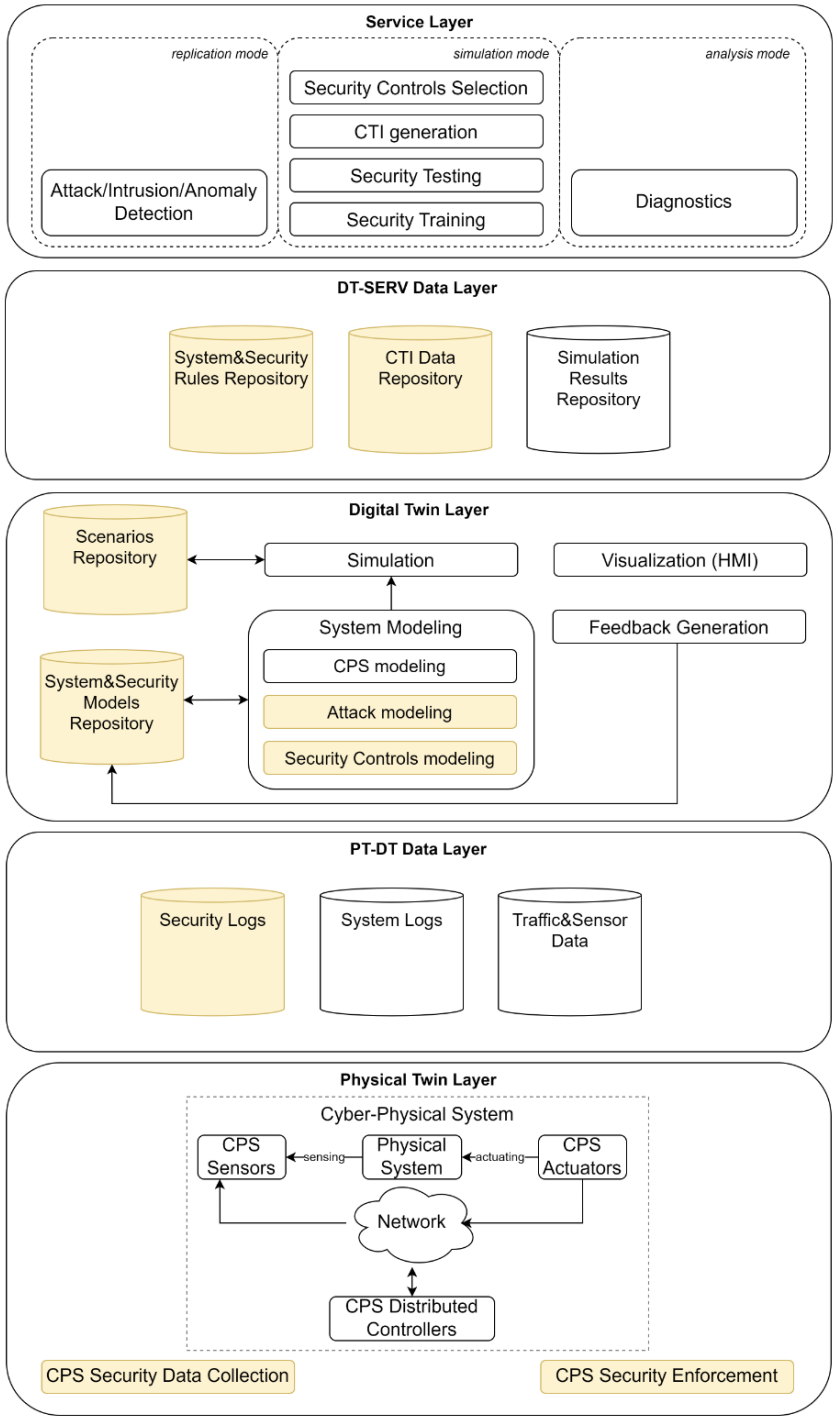
- **Four layers** [Aheleroff et al., 2021]
  - Physical, digital, cyber and application

- Application:
  - Advanced technologies (e.g., AI and data analytics) to extract knowledge from real-time data and underlying
  - build value-added services

S. Aheleroff, X. Xu, R. Y. Zhong, and Y. Lu, "Digital twin as a service (dtaas) in industry 4.0: An architecture reference model," Advanced Engineering Informatics, vol. 47, p. 101225, 2021

DT architectures

- **Five/six layers**
  - Physical = Perception + Control & Actuation [Redelinghuys et al, 2020]
  - Physical = Data collection + Aggregation/pre-processing [Lee et al., 2020]
- Additional layers are introduced to cope with cross-cutting issues
  - security and or privacy
- System Modelling: static or dynamic comprehensive model of the CPS, including functional and security-related aspects
- Attack modelling: attack graphs, attack trees and Petri nets
- Operational modes: analysis, simulation, replication



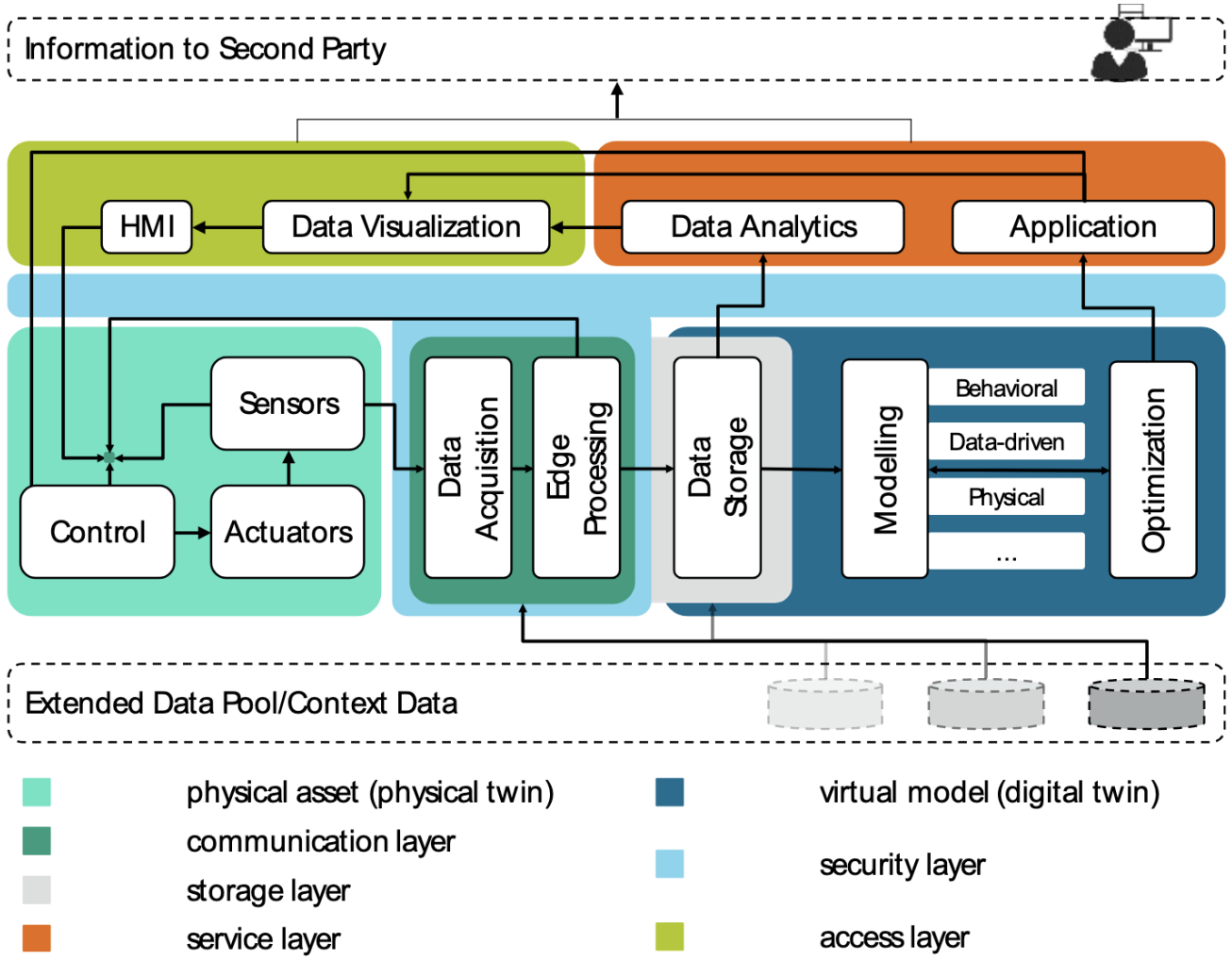
A. J. H. Redelinghuys, A. H. Basson, and K. Kruger, "A six-layer architecture for the digital twin: A manufacturing case study implementation," J. Intell. Manuf., vol. 31, no. 6, p. 1383–1402, aug 2020

J. Lee, M. Azamfar, J. Singh, and S. Siahpour, "Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing," IET Collaborative Intelligent Manufacturing, vol. 2, no. 1, pp. 34–36, 2020

imati

DT architectures

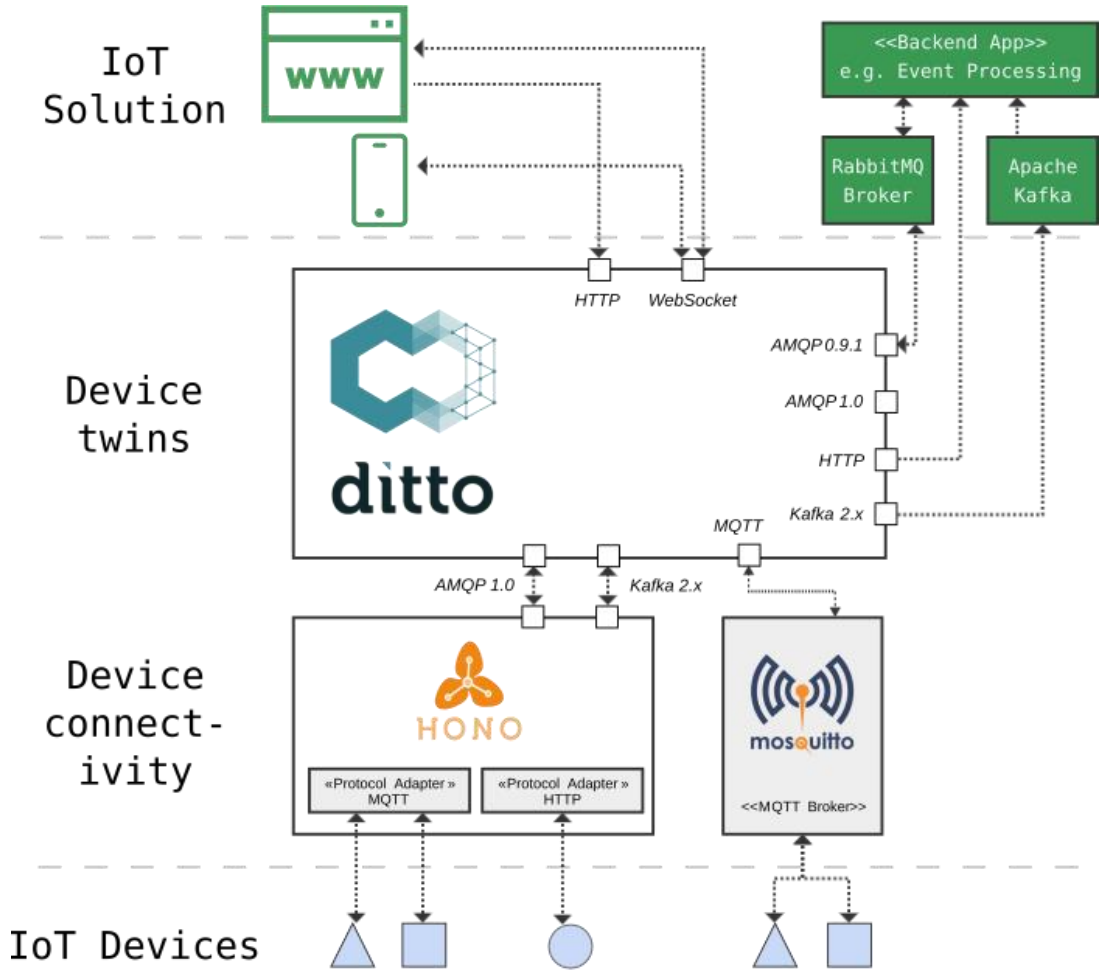
- **Seven layers** [Singh et al, 2020]
- Five layers +
  - security layer
  - access layer
    - interfacing between human and DTs



S. Singh, M. Weeber, and K.-P. Birke, "Advancing digital twin implementation: a toolbox for modelling and simulation," Procedia CIRP, vol. 99, pp. 567–572, 2021, 14th CIRP Conference on Intelligent Computation in Manufacturing Engineering, 15-17 July 2020

Example: Eclipse Ditto

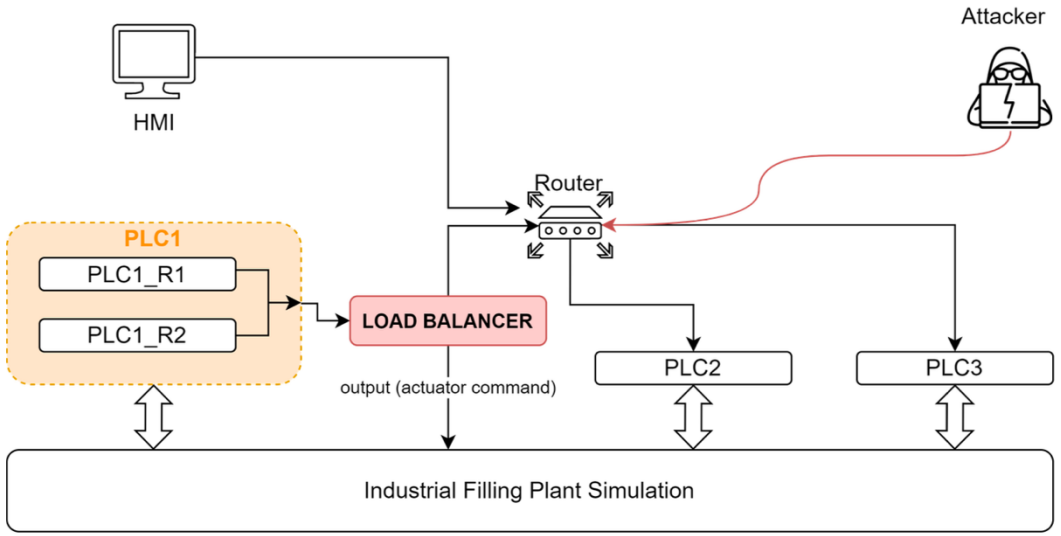
- *Device as a Service*
  - digital twin API to work with physical device
- *State management for digital twins*
  - reported, desired, and current state of devices
  - synchronization and publishing of state changes
- *Access control enforcement*
  - fine-grained resource based access



https://eclipse.dev/ditto/

Simulate cyber-attacks and test countermeasures

- PLC emulated with minicps
  - actuator, sensors, control logic
- 2 attacks against PLC1:
  - command injection
  - DoS
- Countermeasure:
  - load balancer
- *Only simulation, with no physical input/output [where is the DT??]*
- Attack on communication protocols

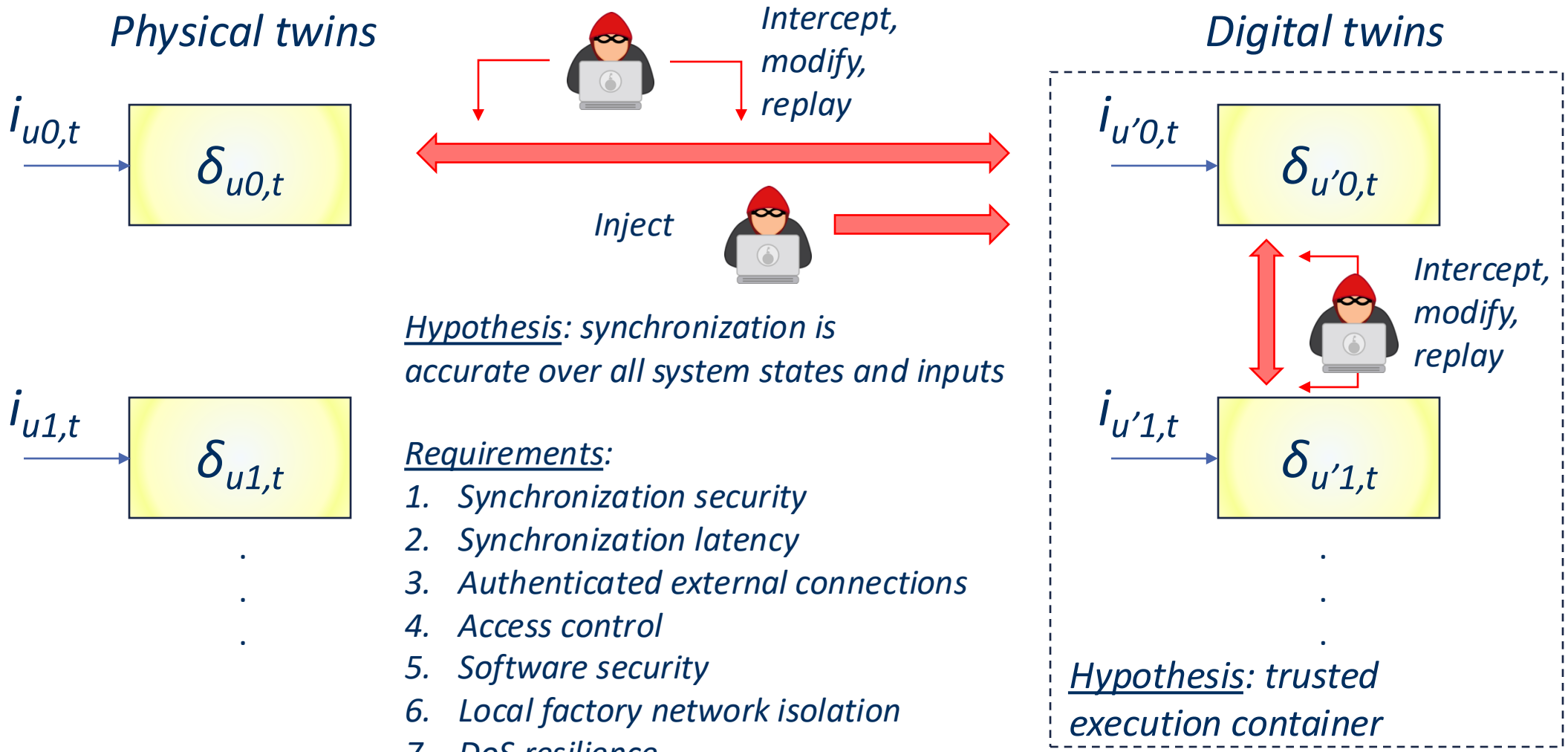


A. Somma, V. Casola, A. R. Cavalli, A. De Benedictis, W. Mallouli, V. E. Valdés. A Cyber Digital Twin Framework to Support Cyber-Physical Systems Security. IEEE Smart World Congress (SWC), Portsmouth, United Kingdom, 28-31 August 2023.

Digital representation to be tested

- Building blocks
  - An extensible/modifiable digital twin representation
    - built semi-automatically from the formal specification (Eckhart and Ekelhart)
    - the framework should provide means for defining characteristics of common physical elements, which can be reused in multiple models
  - A cyber-threat intelligence database
    - the security evaluation will be continuous due to new threats arising
  - Attack simulation toolset
    - implementations of the attacks in the threat intelligence database
  - A data analysis and reporting module
    - makes vulnerability inferences and risk assessment based on the results of attack simulations performed on the digital twin
- **How to design a DT that capture vulnerabilities and weakness of its physical counterpart?!?!**

Attack model



Hypothesis: synchronization is accurate over all system states and inputs

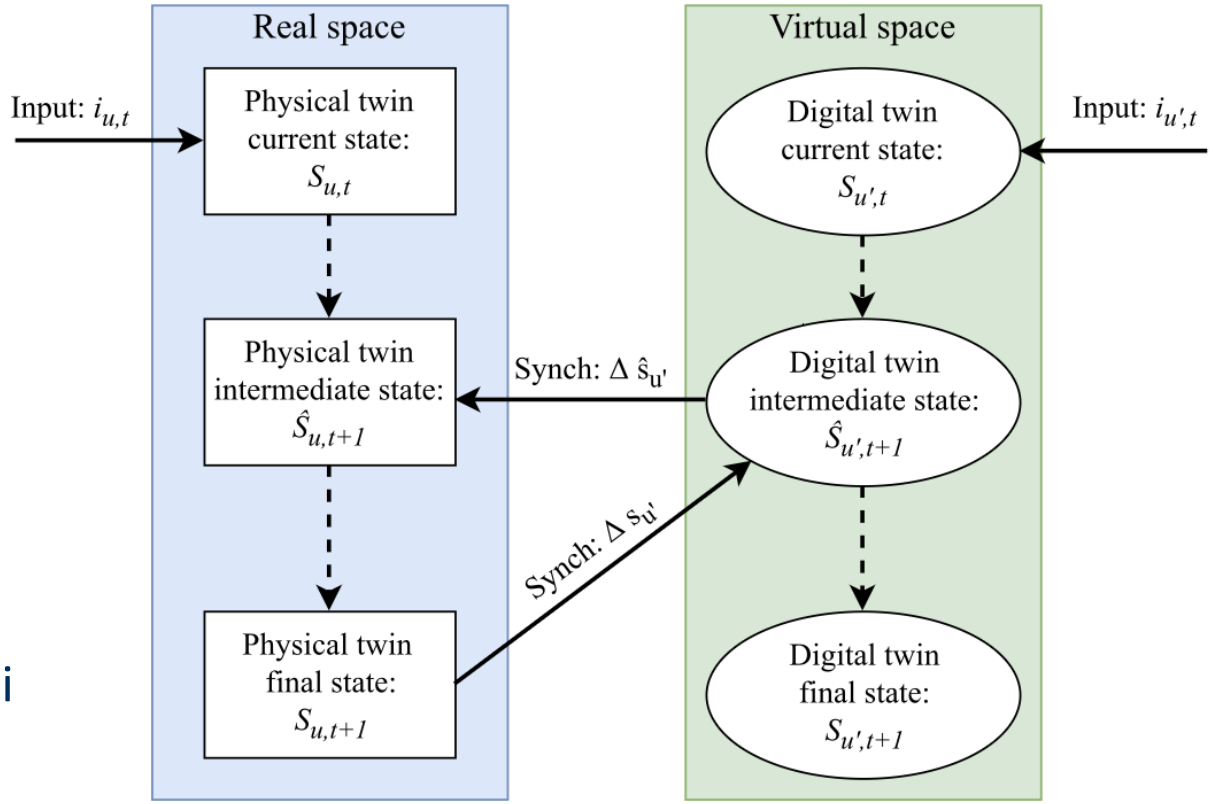
Requirements:

1. *Synchronization security*
2. *Synchronization latency*
3. *Authenticated external connections*
4. *Access control*
5. *Software security*
6. *Local factory network isolation*
7. *DoS resilience*

C. Gehrmann, M. Gunnarsson. A Digital Twin Based Industrial Automation and Control System Security Architecture. IEEE Trans. on Industrial Informatics, Vol. 16, No. 1, pp. 669-680, 2020.

Protect against attacks

- State replication
  - *passive state replication*: physical and digital twins run functionally identical programs
    - evaluate security breaches stemming from the physical domain
  - *direct state replication* or *active monitoring*: physical and digital twins are synchronized on regular basis
    - detect potential hostile, external stimuli on the physical domain



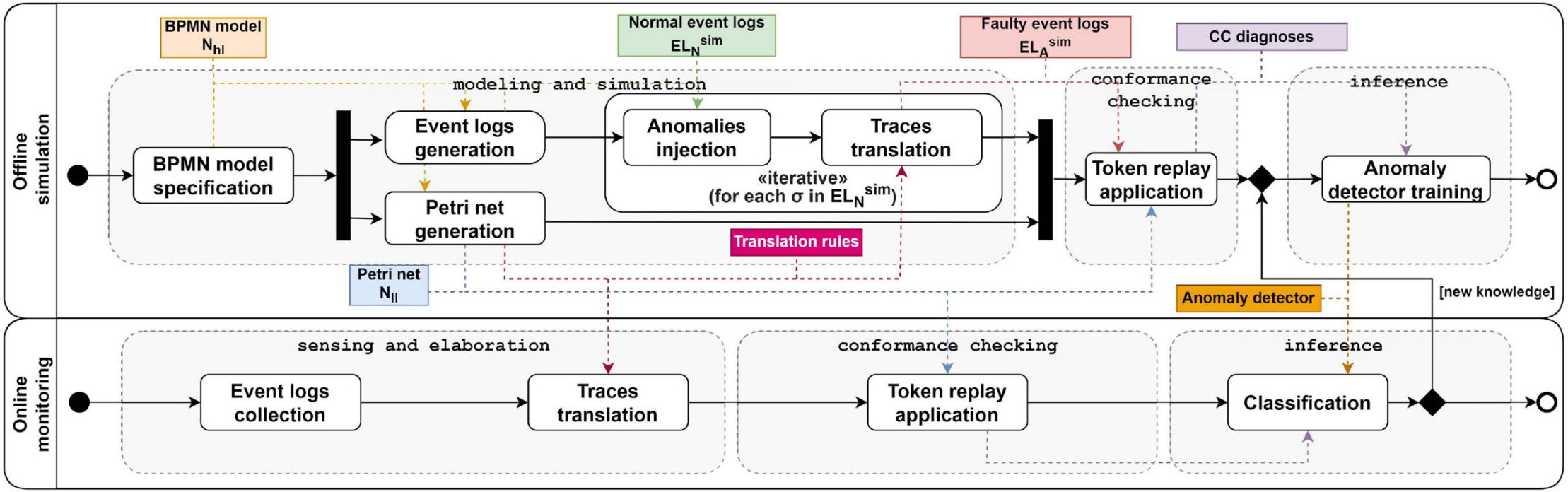
C. Gehrmann, M. Gunnarsson. A Digital Twin Based Industrial Automation and Control System Security Architecture. IEEE Trans. on Industrial Informatics, Vol. 16, No. 1, pp. 669-680, 2020.

Use case

- PLC unit (u_1) (OpenPLC)
- Software upgrade server (u_2)
- A remote operator control u'_2 and u'_1 to download new software packages and trigger the update, respectively
- State synchronization trigger physical systems u_2 and u_1 to perform the same operation
- [*No input is considered!?!*]
- Security mostly relies on the (many) requirements

C. Gehrmann, M. Gunnarsson. A Digital Twin Based Industrial Automation and Control System Security Architecture. IEEE Trans. on Industrial Informatics, Vol. 16, No. 1, pp. 669-680, 2020.

Anomaly detection

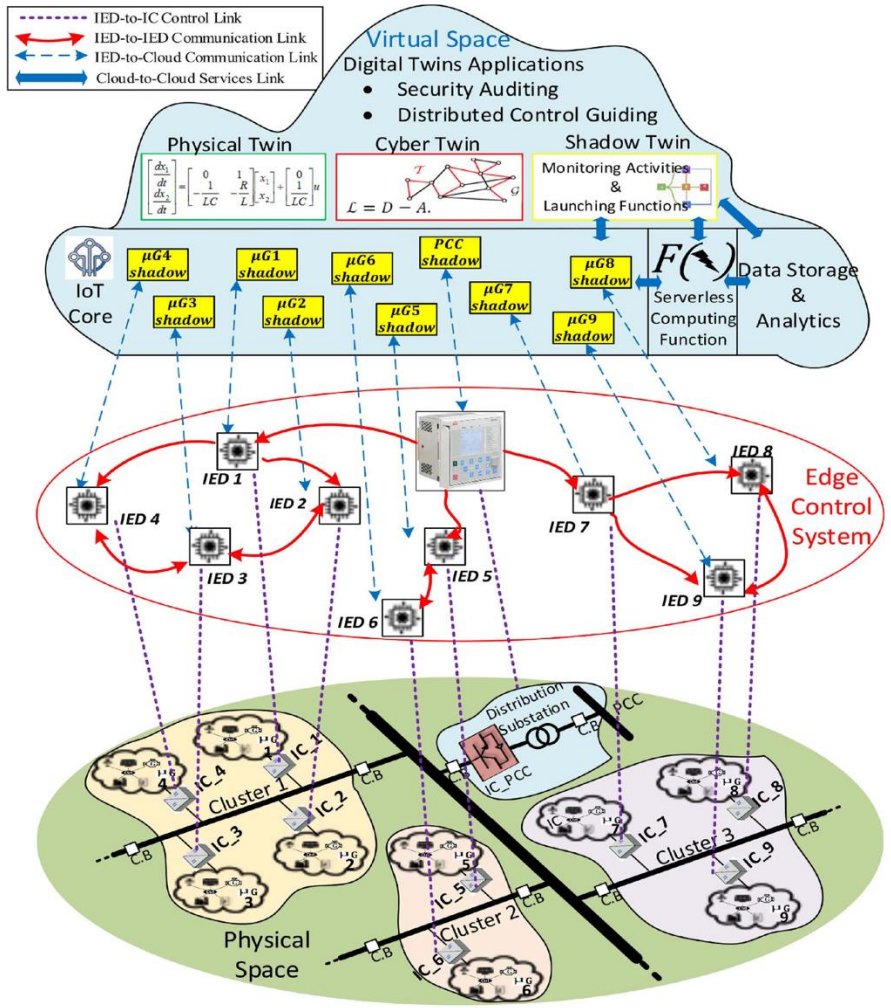


- DT used to train ML-based Anomaly detector
  - Offline simulation
- Only control flow anomalies are generated
  - No cyber-attacks

- Petri Net used to create “features” from event logs
  - Offline simulation & Online monitoring
  - Anomalies are also injected in OM during experiments

A. De Benedictis et al. Digital Twins for Anomaly Detection in the Industrial Internet of Things: Conceptual Architecture and Proof-of-Concept. IEEE Trans. on Industrial Informatics, Vol. 19, No. 12, pp. 11553 – 11563, 2023

Anomaly detection - 2

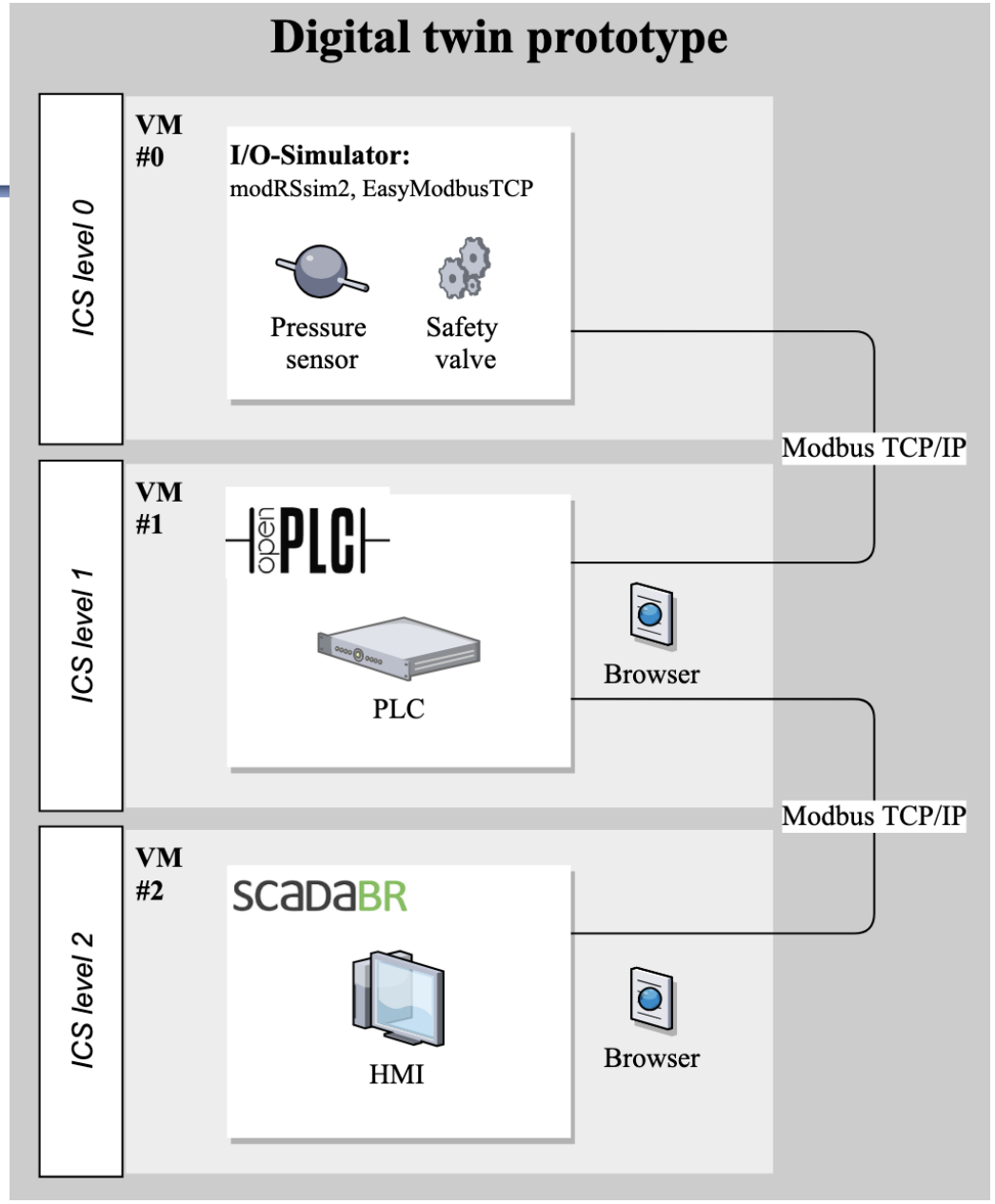


- Digital Twin made of:
  - electrical model of microgrids (PT)
  - control flow model (CT)
  - measures from devices (ST)
- Anomaly detection
  - compares DT status with measures from (emulated) grids
- No real protocols in the emulator
- Only energy flow models, no ICT monitoring
  - *how to distinguish failures?*

A. Saad et al. On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks. IEEE Transactions on Smart Grid, Vol. 11, No. 6, pp. 5138-5150, 2020

Security assessment

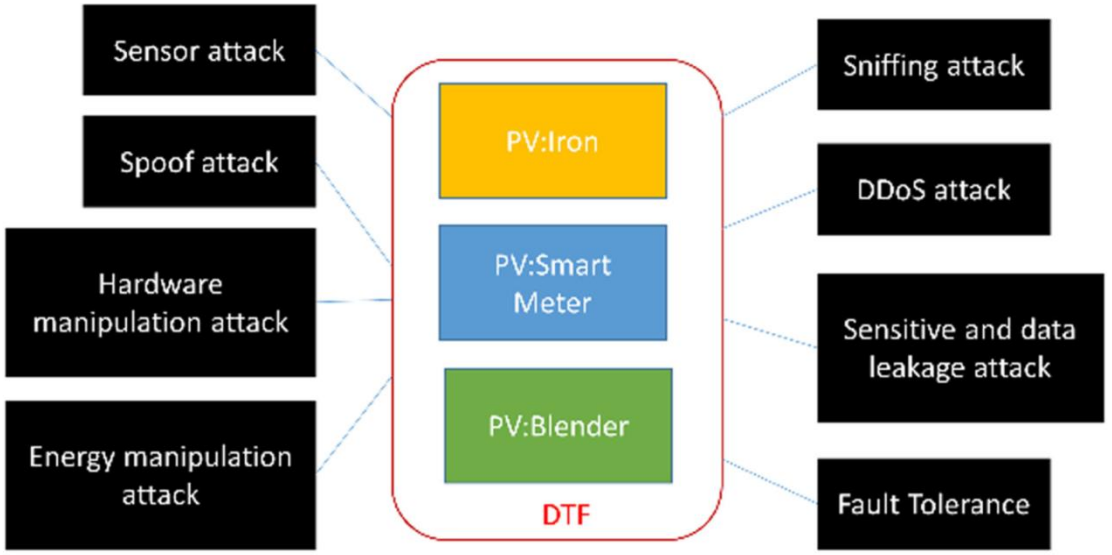
- Pressure vessel use case
  - PLC monitors sensor and controls actuator
- Security-by-design
- Simulator
  - OpenPLC
  - I/O-Simulator
  - ScadaBR
  - Run in VMs
- Metasploit + C++ script to alter ModBus communication
  - [*Weak discovery phase*]

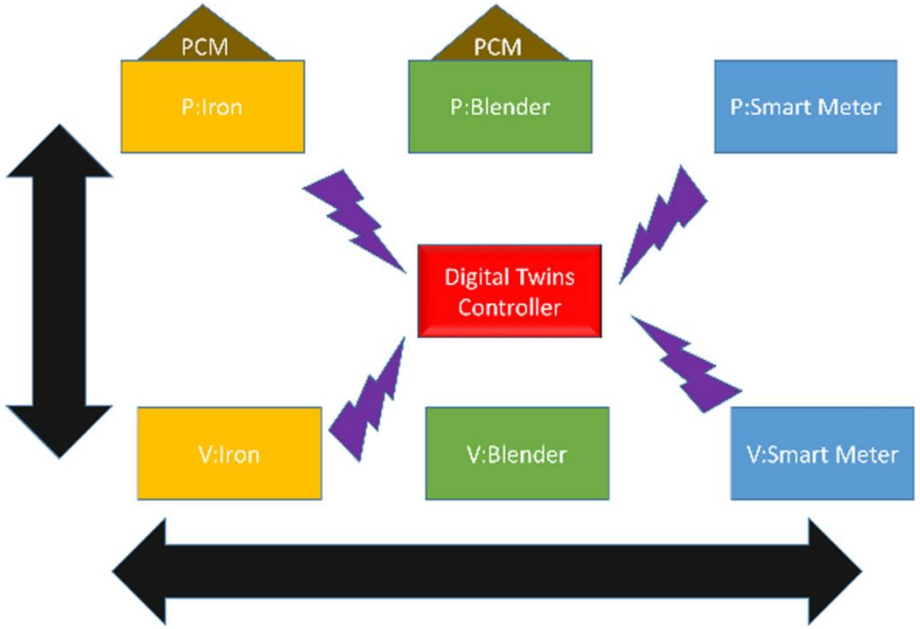


M. Dietz, L. Hageman, C. von Hornung, G. Pernul. Employing Digital Twins for Security-by-Design System Testing. Sat-CPS '22: Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Pages 97 – 106, 2022

Attacks against the DT and its links

- The DT controller collects data about the state of physical objects
  - Historical data are kept
  - Data-only DT (no backward communication channel)
- No indication about ML algorithms detect anomalies
- *What is the DT useful for?*

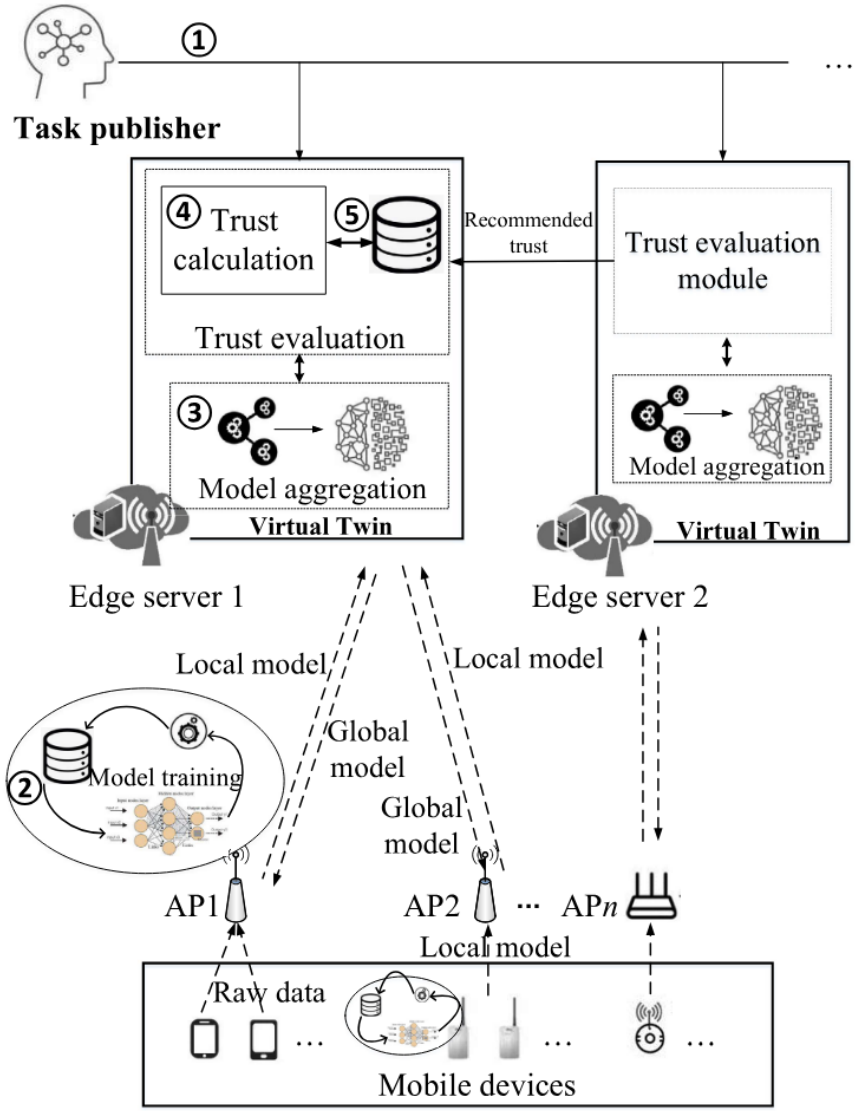




J. C. Olivares-Rojas; E. Reyes-Archundia; J. A. Gutiérrez-Gnecchi; I. Molina-Moreno; J. Cerda-Jacobo; A. Méndez-Patiño. Towards Cybersecurity of the Smart Grid Using Digital Twins. IEEE Internet Computing, Volume: 26, Issue: 3, May-June 2022, pp. 52 - 57

Trusted Federated Learning

- FL as kind of DT
- Privacy-preserving
- Vulnerable to data poisoning
- Distributed trust mechanism
  - local/remote trust levels
  - trust depends on accuracy and delay of updates



J. Guo, Z. Liu, S. Tian, F. Huang, J. Li, X. Li, K. K. Igorevich, and J. Ma. TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks. IEEE Journal on Selected Areas in Communications, Volume: 41, Issue: 11, November 2023, pp. 3548 – 3560

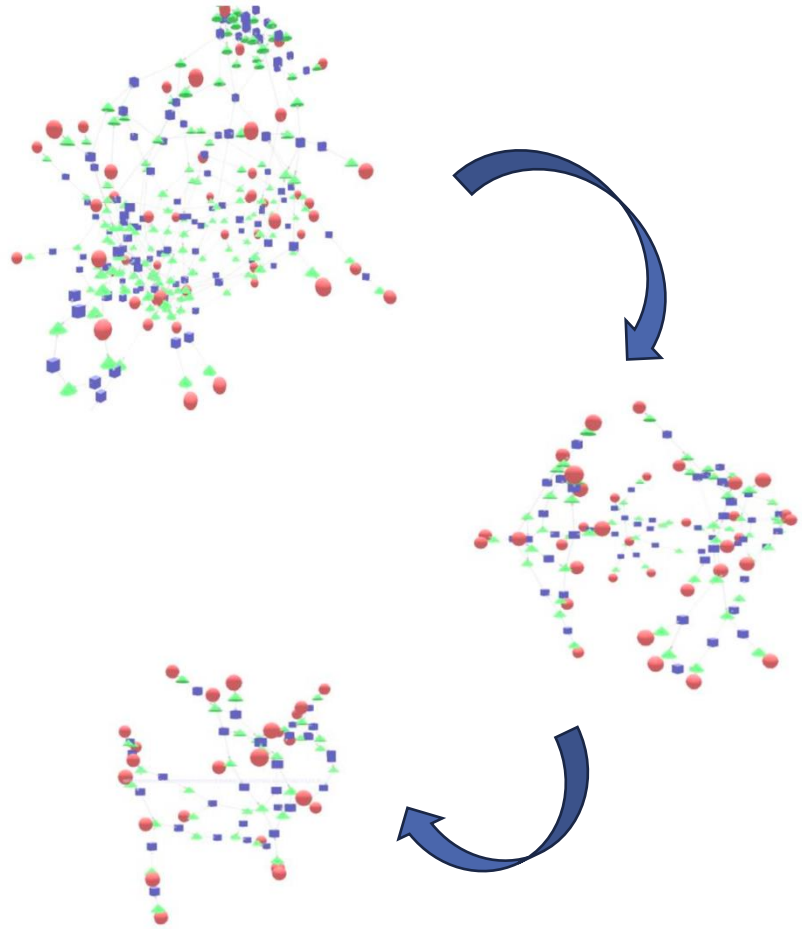
Prioritize security controls

- Analytical Attack Graphs (AAG)
  - logical Rules that define how an attacker advances within the network
  - derived from MITRE ATT&CK
- Graph Risk Value (GRV)
  - a measure of the organization's cyber risk exposure
  - evaluated by cyber-security experts
  - reflects the difficulty to implement rules in AAG
- Security Controls (SCs)
  - countermeasures elaborated by experts to mitigate the impacts of Rules
- Traceability Matrix (TM)
  - maps SCs to Rules in AAG

E. Hadar et al. Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls' Requirements. IEEE 28th International Requirements Engineering Conference (RE), 2020.

Prioritize Security Controls

- Algorithms for risk reduction
  - Gradient reduction
  - Area Under Curve (AUC)
- Select SCs that reduce the number of Rule types nodes in the corresponding AAG
  - implementation of SCRs is costly and time consuming
- Cyber Digital Twin captures
  - attack behaviour
  - system configuration
    - user account hierarchies, installed software and its version, open sessions, memory map, vulnerability, user group membership, or a network-share access permission



imati

E. Hadar et al. Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls' Requirements. IEEE 28th International Requirements Engineering Conference (RE), 2020.

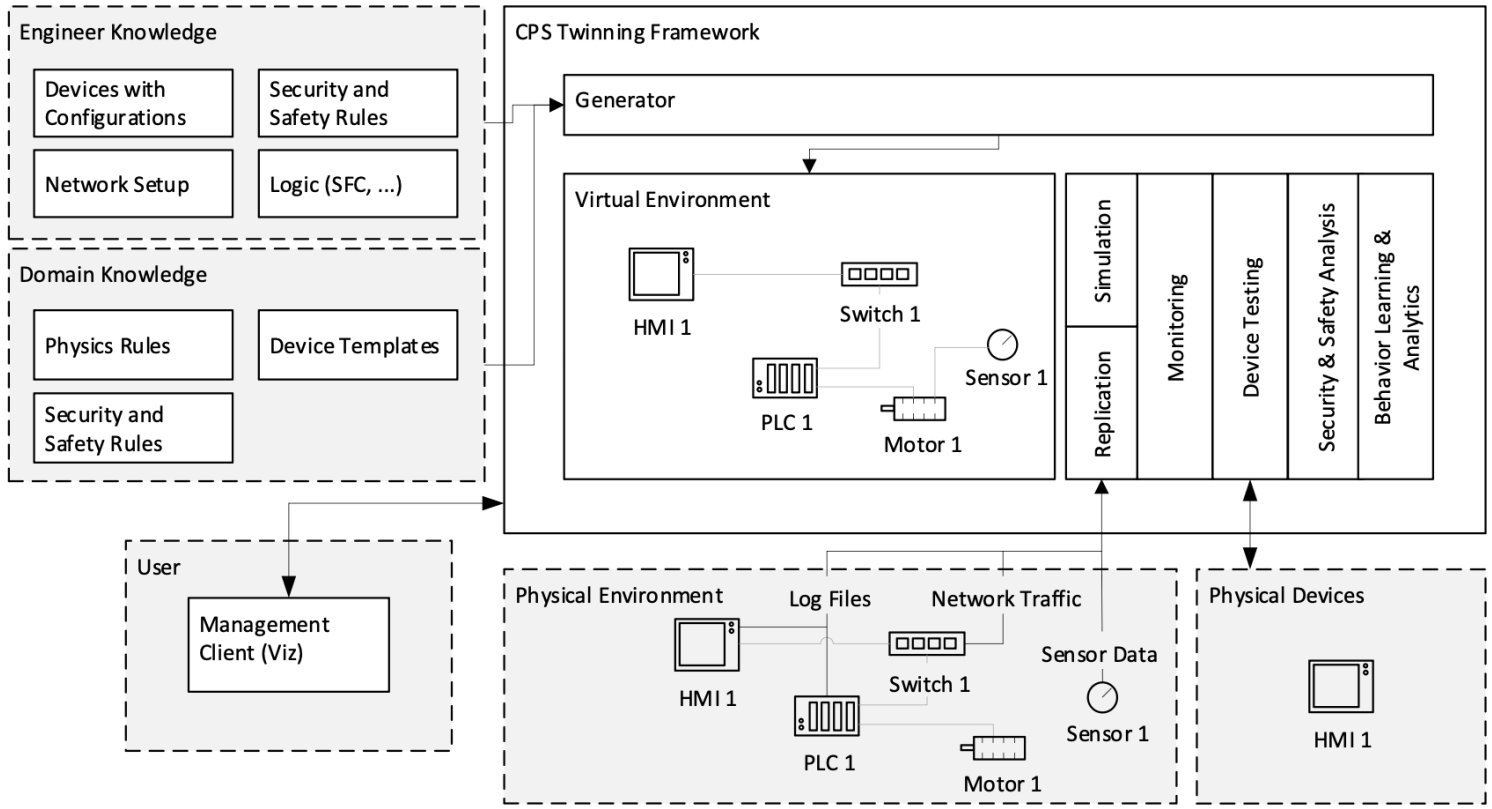
Cost-effective Digital Twin specification

- An adaptive method for deriving a digital twin specification for a given ICS, under strict budget constraints
- Impact evaluated by the number and types of supported pen-tests
  - benefits (detection/protection) vs costs (implementation)
- Three types of implementation:
  - physical, virtualization/emulation, and software simulation
- Output: the type of implementation for each ICS component (physical, emulation, software)
- Optimization: 0–1 non-linear programming problem

Bitton, R. et al. (2018). Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation. In: Lopez, J., Zhou, J., Soriano, M. (eds) Computer Security. ESORICS 2018. Lecture Notes in Computer Science(), vol 11098. Springer, Cham

CPS Twinning

- **Generator**: transforms the specification into a virtual environment
  - parse the specification to extract the topological structure
  - build the virtual environment
  - apply configurations
- **Virtual Environment**: virtualized infrastructure and runtime for virtual devices
  - control logic, network protocols, device types and the physical equipment
  - cloning of cyber components + simulation of physical components
    - file-based storage for sensor and actuator values, or hardware-in-the-loop (HIL)

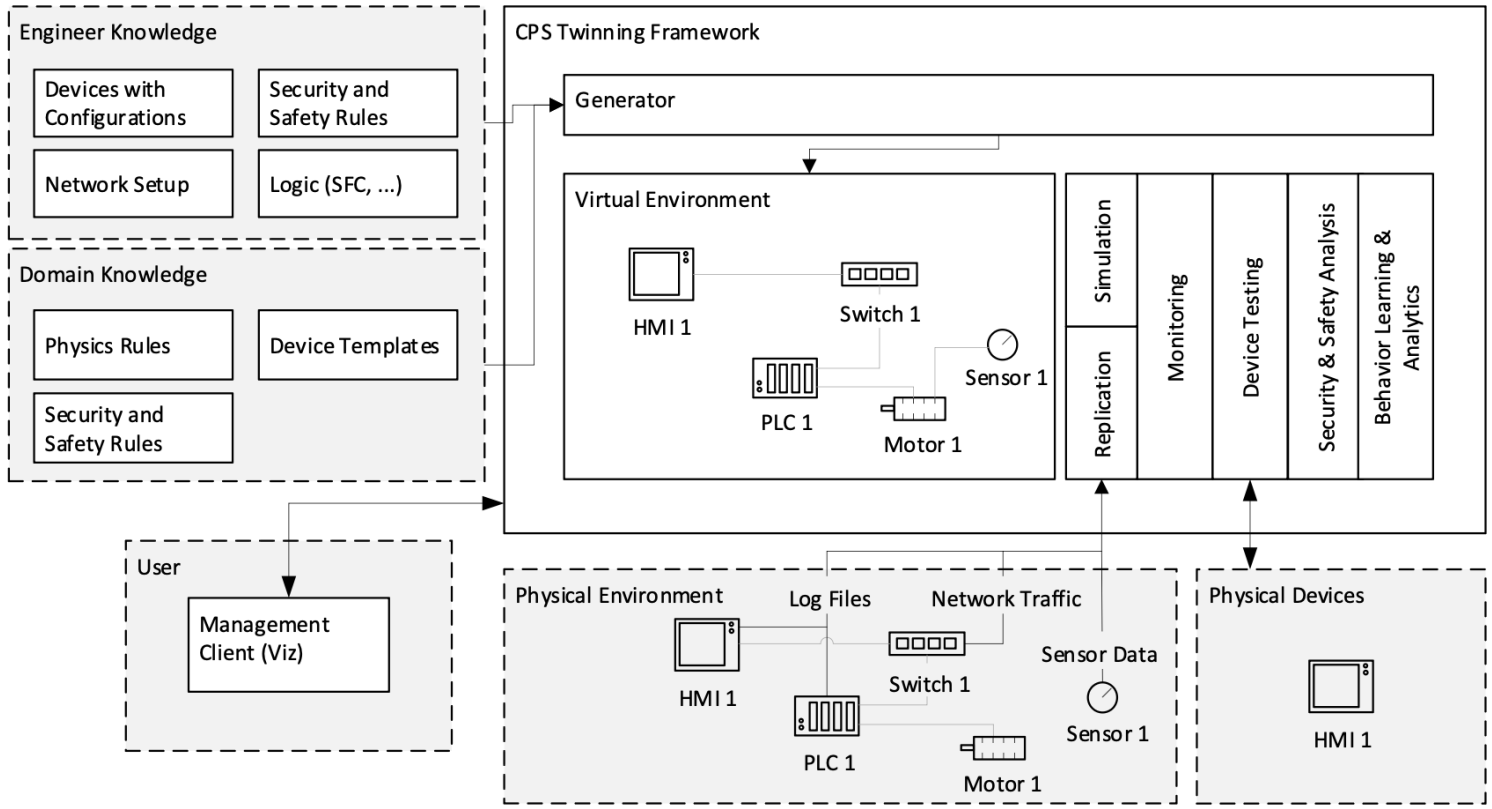


- **Simulation & Replication**:
  - Simulation: the digital twins run independently of physical counterparts. This mode allows users to analyze process changes, test devices or even optimize manufacturing operations
  - Replication: mirrors data (even unidirectional to avoid side effects) from the physical environment (either in real-time or offline). Possible data sources: log files, network traces, and sensor measurements

Eckhart, M., & Ekelhart, A. (2018c). Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, CPSS '18 (pp. 61–72). New York, NY: ACM.

CPS Twinning

- **Monitoring**: sensor values and actuator states can be collected and prepared for analysis and visualization
  - monitoring the physical process in replication mode and then switching to simulation mode allows to investigate a certain state.
- **Device Testing:** virtual commissioning.
  - test physical devices by integrating them into the virtual environment
- **Security & Safety Analysis**: comparison against security and safety rules from the specification
  - In replication mode, abnormalities emerge identically
  - Run simulations in the virtual environment
  - The DT has access to all states and events and thereby can also monitor state changes over time.
  - Foundation for a behaviour-specification-based IDS



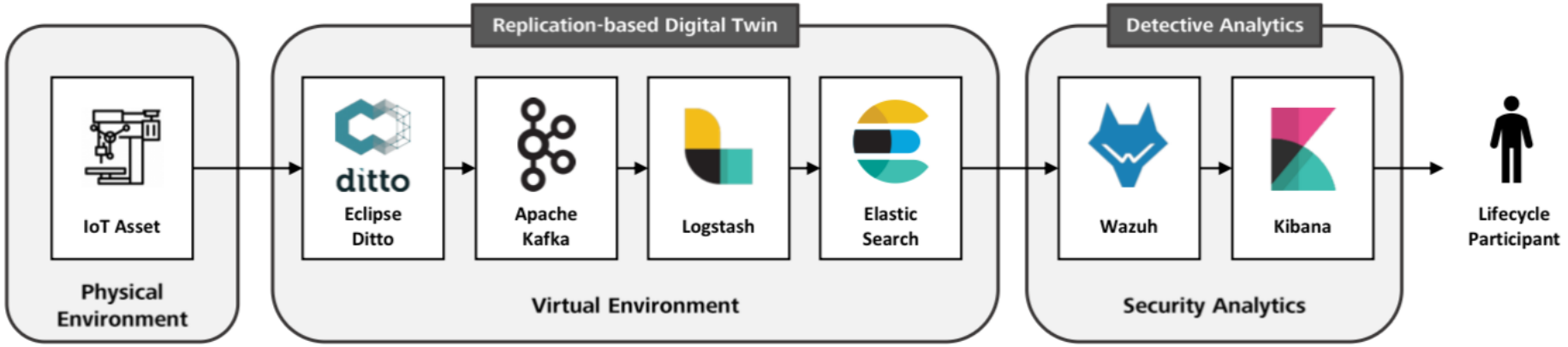
- **Behaviour Learning & Analysis**: valuable input for process optimization and anomaly detection
  - track down process bottlenecks or other factors that negatively affect the process or the quality of manufactured products

Eckhart, M., & Ekelhart, A. (2018c). Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, CPSS '18 (pp. 61–72). New York, NY: ACM.

Detection on IoT devices

- Eclipse Ditto for DT
- DT is the “data” interface to access devices
- Security analytics linked to DT API instead of security agents

- IoT devices “controllable” or “accessible”
- Challenging to link security data to complex system
  - No agents
- *Not clear how Wazuh takes data without its agents*



P. Empl, G. Pernul, Digital-Twin-Based Security Analytics for the Internet of Things, Information 2023, 14(2), 9.

Evolving CPS: The rise of digital ecosystems

Service chaining

Recursive (and hidden) service chaining

Recursive (and hidden) service chaining

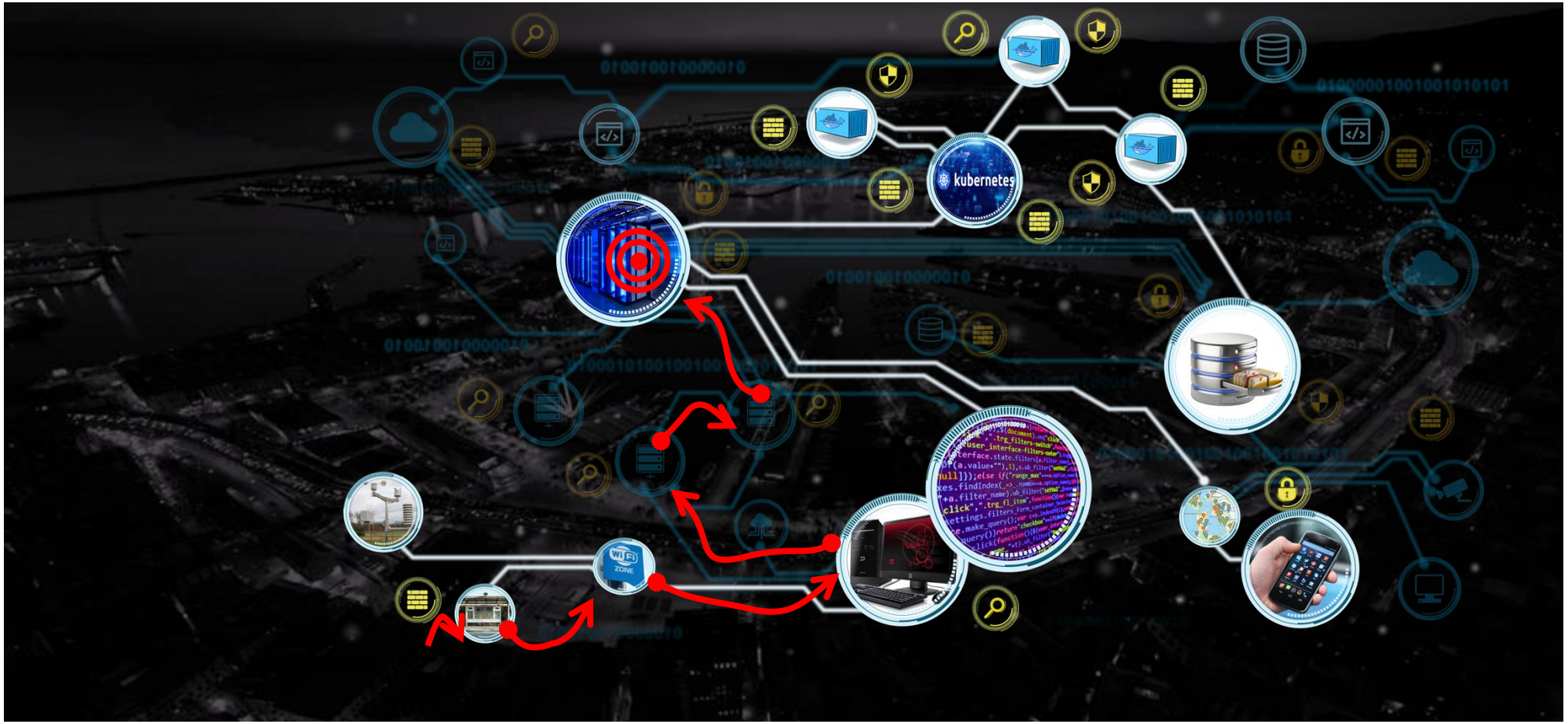
The dark side of interconnectedness

Security functions

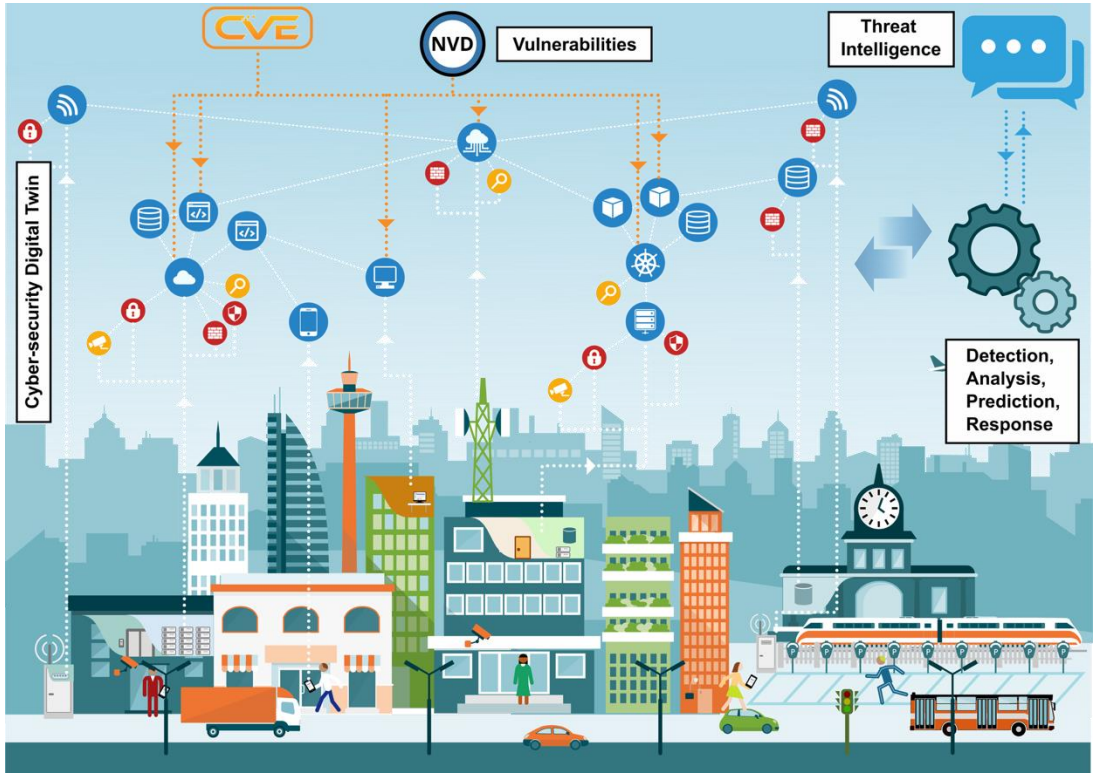
Security challenges

- Fragmentation of security operations
- Visibility
- Coordinated and timely detection and response
- Integration and automation
- Trust and confidentiality
- **Multi-step attacks and cyber kill chains**

Security pitfalls



The challenge



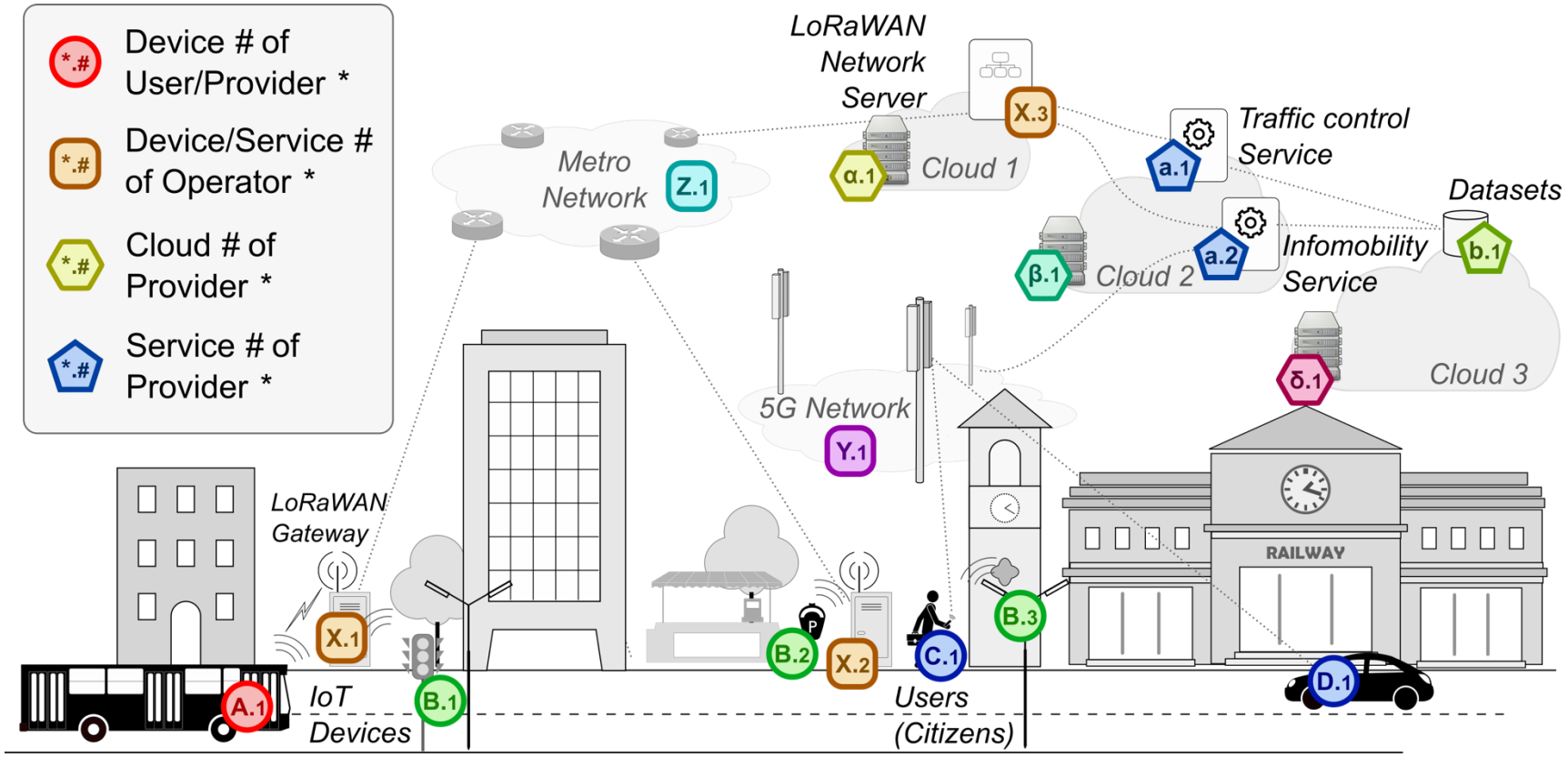
- A framework for **collaborative** cyber-security operations over service supply chains:
- a Cybersecurity Digital Twin (CDT)
  - discovers the composition and topology,
  - models potential threats,
  - predicts their materialization and propagation;
- monitoring, detection, investigation, and response processes
  - leverage the CDT to
  - **proactively and adaptively** protect single components as well as the whole system.

Discovering and modelling

Discovering and modelling

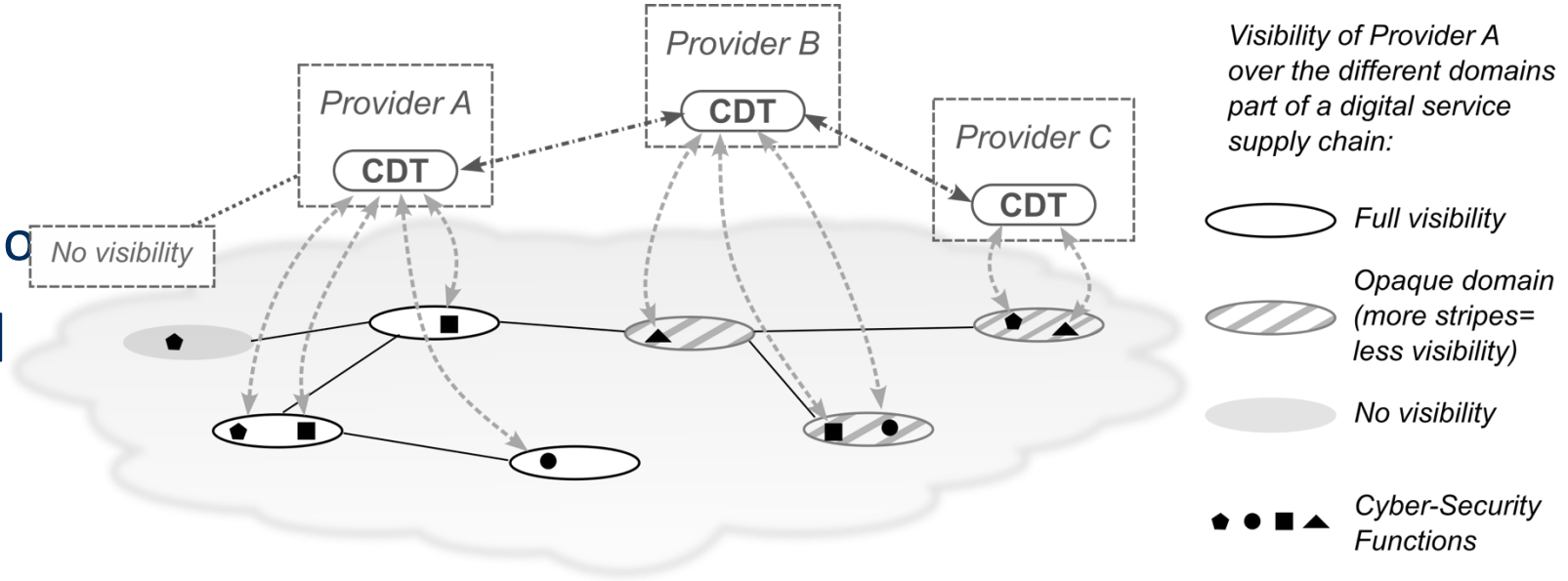
Cyber-security Digital Twin (CDT)

The main purpose for a CDT is **mapping threat intelligence** to the real system, to **make hypothesis, perform analysis, and draw predictions** of what could happen in the real system in a proactive yet not invasive way

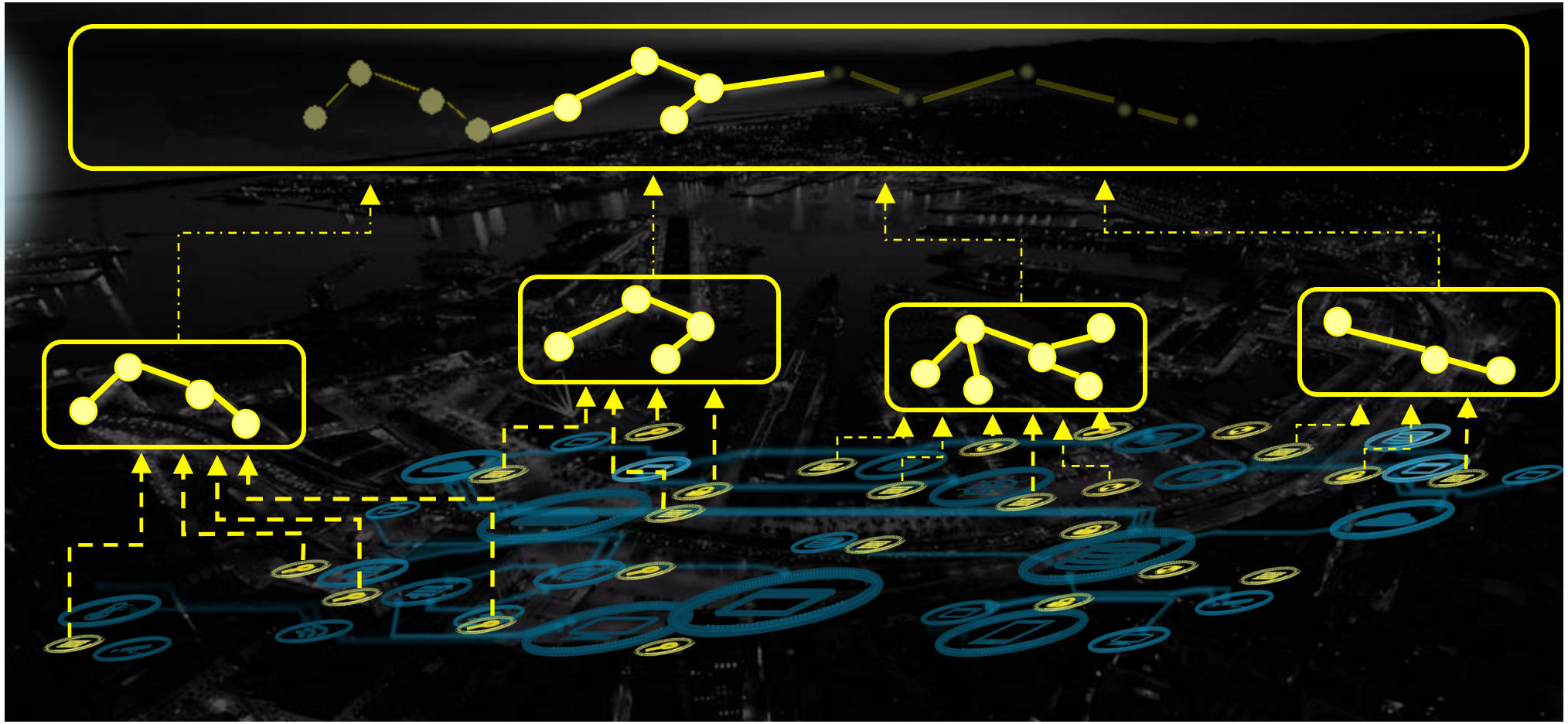


Federation of CDTs

- Exchange models and run predictions
- Opaque models
  - not divulging any unnecessary informatio
- Attest the identity and the integrity of other domains
- Recursively discovers additional providers



Federation



Concept

Modelling and prediction capabilities of a CDT should focus on **the evolution of cyber-attacks and the risk that potential threats materialize** in the **current or an hypothetical context** in which the system operates.

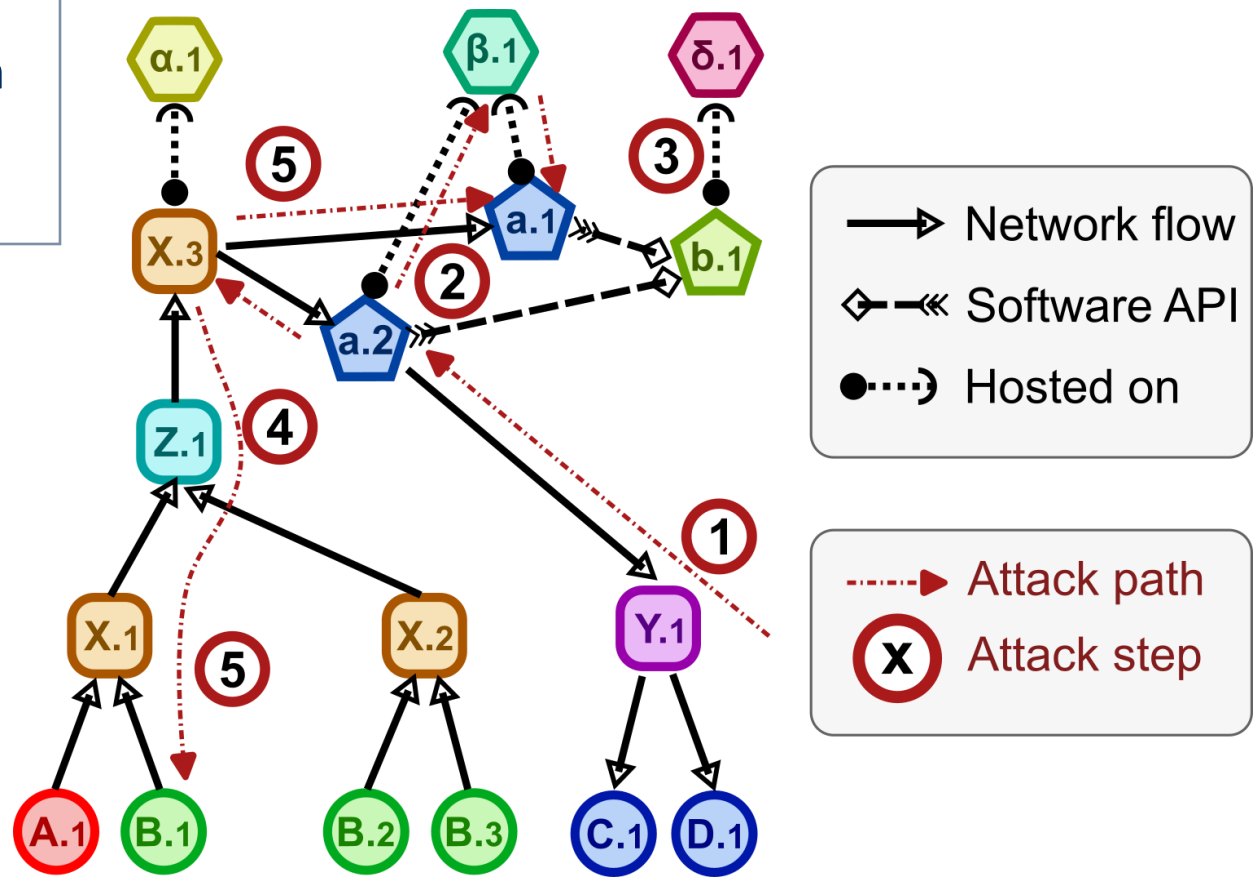
The CDT will be composed of two main layers:

a) Context abstraction

- technical and functional properties
- business and operational relationships

b) Attack modelling

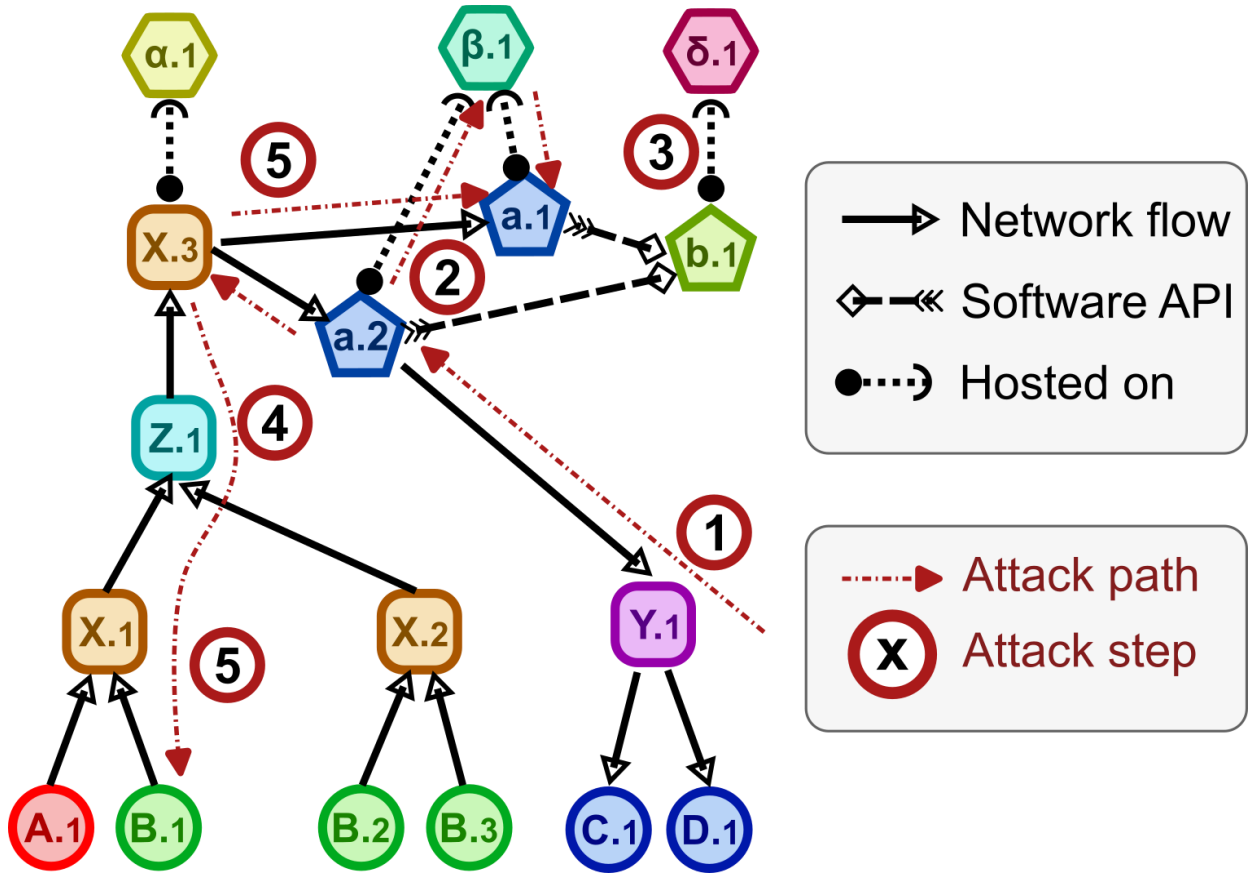
- analytical representations for
- prediction and emulation of attacks.



Context abstraction

Service Context Graphs (SCGs)

- **identity and ownership** of digital services
- the **execution environment** of each service
  - OS, libraries, configurations, …
- **operational relationships and communication patterns**
  - network flows, hosting, APIs, …
- known **cyber-vulnerabilities and threats,**
- **Cyber-Security Functions (CSFs)**
  - capabilities and controls



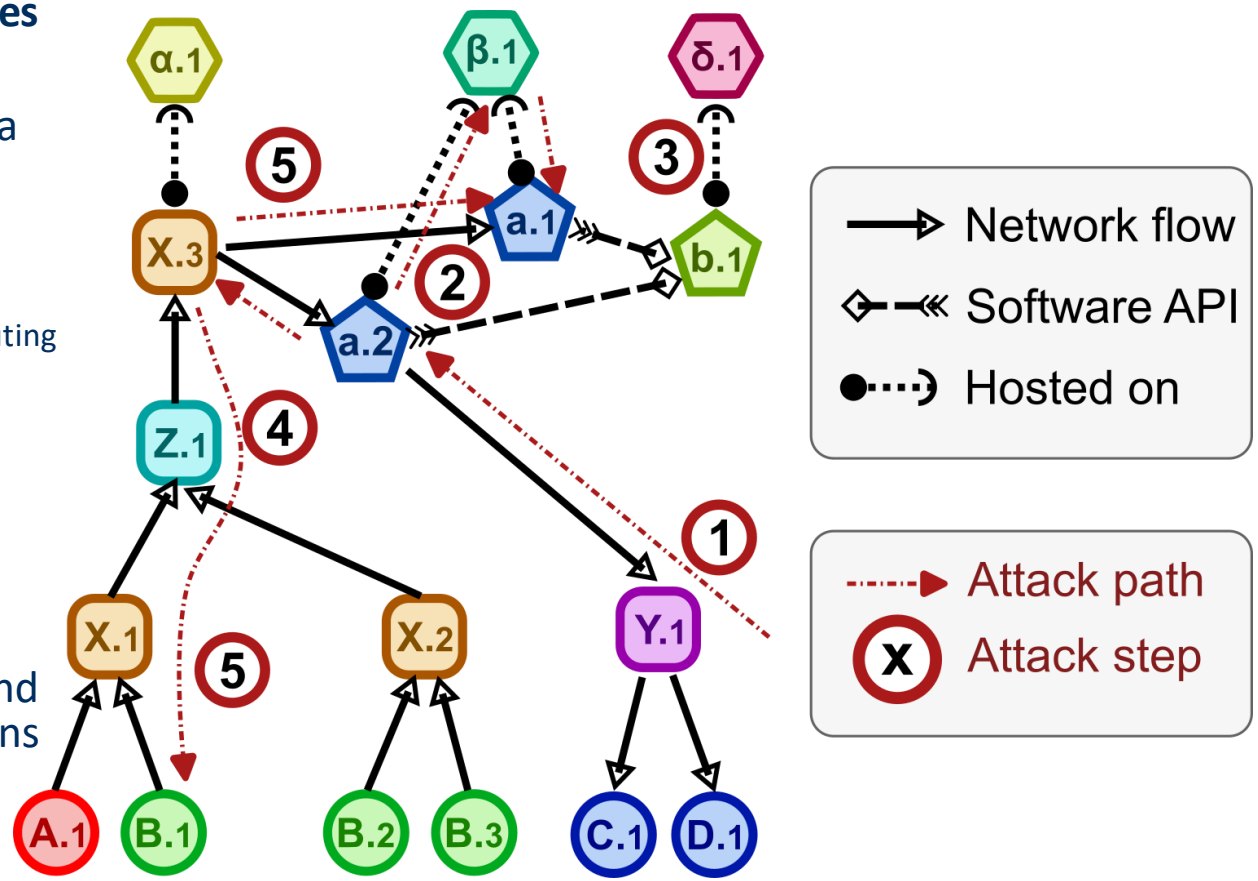
Prediction and Response

Attack modelling

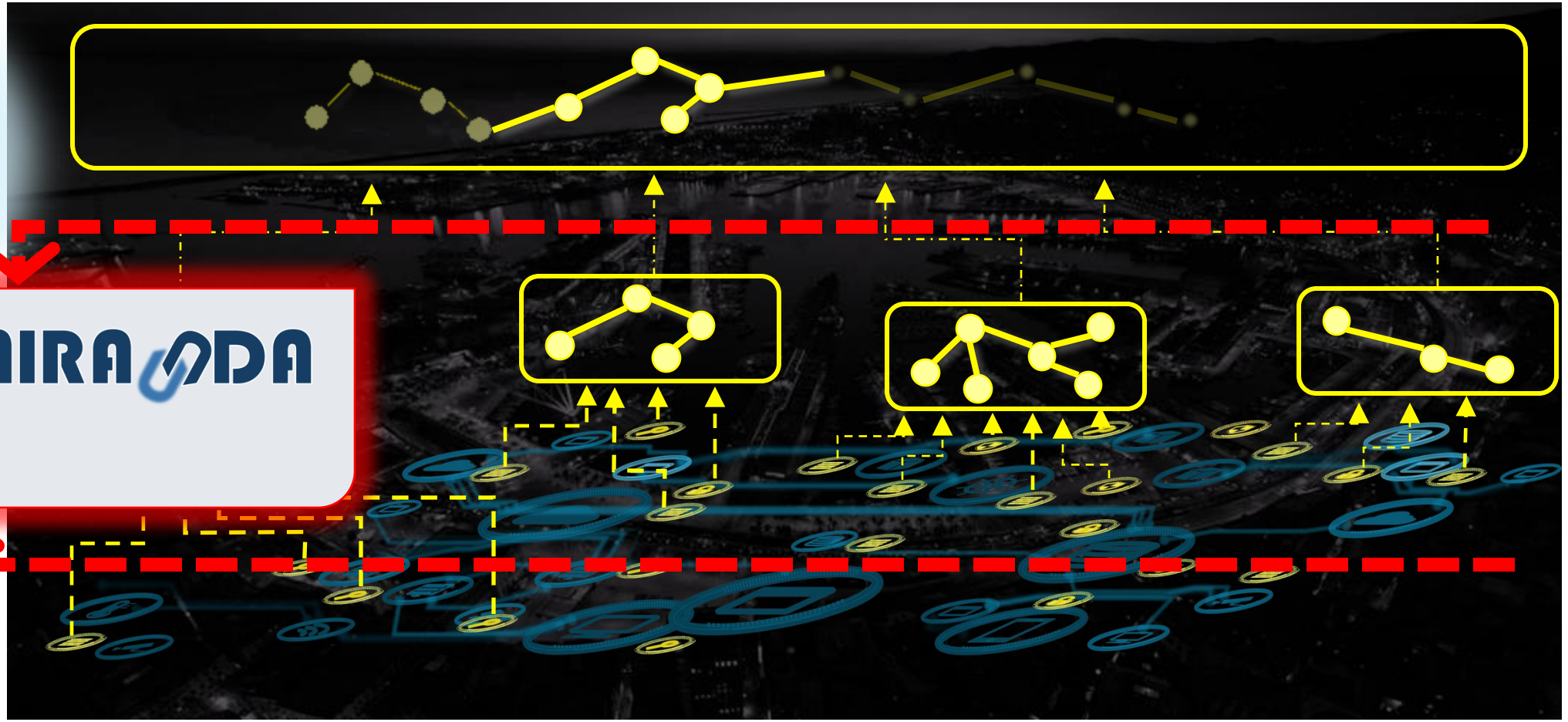
- **logical rules that define how an attacker advances within the service chain**
- enablers to adversarial lateral movement, which a defender is required to eliminate and nullify
- **integration with external models** to improve the overall prediction and correlation capabilities
  - E.g., the distribution of people around the city or commuting patterns, digital models of IoT devices for attestation

Advanced cybersecurity operations

- monitoring, detection, hunting, and response,
- **agile, automatic and adaptive**,
- to recognize on-going multi-step attacks, predict potential attack paths, identify the final target, and to tailor detection and mitigation/response actions to the current configurations



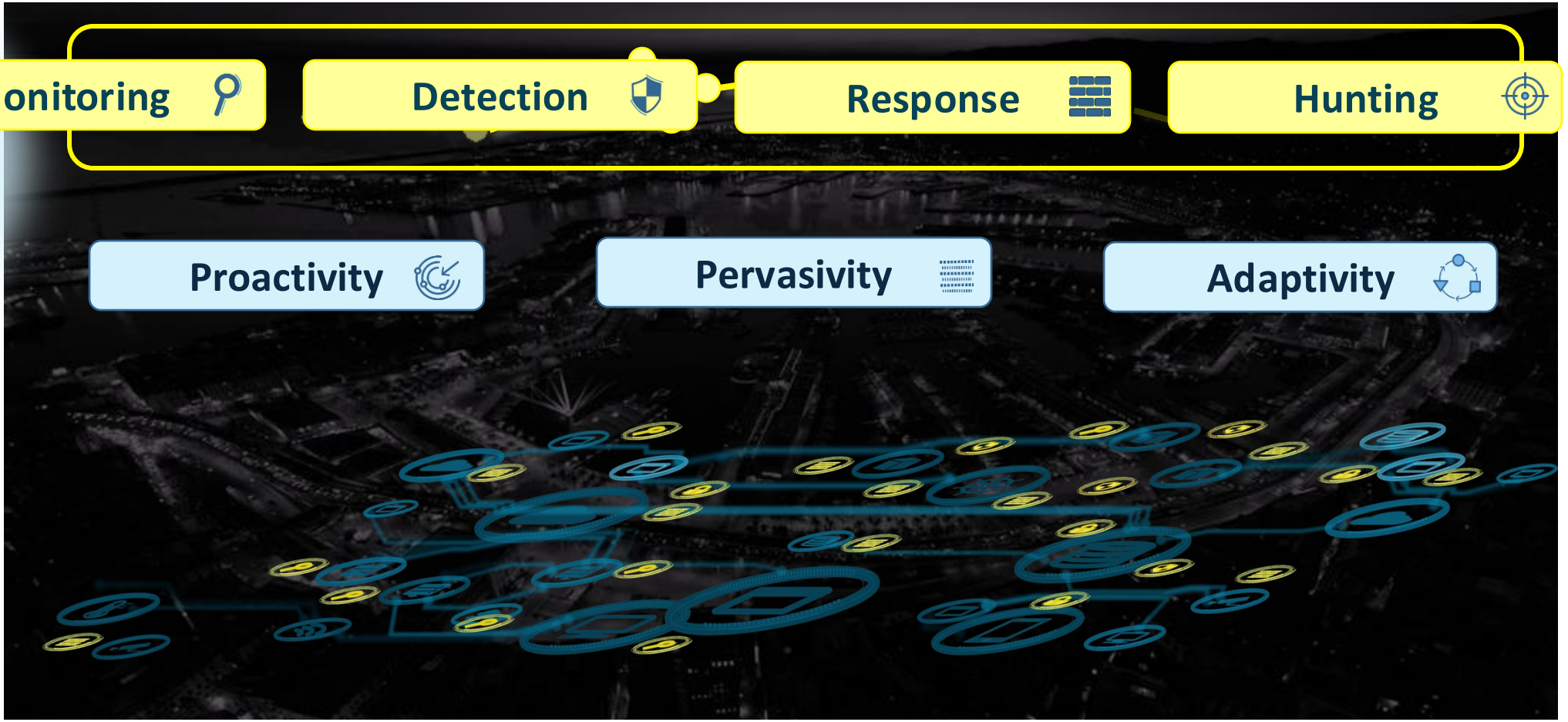
Cross-domain security API



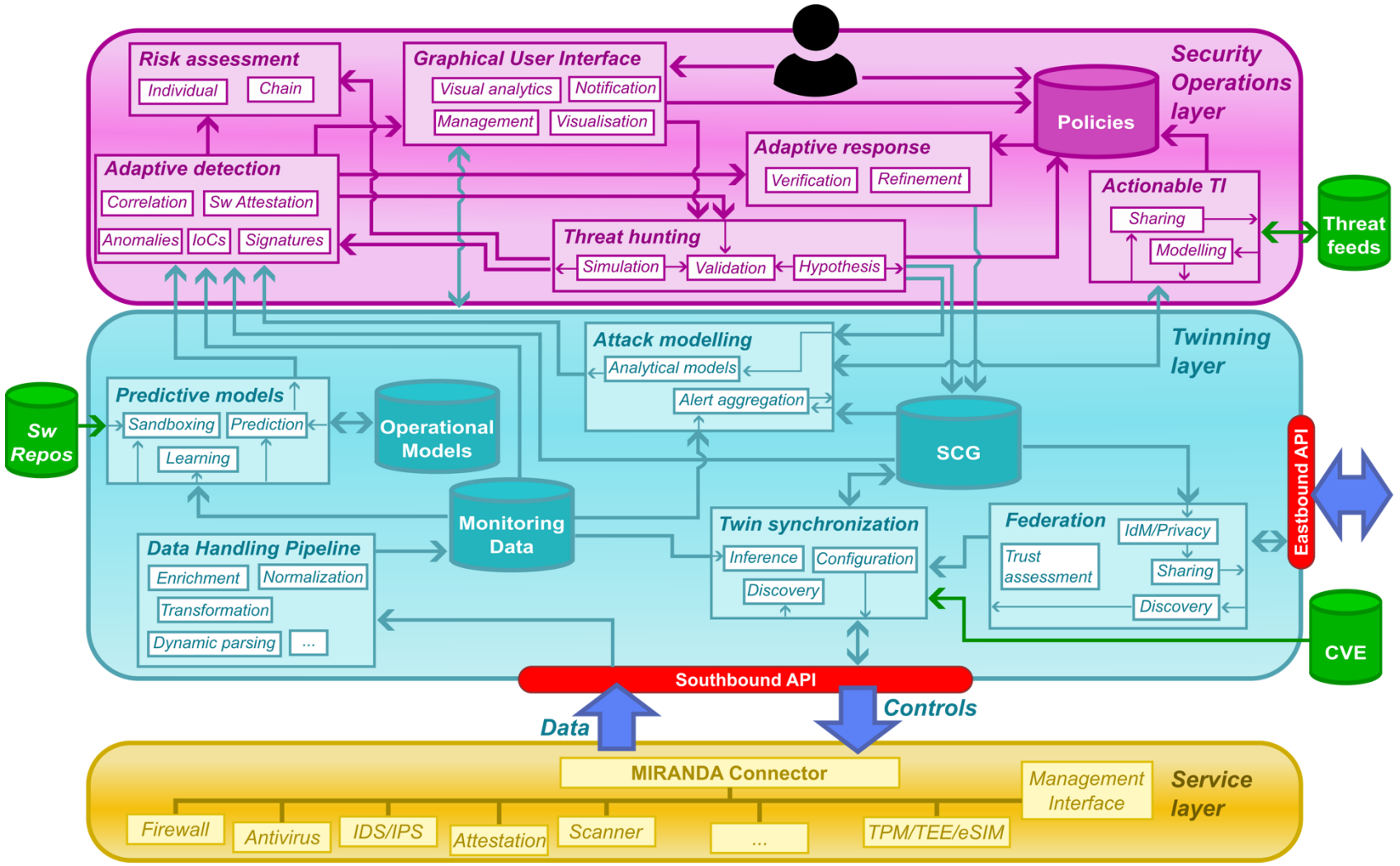
Security API
- REST-full
- Open
- Extensible
- Cross-platform
- Multi-ownership

MIRANDA

Improving cyber-security operations



The MIRANDA Architecture



A step behind: CPS

- Heterogeneous technological value chains
  - Information Technology (IT)
  - Operational Technology (OT)
  - Industrial equipment
- Tight physical/cyber interdependencies
- **Security of the whole system is not the plain sum of security of each chain**
  - Failures and breaches propagates across them
  - Cascading effects (e.g., energy systems)

Security issues in technological value chains

- Resilience of single components is not enough
  - the **cyber-space offers virtually unlimited attack paths**
  - they can be exploited in parallel to make hardware redundancy ineffective
  - **systematic and coordinated attacks** likely lead to power outage and/or significant damages
- The Reactive approach is largely ineffective
  - zero-day attacks
  - Advanced Persistent Threats
  - (stegomalware, cover channels)
  - collection of IoC delays the detection (when physical damage might also be happened)

The need for *Proactive* cyber-security

- Anticipation of attack path and impact
  - prioritize risks,
  - nullify or at least mitigate threats,
  - elaborate response strategies

  well in advance!
- => Continuous and seamless operation of physical systems
- **Reactive operation should remain as last-resort only**

- Don’t forget multi-ownership!

Proactive and *collaborative* posture

i. **identifies interdependencies**
   - across technology and business value chains;

ii. **anticipates attacks**
   - detect threats in the very early stages of the cyber kill chain;

iii. **predicts cascading effects**
   - on interconnected value chains

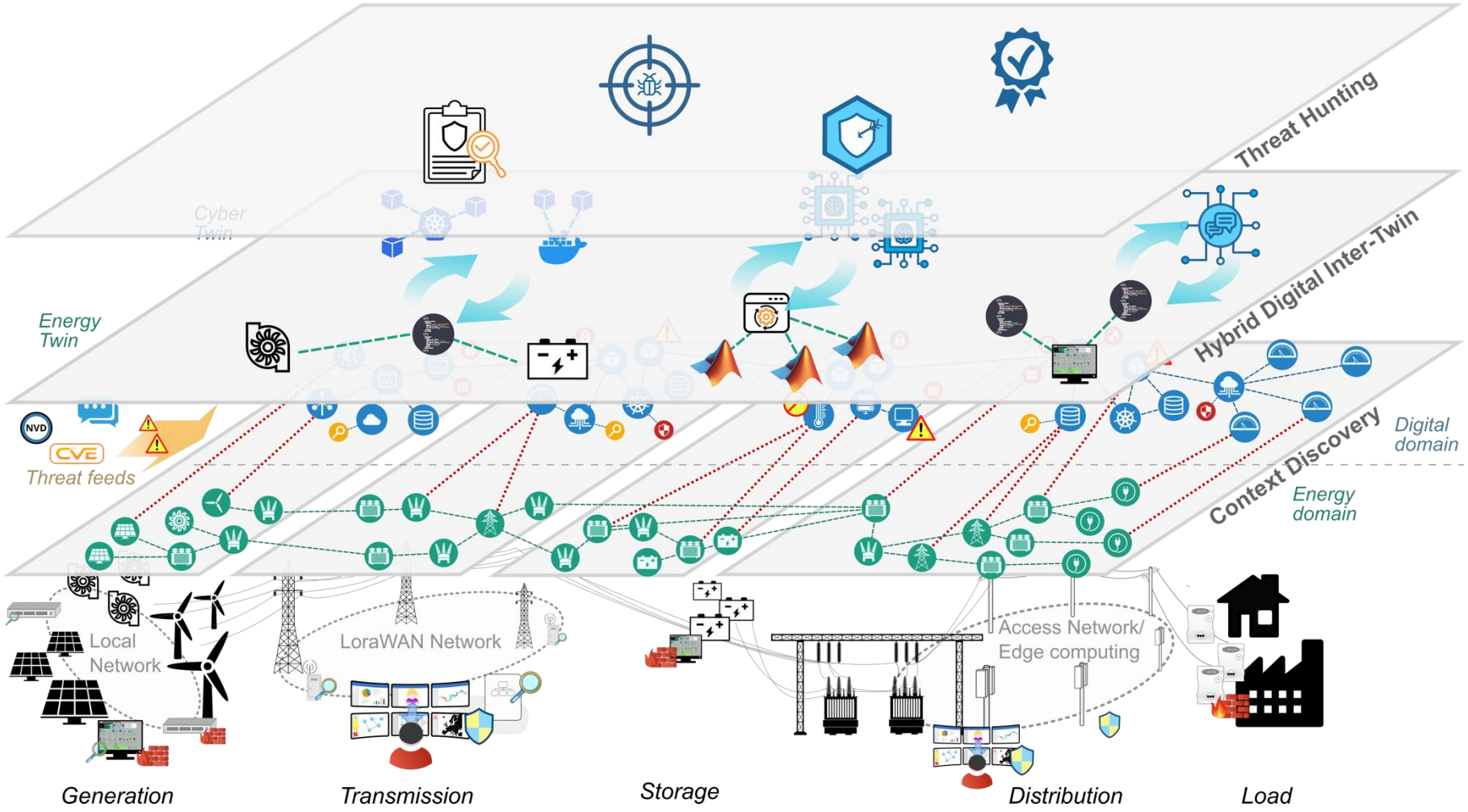
Challenges

- **Visibility across domains**
  - reluctance to share information
- **Abstraction and modelling of resources and their interactions**
  - in multiple domains
  - continuously fed by real-time data
- **Make predictions under various scenarios**
  - agnostic of specific communication protocols and market models.

Inter-Twinning

- Combination **domain-specific Digital Twins**
- **Capture manifest (and also hidden) interdependencies**
- Make hypothesis and test them under different conditions
- Explore as many threat scenarios as possible before they materialize in practice

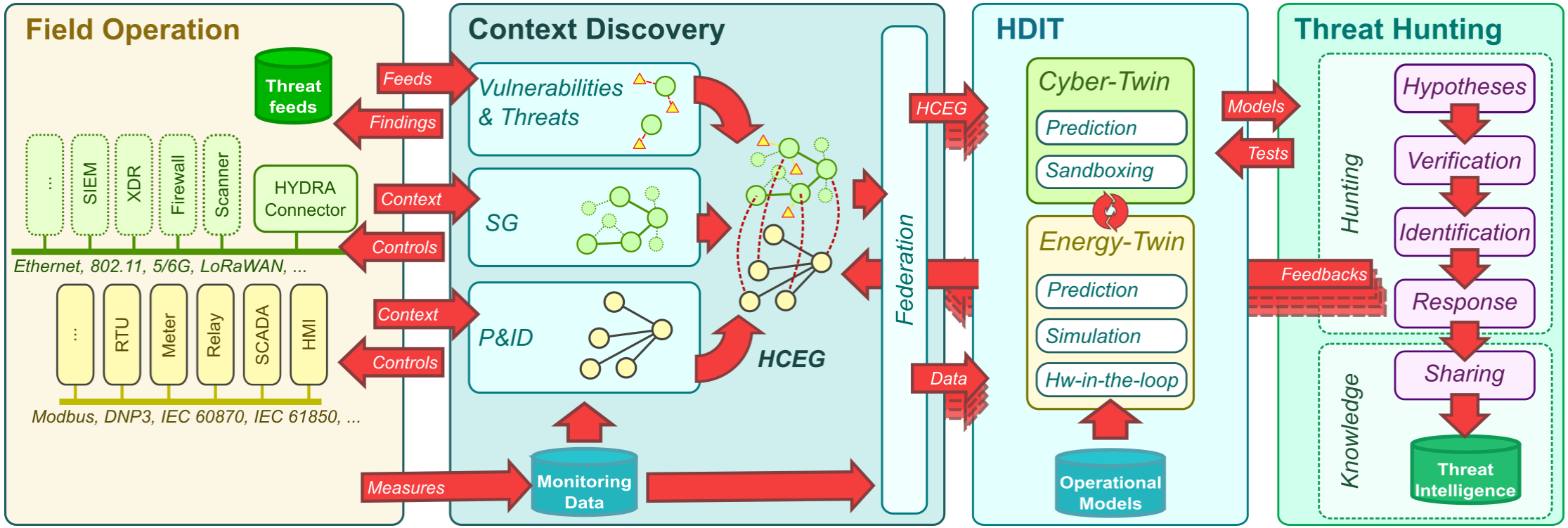
Inter-Twinning concept



Inter-Twinning layers

1. ***Context Discovery*** (individual providers)
   - **abstractions** of physical and cyber resources, operational and security properties, and relationships
     - including **dependencies between different technology value chains**
   - **adaptive level of granularity and aggregation**
     - allows to “blur” or “opacify” the abstraction based on trust concerns.
2. ***Hybrid Digital Inter-Twin (HDIT)*** for the whole chain
   - **combines Cyber and Energy Twins** (including HW/SW-in-the-loop emulation)
     - feeds them with context and data from individual providers
   - **identification of mutual relationships**
     - e.g., data communication patterns under different operating conditions of grid elements and subsystem,
     - operational states and energy flows in response to commands sent over data networks
   - **improve visibility and understand cascading effects** across the whole value chain
3. ***Threat Hunting*** over the whole system
   - leverages the rich set of modelling and emulation capabilities of the HDIT
   - **carries out proactive investigations**
     i. penetration testing and dynamic/runtime application security testing (DAST/RAST)
     ii. compliance verification,
     iii. identification of existing threats
     iv. anticipation of new attack paths
     v. detection of stealthy attacks and advanced persistent threats.

The HYDRA architecture



Layers

- Field operation
  - Collects data and measure and applies controls in a homogeneous way
  - Electrical protocols: IEC 61850, IEC 61970, IEC 60870
  - IT/OT protocols: OpenC2
- Context Discovery
  - abstraction of physical and cyber-properties (SCADA, AMI, RTU, OpenStack, Kubernetes
  - inventory of known vulnerabilities and threats (CVE, OWASP, MITRE ATT&CK)
  - discovery of intra- and inter-domain relationships (SSDP, WS-DD, MUD, IEC 61850 MMS)
  - federation with other domains while preserving privacy and confidentiality
- Hybrid Digital Inter-Twin (HDIT)
  - Energy Twin: steady and dynamic energy/power flows, DER and EM optimization
  - Cyber Twin: logs and network flows, attack strategies, protocol operation
  - Modes: data-driven (ML/FL/TL), simulation (Simulink, OpenPLC4, ScadaBR, modRSsim2, EasyModbusTCP), emulation (sandboxing, HiL)
- Threat hunting
  - hunts for new threats and shares findings (as TTPs, IoCs)
  - 4 steps process: 1) automatic hypothesis generation; 2) verification through the HDIT; 3) discovery of new patterns and TTPs; 4) elaboration of response and mitigation strategies

Take-aways

- IoT are just **one (weakest) link** of big chains
  - look the forest behind the trees!
- IoT security is **no more (only) a matter** of device **hw/sw** vulnerabilities
  - the *impact* on other components/chains really makes the different
- Digital Twins for cyber-security are still a **largely unexplored field**
  - concept, usage, purposes
- **Proactive is better** than reactive, yet more **challenging**
  - physical systems are severely affected by cyber-attacks (safety)
  - physical damages and disruption are more difficult to recover
  - **anticipating** human creativity is challenging… will it be easier or more difficult for artificial intelligence?

MIRANDA Project Factsheet

Coordinator

Consiglio Nazionale delle Ricerche

- Duration: 1/9/2024-31/8/2027
- Budget: 7 308 925.00 €
- Use Cases: Wolfsburg, Genoa, Athens

Partners

SPACE
ONESOURCE
security Stelar tech law research
Logstail
Politecnico di Torino
NASK
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Sphynx Technology Solutions
Plaixus
UBITECH ubiquitous solutions
WOBCOM
MINDICITY
DAEM

Contacts

- **Project coordinator**

Matteo Repetto

Institute for Applied Mathematics and Information Technologies (IMATI), CNR

Genoa, Italy

matteo.repetto@cnr.it

info@mirandaproject.eu

www.mirandaproject.eu

https://www.linkedin.com/company/105119663

@mirandaprj

@MIRANDA-Project