Enhancing cybersecurity using Digital Twin and AI

How to conceive DT for cybersecurity and predict attacks?

Hugo BOURREAU
hugo.bourreau@cyberCNI.fr

CYBER CNI.FR

security research

speaker series

PhD schools

MOOCs

Why Digital Twin?

The concept “Digital Twin” is a **hybrid** of multiple previously existing **technologies**.

Fig 1: Roots of Digital Twin

Why Digital Twin?

Digital Twins target enhancing their **capacity** to …

Realism | Insights | Prediction

Fig 2: Advantages of Digital Twin

Context

Who Am I?

ISEN Nantes
Engineering degree

UQAC
Double degree, master in computer science

Interested in research

First conference paper in 2022

On Securing the Communication in IoT Infrastructure using Elliptic Curve Cryptography

PhD settings

PhD Started in
June 2024

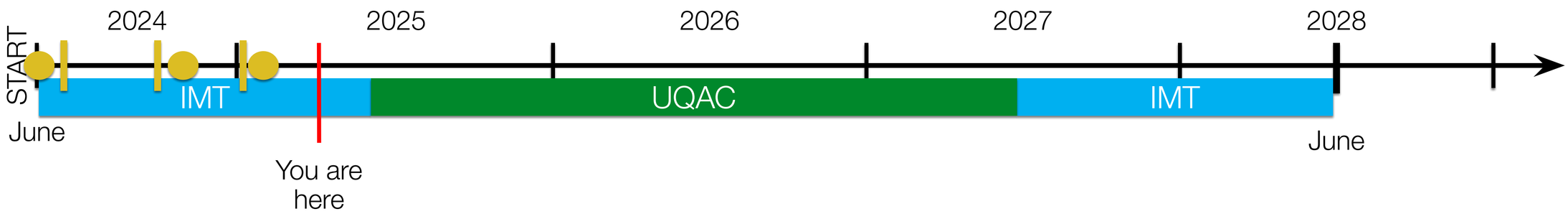
Cotutelle
France - Canada

Industrial Partners
EDF - Airbus

UQAC IMT

in-person meeting

online meeting



Supervisors

Software safety and security

Fabien DAGNAT
IMT Atlantique

IoT and cybersecurity

Fehmi JAAFAR
UQAC
Chaire CybPro

Autonomous management of IoT cybersecurity

Marc-Oliver PAHL
IMT Atlantique
Chaire Cyber CNI

4

Definition

Digital Twin definition

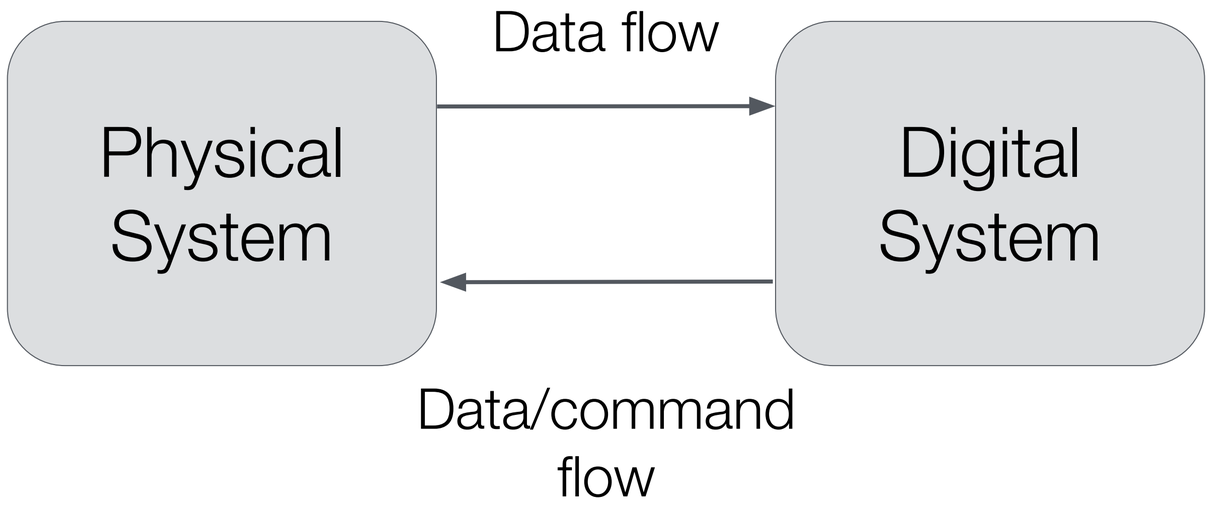
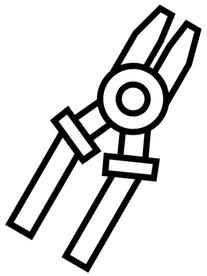


Fig 3: Digital Twin core principle

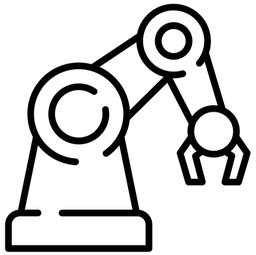
Digital Twin definition

Digital Twin scale

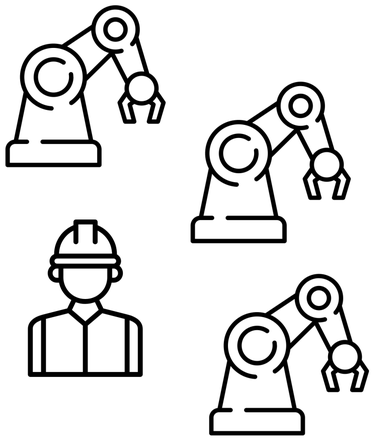
Component twin



Asset twin



System twin



Process twin

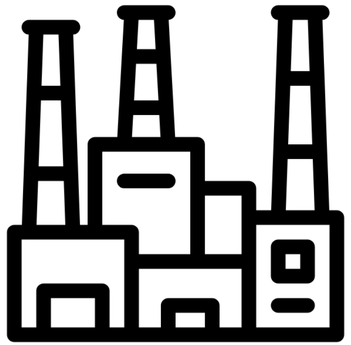


Fig 4: Digital Twin scale

Digital Twin definition

Digital Twin temporal stage

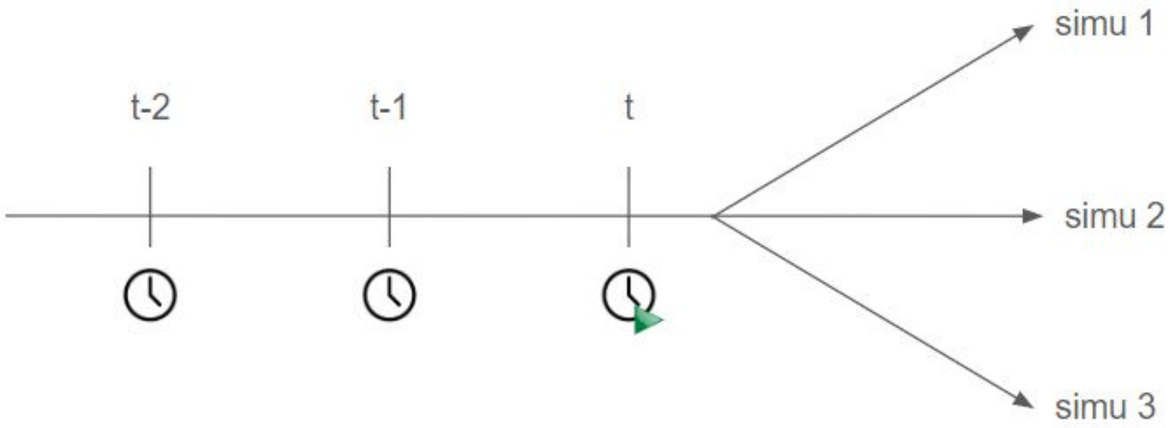


Fig 5: States of a Digital Twin

4

Main issue

Why Digital Twin for cybersecurity?

Digital Twin starts to be famous since 2018 but
cybersecurity is rarely employed with it

Why Digital Twin for cybersecurity?

Research questions

RQ1 Why researchers and practitioners using DTs rather than other cybersecurity solutions?

RQ2 What makes a DT different for cybersecurity than other areas?

RQ3 What are the current research areas concerning DTs?

RQ4 How is the impact of DTs on cybersecurity measured?

Why Digital Twin for cybersecurity?

Research questions - With AI

RQ* How can artificial intelligence be integrated with digital twins to predict and detect security threats?

RQ* What types of AI models are most effective for detecting anomalies in a digital twin?

4

Litterature

SLR Methodology

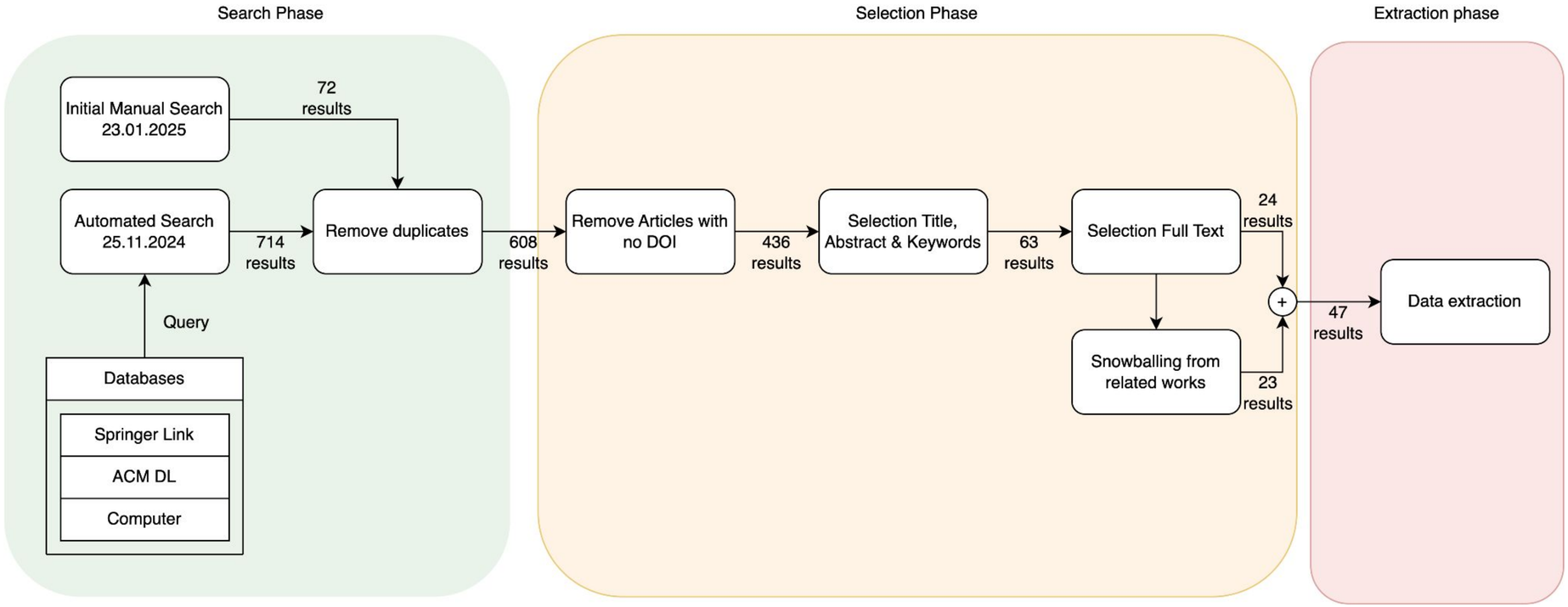


Fig 6: SLR Methodology

SLR Methodology

Python script to parse literature
Publicly accessible on GitHub[1]

1: https://github.com/SkYiMlTo/dt4sec_survey_slr

Reference architecture

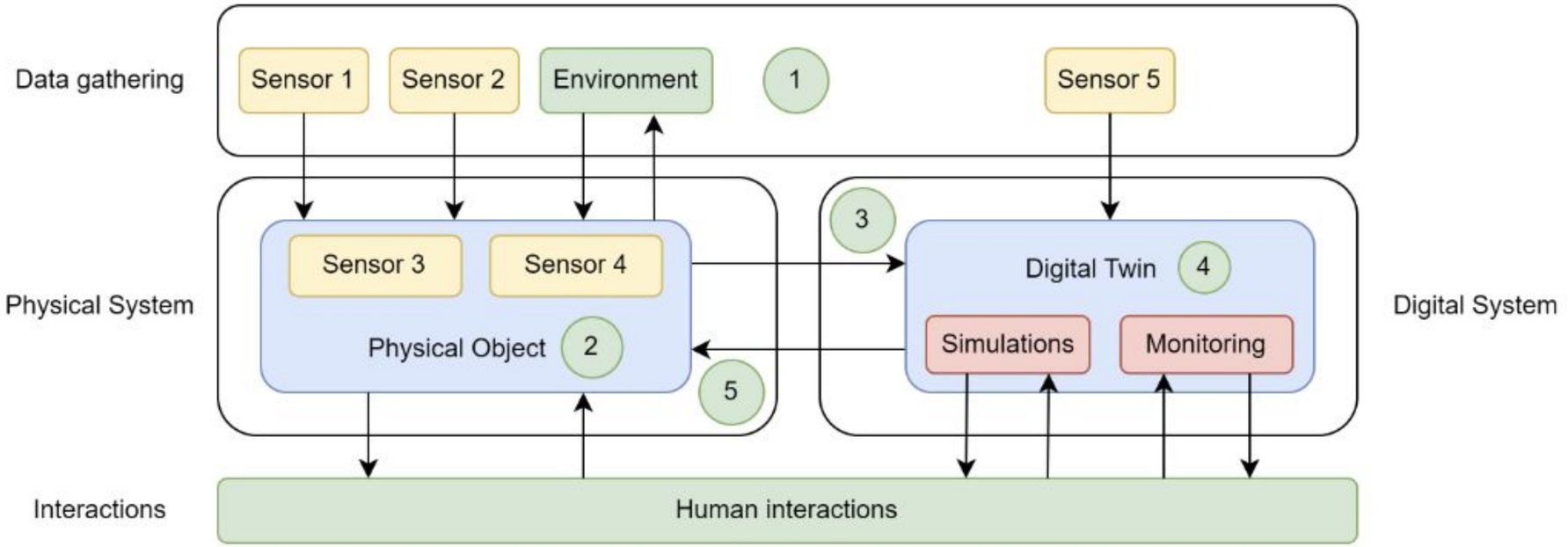


Fig 7: Reference architecture

Other surveys

TABLE I
EXISTING SURVEYS ABOUT DIGITAL TWIN

Authors	Reference	Publication year	Scope	Case studies	Tooling	DT sectors and areas	SLR methodology	Highlight the literature gaps	Cybersecurity aspects
Kritzinger et al.	[7]	2018	2010 - 2017	✓	-	-	✓	-	-
Enders et al.	[15]	2019	2012 - 2019	-	-	✓	-	-	-
Eckhart et al.	[16]	2019	2009 - 2018	✓	-	✓	-	✓	✓
Jones et al.	[17]	2020	2009 - 2018	-	-	✓	✓	✓	-
Semeraro et al.	[18]	2021	2007 - 2020	-	✓	✓	✓	-	-
Liu et al.	[19]	2021	2010 - 2019	✓	-	-	✓	-	-
Singh et al.	[20]	2022	2015 - 2022	✓	✓	✓	✓	-	-
Shi et al.	[21]	2022	2010 - 2022	✓	✓	✓	-	-	✓
Wen et al.	[22]	2022	1998 - 2022	✓	-	✓	-	✓	✓
Somers et al.	[23]	2023	2012 - 2023	✓	✓	✓	✓	-	-
Nguyen et al.	[24]	2023	2015 - 2023	✓	✓	✓	✓	✓	-
Wang et al.	[25]	2023	2019 - 2023	✓	-	✓	-	-	✓
Alhamam et al.	[26]	2025	2016 - 2024	✓	-	✓	✓	-	✓
Bourreau et al.	Our survey	2025	2015 - 2025	✓	✓	✓	✓	✓	✓

Fig 8: Other surveys about Digital Twin

Other surveys

TABLE I
EXISTING SURVEYS ABOUT DIGITAL TWIN

Authors	Reference	Publication year	Scope	Case studies	Tooling	DT sectors and areas	SLR methodology	Highlight the literature gaps	Cybersecurity aspects
Kritzinger et al.	[7]	2018	2010 - 2017	✓	-	-	✓	-	-
Enders et al.	[15]	2019	2012 - 2019	-	-	✓	-	-	-
Eckhart et al.	[16]	2019	2009 - 2018	✓	-	✓	-	✓	✓
Jones et al.	[17]	2020	2009 - 2018	-	-	✓	✓	✓	-
Semeraro et al.	[18]	2021	2007 - 2020	-	✓	✓	✓	-	-
Liu et al.	[19]	2021	2010 - 2019	✓	-	-	✓	-	-
Singh et al.	[20]	2022	2015 - 2022	✓	✓	✓	✓	-	-
Shi et al.	[21]	2022	2010 - 2022	✓	✓	✓	-	-	✓
Wen et al.	[22]	2022	1998 - 2022	✓	-	✓	-	✓	✓
Somers et al.	[23]	2023	2012 - 2023	✓	✓	✓	✓	-	-
Nguyen et al.	[24]	2023	2015 - 2023	✓	✓	✓	✓	✓	-
Wang et al.	[25]	2023	2019 - 2023	✓	-	✓	-	-	✓
Alhamam et al.	[26]	2025	2016 - 2024	✓	-	✓	✓	-	✓
Bourreau et al.	Our survey	2025	2015 - 2025	✓	✓	✓	✓	✓	✓

Fig 9: Other surveys about Digital Twin

Other surveys

TABLE I
EXISTING SURVEYS ABOUT DIGITAL TWIN

Authors	Reference	Publication year	Scope	Case studies	Tooling	DT sectors and areas	SLR methodology	Highlight the literature gaps	Cybersecurity aspects
Kritzinger et al.	[7]	2018	2010 - 2017	✓	-	-	✓	-	-
Enders et al.	[15]	2019	2012 - 2019	-	-	✓	-	-	-
Eckhart et al.	[16]	2019	2009 - 2018	✓	-	✓	-	✓	✓
Jones et al.	[17]	2020	2009 - 2018	-	-	✓	✓	✓	-
Semeraro et al.	[18]	2021	2007 - 2020	-	✓	✓	✓	-	-
Liu et al.	[19]	2021	2010 - 2019	✓	-	-	✓	-	-
Singh et al.	[20]	2022	2015 - 2022	✓	✓	✓	✓	-	-
Shi et al.	[21]	2022	2010 - 2022	✓	✓	✓	-	-	✓
Wen et al.	[22]	2022	1998 - 2022	✓	-	✓	-	✓	✓
Somers et al.	[23]	2023	2012 - 2023	✓	✓	✓	✓	-	-
Nguyen et al.	[24]	2023	2015 - 2023	✓	✓	✓	✓	✓	-
Wang et al.	[25]	2023	2019 - 2023	✓	-	✓	-	-	✓
Alhamam et al.	[26]	2025	2016 - 2024	✓	-	✓	✓	-	✓
Bourreau et al.	Our survey	2025	2015 - 2025	✓	✓	✓	✓	✓	✓

RQ2

Fig 10: Other surveys about Digital Twin

Other surveys

TABLE IV
OVERVIEW OF TOOLS AND TECHNIQUES RELATED TO DIGITAL TWINS FOR CYBERSECURITY

Category	Tool / Technique	Reference
Digital Twin Products	Azure Digital Twin, Siemens Digital Twin, Greycat	[65]
Digital Twin Frameworks	Eclipse Ditto (open-source DT framework)	[66]
Intrusion Detection Tools	IDS integrated into DTs, Cyber Situational Awareness Framework for real-time monitoring	[56], [64]
Machine Learning Methods	LSTM, BiLSTM, Attention-BiLSTM, Logistic Regression (LR), SHAP, STL (Signal Temporal Logic)	[56], [66], [67]
Privacy Techniques	Differential Privacy Frequent Subgraph (DPFS)	[67]
Simulation Environments	Tennessee Eastman (TE) Process, Mininet-WiFi (UAV network simulation)	[67], [68]
Network Tools	Mininet-WiFi, Open Network Operating System (ONOS) for SDN	[68]
Testing Tools	SimComponents (SimPy-based network performance testing)	[68]

RQ2

Fig 11: Existing tools for DT

Implementations classification

Ref	Year	Sector / Domain	Type of Work	DT Scope	Cybersecurity Focus	Methodology / Techniques	AI/ML/DL Used	Attack Simulation	Uses Real Testbed	Real Attacks or Datasets
[47]	2023	Smart grid/lab	Case study, HIL platform	Smart grid DT: power + comm.	Countermeasure verification/-validation	HIL simulation/-grid lab	Not stated	Yes	Yes	Yes
[48]	2020	ICS	Framework/case study	DT security simulation	Security simulation, MITM attack, SIEM	SOC workflow, simulated MITM	No	Yes	No	Yes
[49]	2023	Smart grid	Survey/review	Not specified	DTs for grid cyber resilience	Architecture review	No	No	No	No
[50]	2020	Water distribution (CPS)	Co-simulation platform	Plant, control, and network layers	Attack emulation/experimentation	DHALSIM: WNTR+MiniCPS	Not stated	Yes	No	Yes
[51]	2020	ICS	Primary research	Virtual replica of ICS	Intrusion detection/-classification	Novel IDS algorithm in DT	No	Yes	No	Yes
[52]	2023	V2G-CPS	Framework, case study	V2G-CPS DT; actor-critic RL	CCA (coordinated attack) detection/mitigation	LSTM-based DRL, case studies	Yes	Yes	No	Yes
[53]	2020	Microgrid/energy	Primary research	IoT, networked microgrids DT	Resilience (DoS, FDI mitigation)	IoT cloud, physical controller integration	Not stated	Yes	Yes	Yes
[54]	2023	Industry 4.0, general CPS	Survey/review	Not specified	DTs for APT detection/-coverage, dataset generation	Conceptual survey	No	No	No	No
[55]	2023	I4.0; CNC manufacturing	Framework, empirical	DT via models, CNC process	Attack detection, anomaly detection	DT prediction, EWMA	Not stated	No	No	No
[56]	2020	Multi-sector; generic	Review/SLR	Not specified	Usability for incident prediction	Systematic literature review	No	No	No	No

TABLE III
SYNTHESIS OF DT IMPLEMENTATIONS

RQ3

Fig 12: Classification DT implementation for CPS

Implementations classification

Ref	Year	Sector / Domain	Type of Work	DT Scope	Cybersecurity Focus	Methodology / Techniques	AI/ML/DL Used	Attack Simulation	Uses Real Testbed	Real Attacks or Datasets
[47]	2023	Smart grid/lab	Case study, HIL platform	Smart grid DT: power + comm.	Countermeasure verification/-validation	HIL simulation/-grid lab	Not stated	Yes	Yes	Yes
[48]	2020	ICS	Framework/case study	DT security simulation	Security simulation, MITM attack, SIEM	SOC workflow, simulated MITM	No	Yes	No	Yes
[49]	2023	Smart grid	Survey/review	Not specified	DTs for grid cyber resilience	Architecture review	No	No	No	No
[50]	2020	Water distribution (CPS)	Co-simulation platform	Plant, control, and network layers	Attack emulation/experimentation	DHALSIM: WNTR+MiniCPS	Not stated	Yes	No	Yes
[51]	2020	ICS	Primary research	Virtual replica of ICS	Intrusion detection/-classification	Novel IDS algorithm in DT	No	Yes	No	Yes
[52]	2023	V2G-CPS	Framework, case study	V2G-CPS DT; actor-critic RL	CCA (coordinated attack) detection/mitigation	LSTM-based DRL, case studies	Yes	Yes	No	Yes
[53]	2020	Microgrid/energy	Primary research	IoT, networked microgrids DT	Resilience (DoS, FDI mitigation)	IoT cloud, physical controller integration	Not stated	Yes	Yes	Yes
[54]	2023	Industry 4.0, general CPS	Survey/review	Not specified	DTs for APT detection/-coverage, dataset generation	Conceptual survey	No	No	No	No
[55]	2023	I4.0; CNC manufacturing	Framework, empirical	DT via models, CNC process	Attack detection, anomaly detection	DT prediction, EWMA	Not stated	No	No	No
[56]	2020	Multi-sector; generic	Review/SLR	Not specified	Usability for incident prediction	Systematic literature review	No	No	No	No

TABLE III
SYNTHESIS OF DT IMPLEMENTATIONS

Fig 12: Classification DT implementation for CPS

Implementations classification

Table 1
Classification des méthodes de ML et attaques étudiées

Ref	Domain(s)	Paper type	DT Role	AI/ML integration	attack focus
[1]	General	Revue de la literature	Simulation, monitoring, analyse		Prediction (holistic), enhancement of maturity
[2]	General	Revue de la literature	Optimisation, prédiction	Discusses AI/ML but no unique technique implemented	Incident prediction (review of SOTA/tools)
[3]	IoT	Méthode, Framework, Expétimentation	Simulation	CNN+RNN hybrid for anomaly/threat detection & prediction	Detection & Prediction (simulates, forecasts, reacts)
[4]	SCADA/Smart Grid	Méthode, Framework	Visualisation, prediction	Hybrid ML (algorithm unspecified): visualizes/predicts effects	Visualization & Prediction of attack consequences
[5]	Smart Infrastructure Networks	Framework, Expérimentation	Monitoring, prediction	Autoencoder (feature learning) + RNN (sequence)	Detection, predictive analysis, anomaly detection
[6]	Smart City (city subsystems)	Framework, Expérimentation	Simulation	CNN-LSTM ML trained on CICIDS2017	Detection, Prediction, Evaluation of attacks
[7]	ICS (Industrial Filling Plant)	Framework, Expérimentation	Simulation, détection	Autoencoders, RNN	Intrusion detection/classification
[8]	IoT	Framework, Expérimentation	Monitoring	AI-driven anomaly detection, predictive analysis	Detection and Proactive (termed predictive) security
[9]	ICS (Water Distribution)	Framework, Expérimentation	Simulation	Hybrid CNN & RNN	Detection of attacks
[10]	Generic CPS (synthetic & physical)	Experimentation	Simulation	PCA, autoencoder, Random Forest, XGBoost	Intrusion detection

Fig 13: Classification of AI and attacks for DT

Table 2
Comparaison des approches intégrant les JN et l'IA pour la détection et la prédiction d'attaques

Ref	Cross-Domain	Evaluated with real attacks	Proactive prediction	Closed-loop DT	Experimentally validated
[1]	Yes	No	No	No	No
[2]	Yes	No	No	No	No
[3]	No	Yes	Yes	Yes	Yes
[4]	No	No	Yes	No	N/A
[5]	No	No	No	Yes	Yes
[6]	No	Yes	Yes	No	Yes
[7]	No	Yes	No	Yes	Yes
[8]	No	No	Yes	Yes	Yes
[9]	No	Yes	No	N/A	Yes
[10]	No	Yes	No	N/A	Yes

RQ*

Fig 14: Comparison of implementations

To continue

Classification Relevant implementations

Architecture Internal functioning of DT

4

Current work

Current work

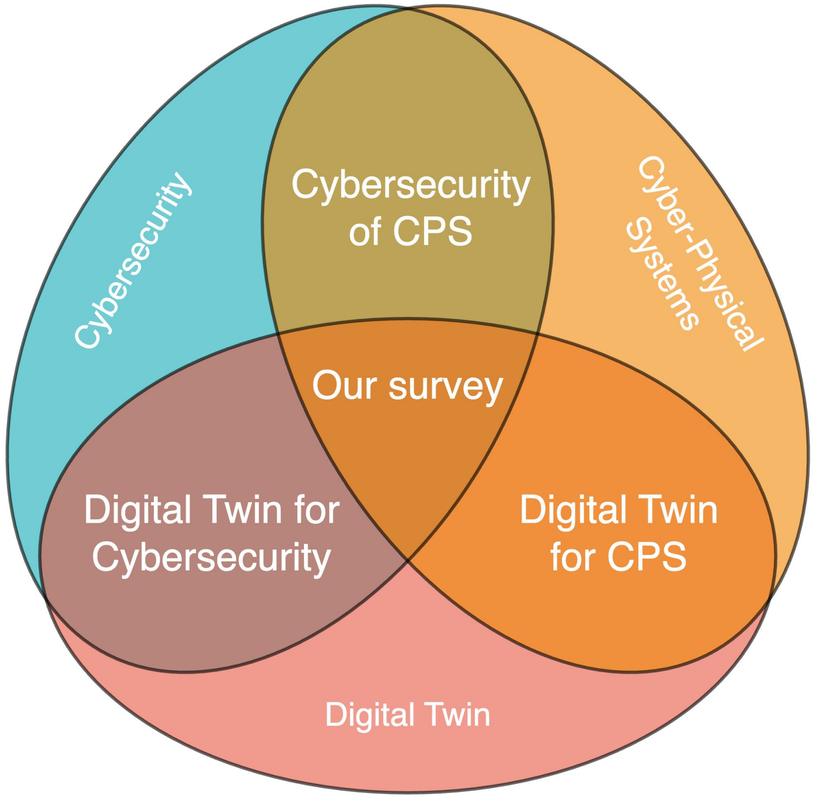
Aspect 1 Conception of Digital Twin

Aspect 2 Process of creation

Aspect 3 Analysis and predictions

Digital Twin conception

IoT



AI

Industry 4.0

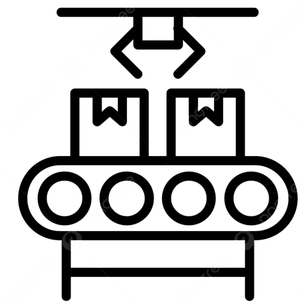
Fig 11: Topics of my research

Current work

Digital Twin for cybersecurity

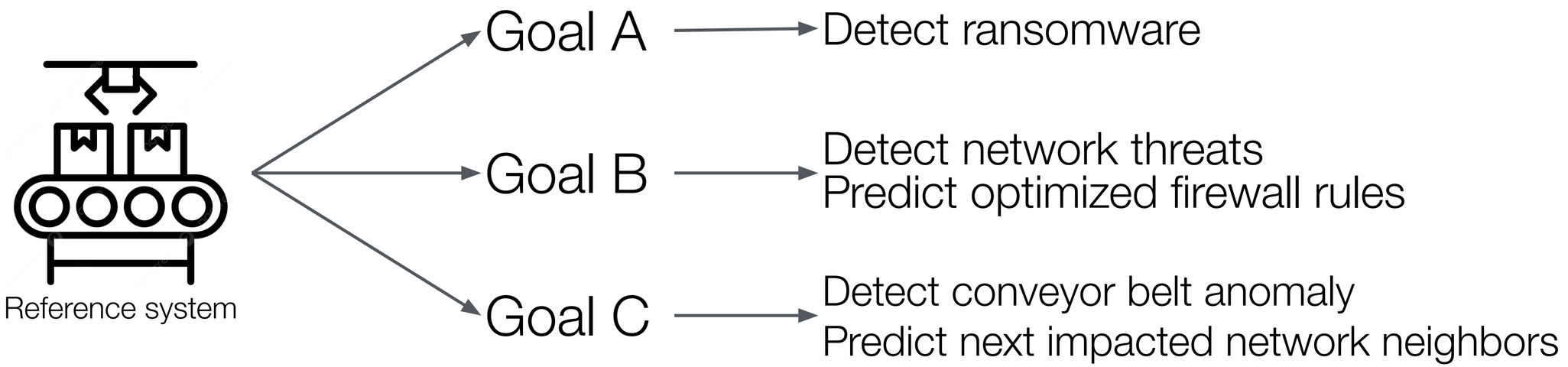
Not cybersecurity of digital twin

Digital Twin conception

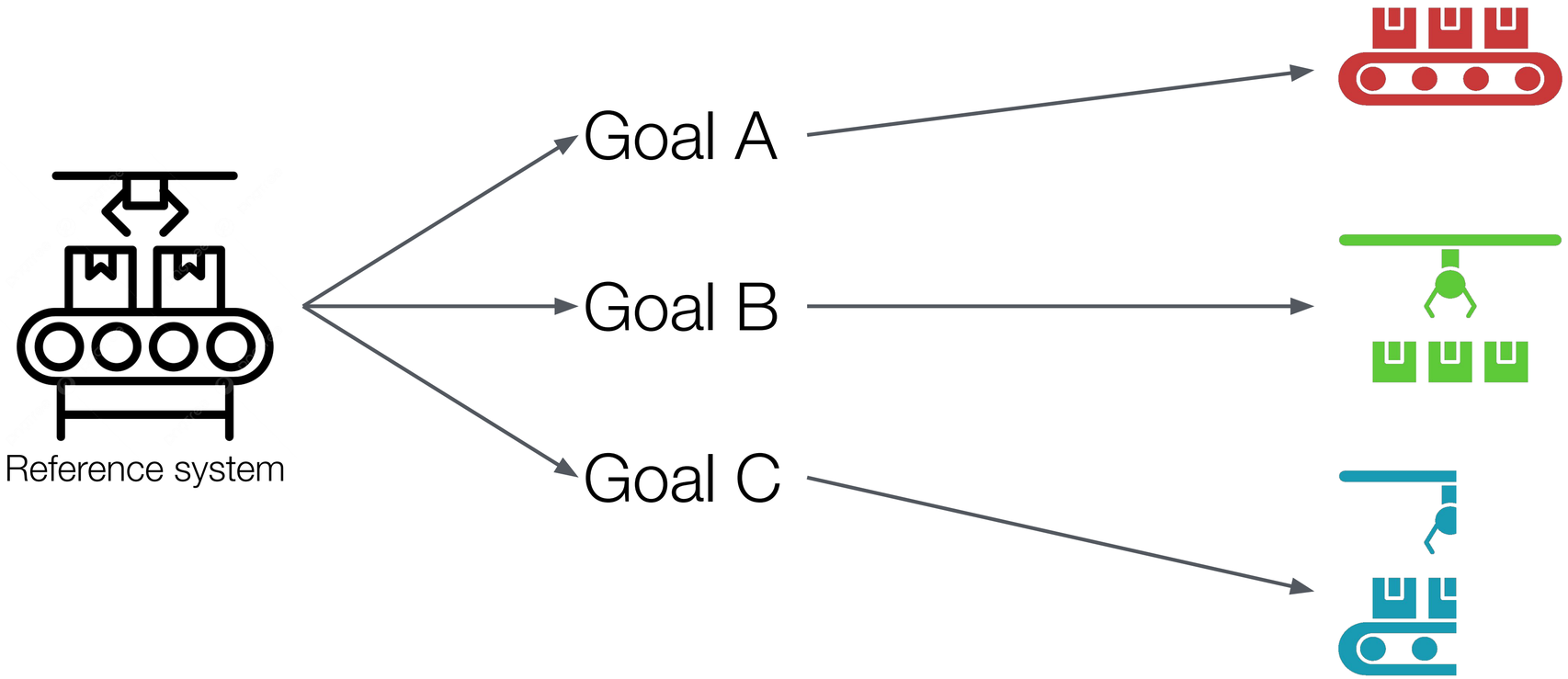


Reference system

Digital Twin conception

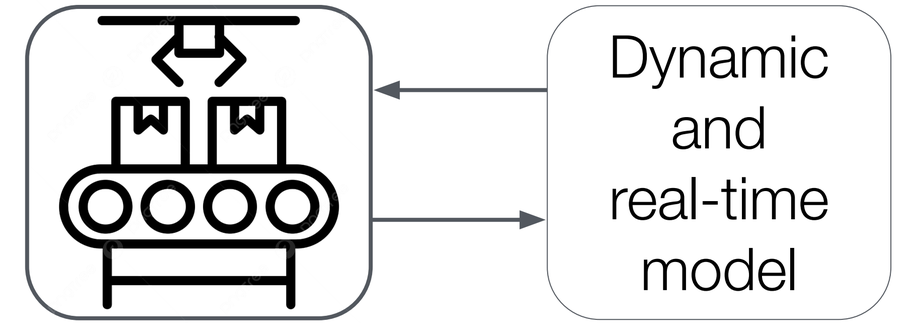


Digital Twin conception



Digital Twin conception

SWAT

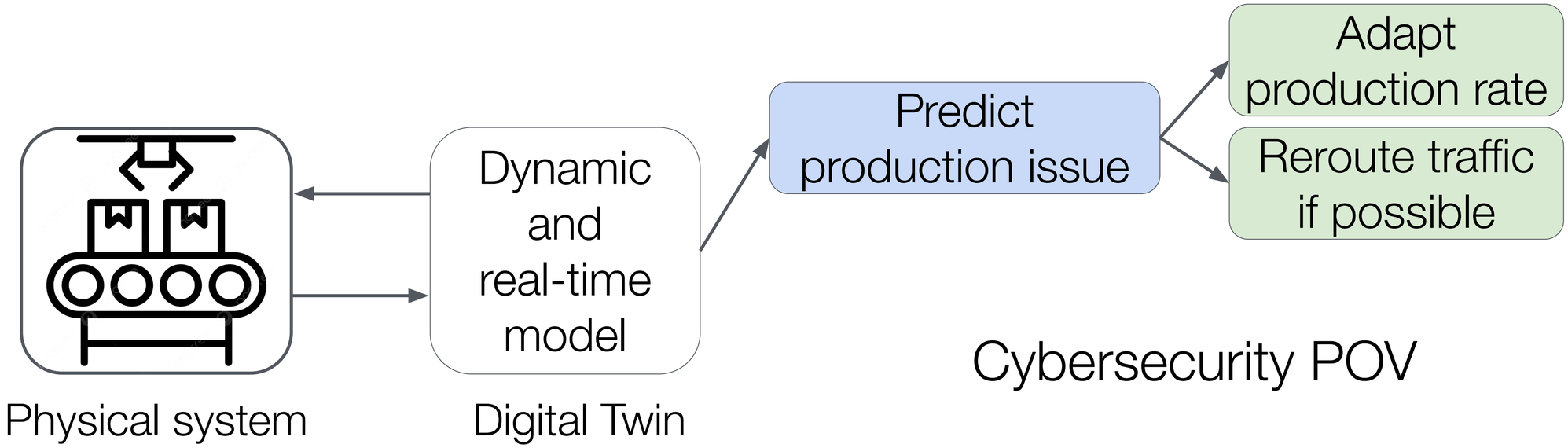


Industrial POV

Cybersecurity POV

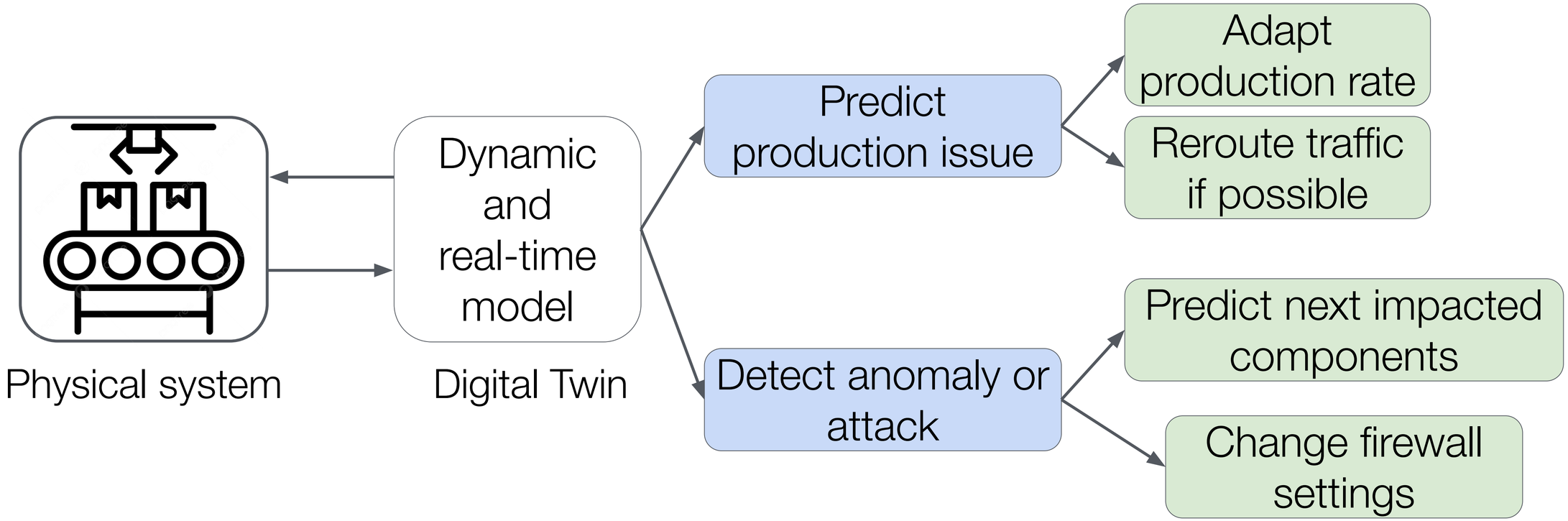
Digital Twin conception

SWAT



Digital Twin conception

SWAT



Digital Twin conception

Feature selection

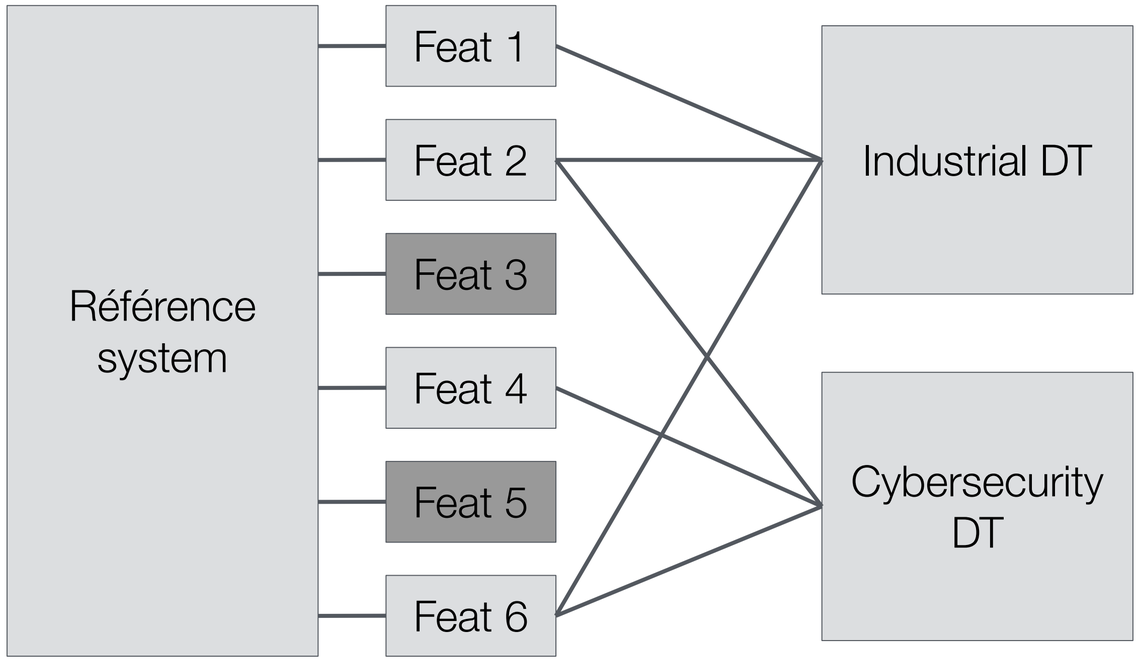
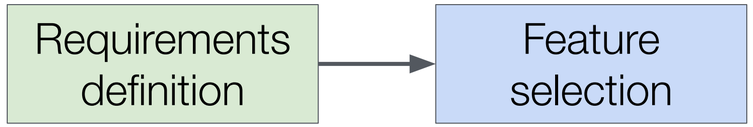
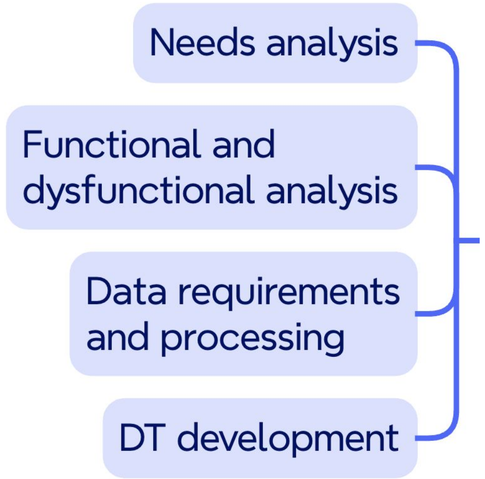


Fig 12: Feature Selection process



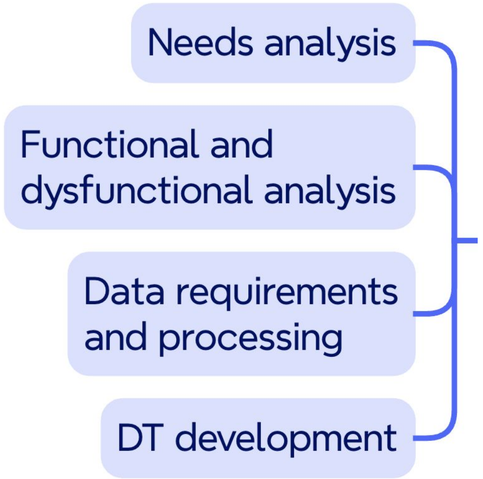
Process of creation



Process of creation

Human world → Implementation independent

Physical world → Implementation specific



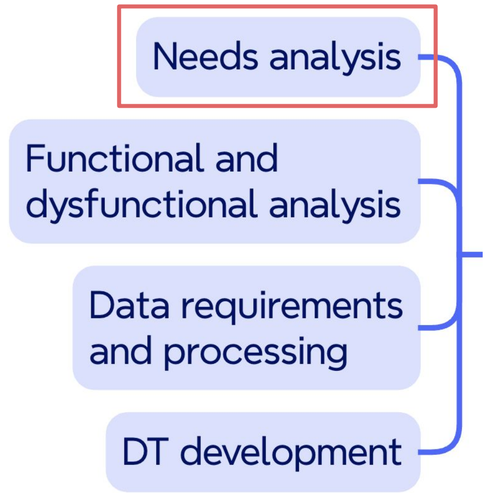
Process of creation

Needs

Identify the relevant use cases
Define the useful features
Define objectives and scenarios

Hardware

Identify the sensors
Security layers
Components we want to modelize
Do we use AI? What is the purpose?



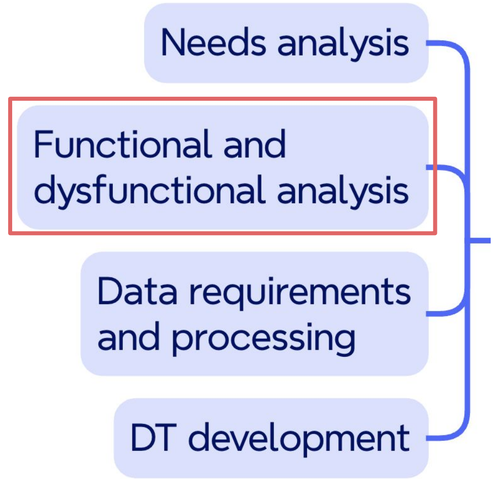
Process of creation

Expected comportments

What is the expected behavior?
structured analysis and design technique (SADT)
Failure Mode, Effects & Criticality Analysis (FMECA)

Connection

Risk assessment on technology used
Durability over time



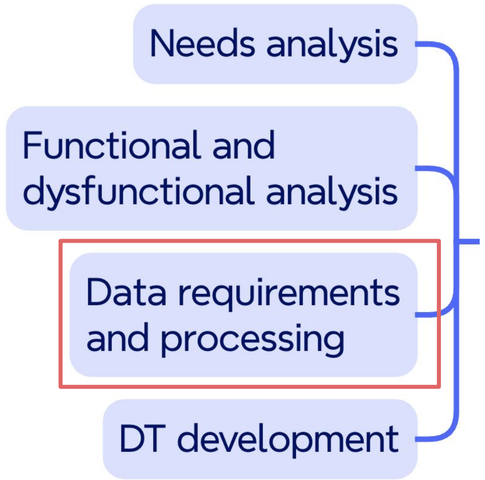
Process of creation

Data conceptualisation

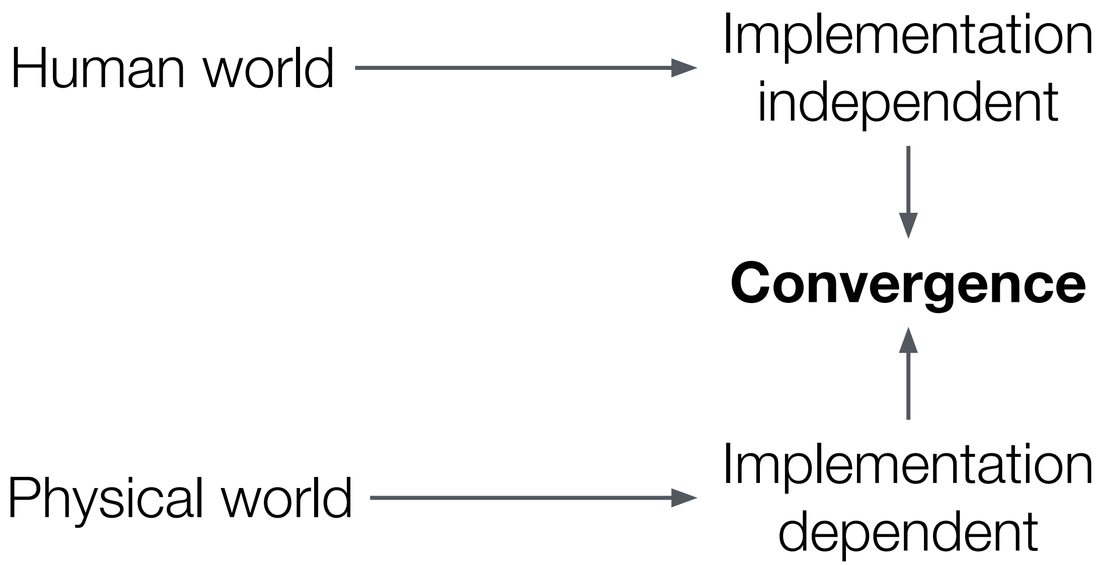
Which data is required
Define data objectives according to use case
Conceptual data flow

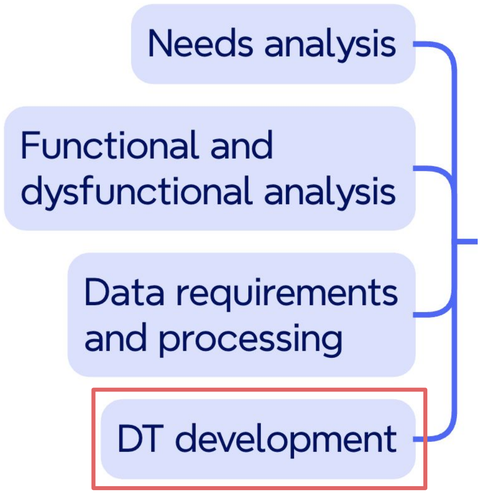
Data processing

Data storage
Data encryption
Data Communication



Process of creation





Process of creation

Maturity

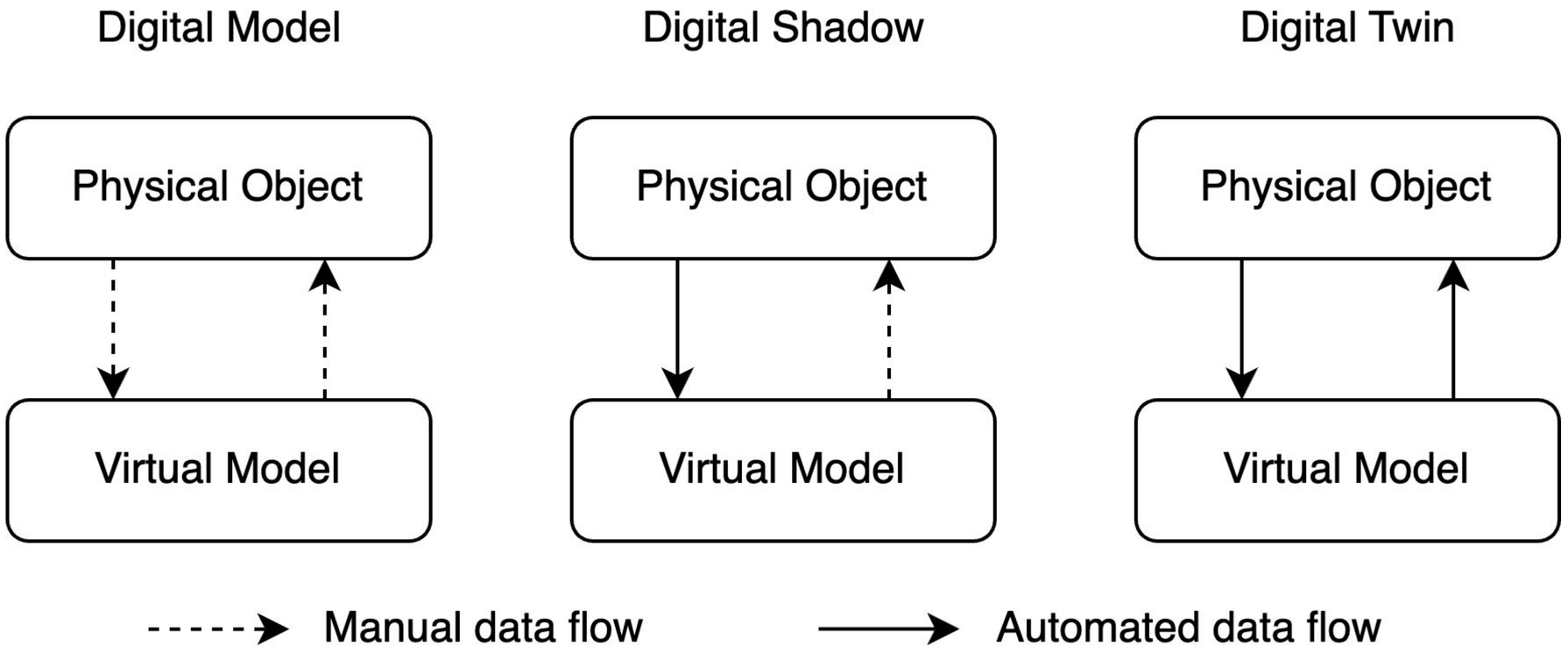


Fig 13: Level of twinning

Prediction aspects

Why Digital Twin predictions?

Prediction aspects

- Scenario simulation
- Risk analysis
- Replay attacks
- Attack impact and limitation
- Early threat detection
- Proactive defense
- Cascading effects

Prediction aspects

- Scenario simulation
- Risk analysis
- Replay attacks
- Attack impact and limitation
- Early threat detection
- Proactive defense
- Cascading effects

Prediction aspects

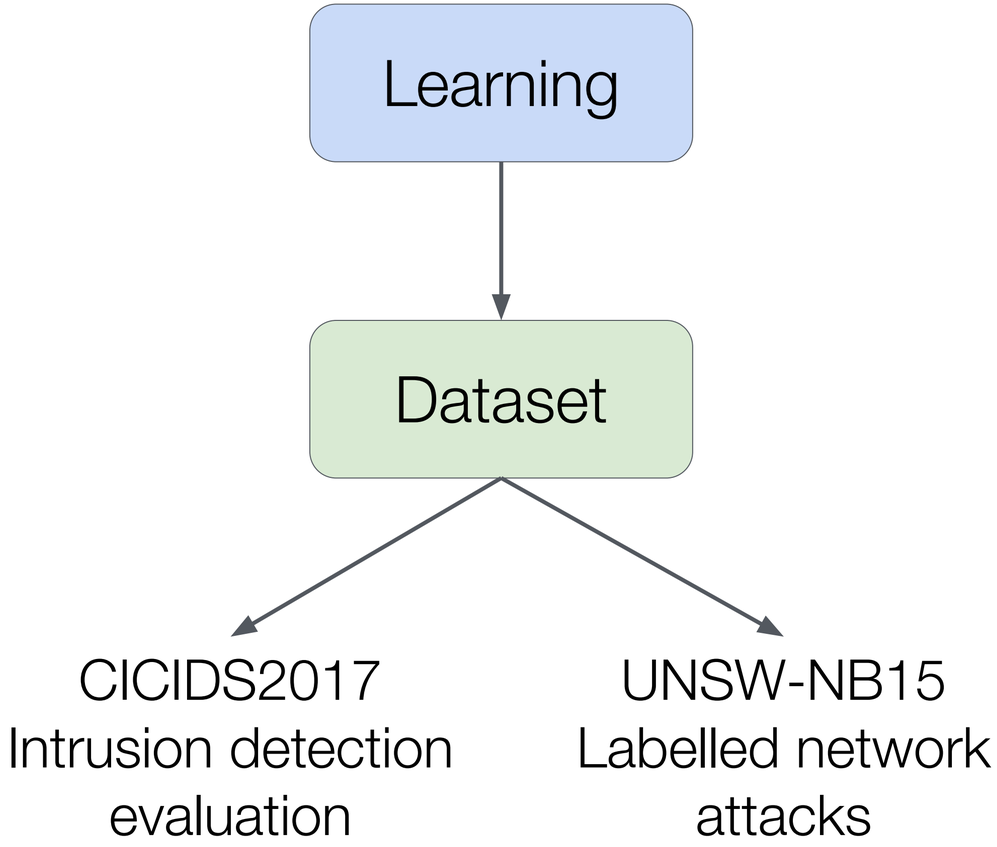
How does Digital Twin predict?

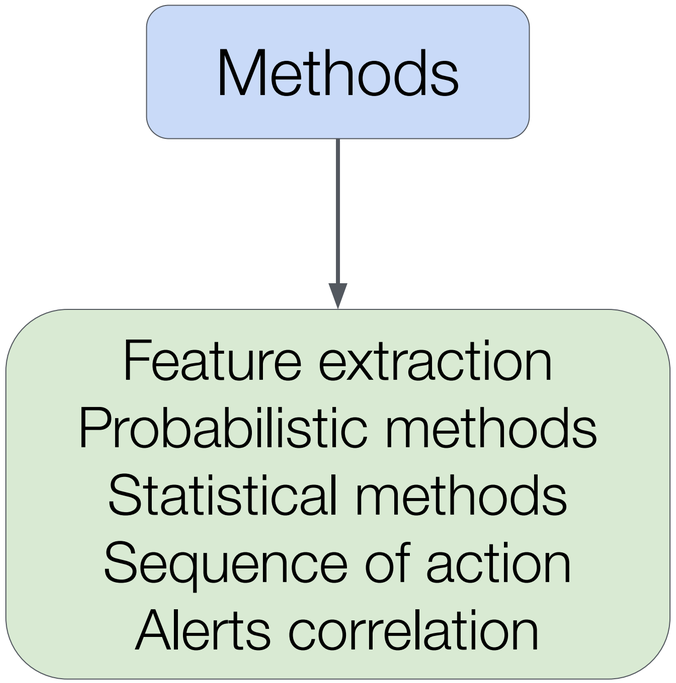
Prediction aspects

Learning

Methods

Prediction aspects





Prediction methods based on [1]

1: J. Luzzi, R. Naha, A. Arulappan and A. Mahanti, "SoK: A Holistic View of Cyberattacks Prediction with Digital Twins," 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 2024, pp. 1-7, doi: 10.1109/ic-ETITE58242.2024.10493514.

4

Results

Results

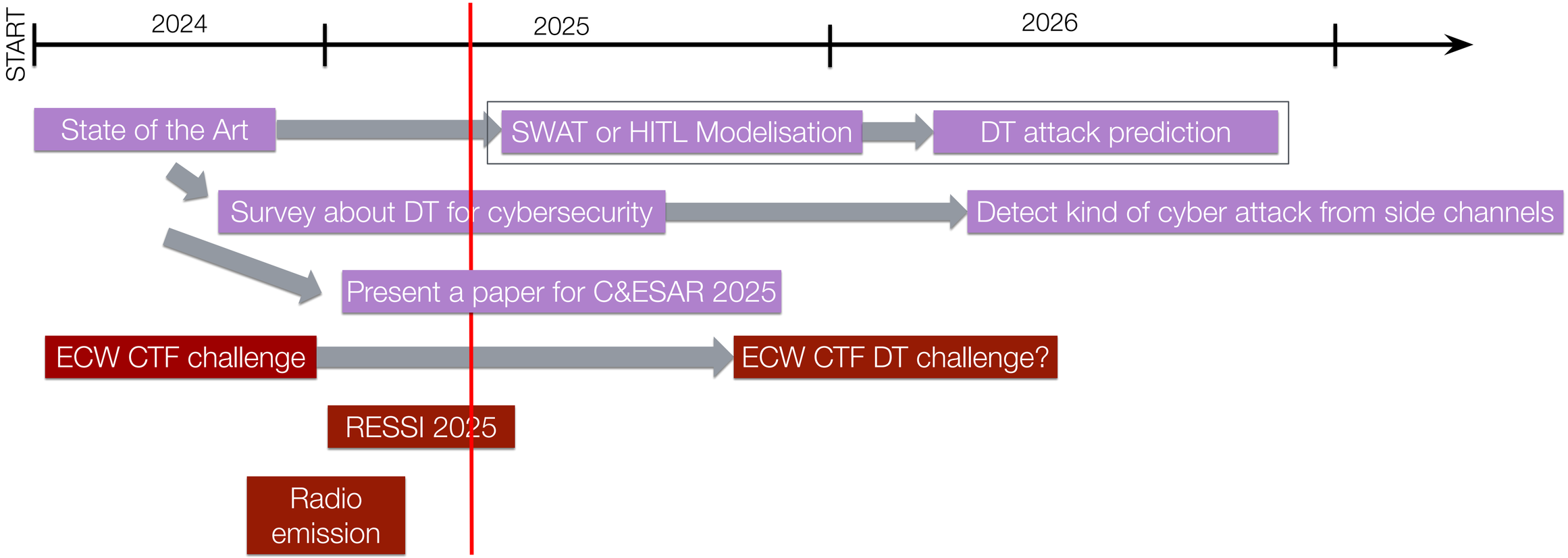
Interesting directions

Direction 1 DT modelization between industry and cybersecurity ?

Direction 2 Prediction aspect of the DT for anomaly detection

Timeline

Timeline


START
2024
2025
2026
State of the Art
SWAT or HITL Modelisation
DT attack prediction
Survey about DT for cybersecurity
Detect kind of cyber attack from side channels
Present a paper for C&ESAR 2025
ECW CTF challenge
ECW CTF DT challenge?
RESSI 2025
Radio emission

Thesis challenges

Goals

Goal 1 Developing a metric for the realism of a DT.

Goal 2 Using DTs for more comprehensive risk analysis.

Goal 3 Using DTs for simulating side-channel measurements for better attack detection.

4

Experimentation with Digital Twin

Experimentation with Digital Twin

Definition

Aim: Consequence prediction

Target: SWAT

Context: Cyber-physical system

Experimentation with Digital Twin

Use cases

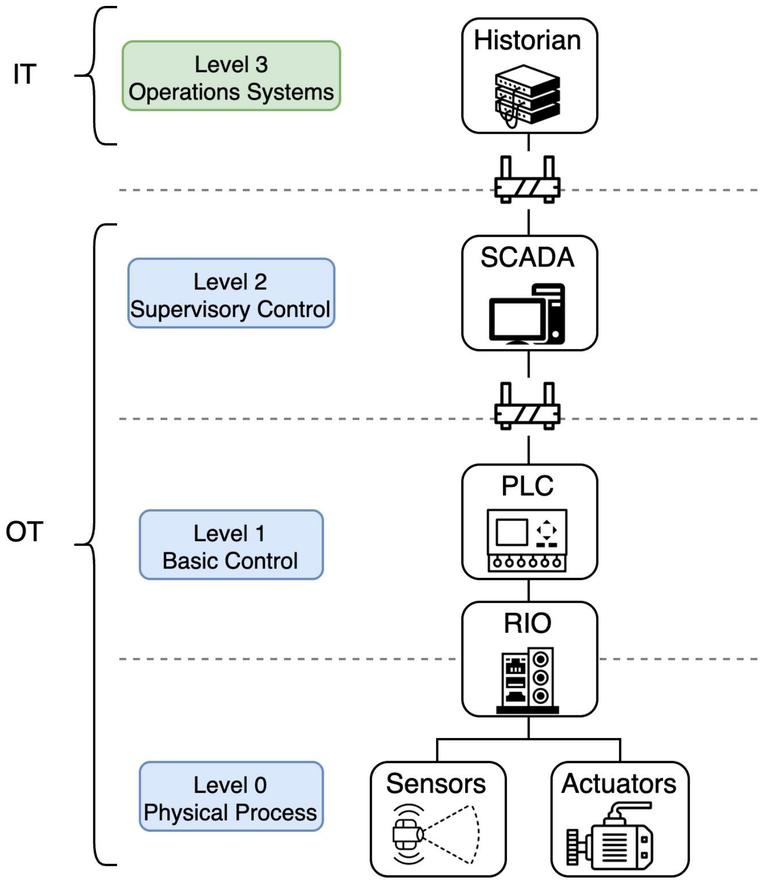


Fig 15: Use cases parameters

Schema based on Singapore University of technology and design presentation[1]

1: https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/

Experimentation with Digital Twin

Use cases

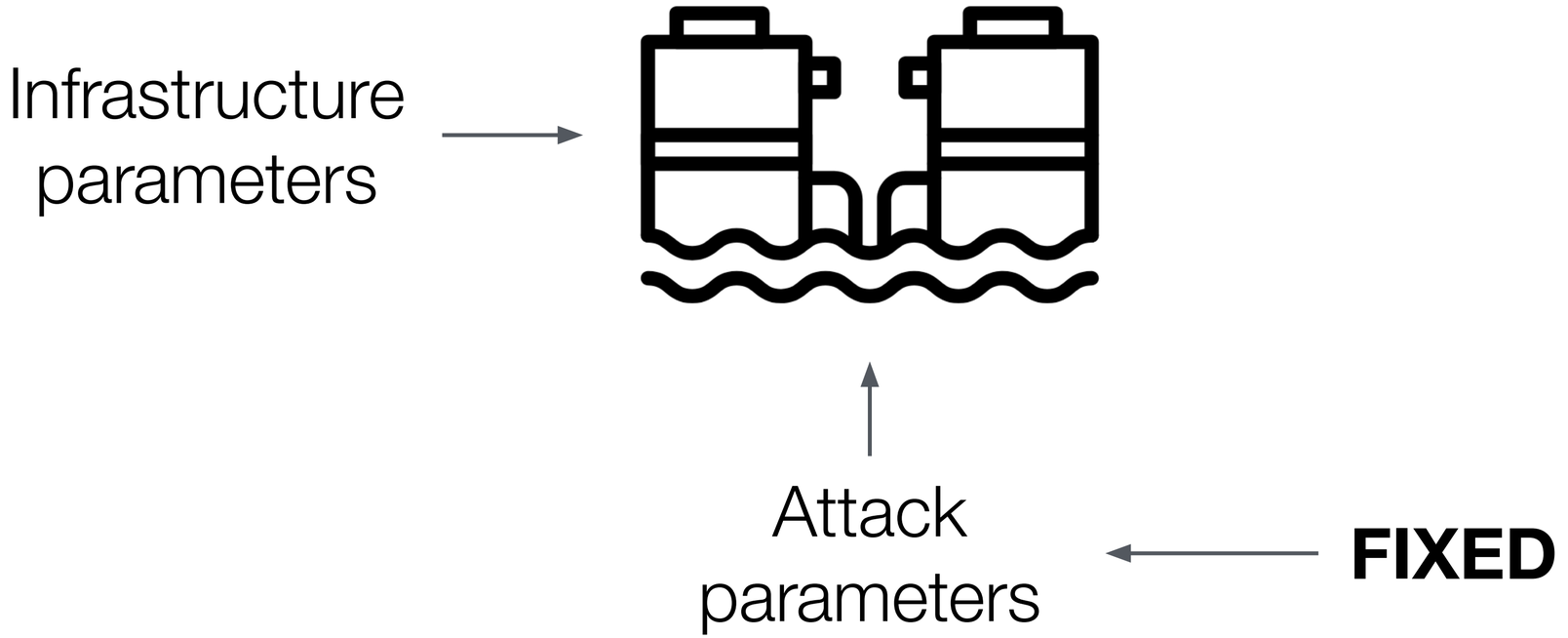


Fig 16: Use cases parameters

Experimentation with Digital Twin

Use cases - Attacks

Use case 1: Resilience when Denial of Service

Use case 2: Resilience when there is a Ransomware

What is required: Advices about getting a representative dataset of attacks

Experimentation with Digital Twin

Use cases - Infrastructure

Use case 1: Pump (SWAT)

Use case 2: Controller (SWAT)

Experimentation with Digital Twin

Projects

Project 1 Implement a Digital Twin for the SWAT system targeting attack consequence prediction

Project 2 Go further and modify the model to side channels for more complex attack monitoring and attack consequence prediction

4

Next Steps

Next steps

Short term

Objective 1 Attend RESSI

Objective 2 Send my paper for C&ESAR 2025

Objective 3 Finish my survey

Next Steps

Long term

Objective 1 Create a DT challenge for ECW

Objective 2 Implement a SWAT System

Objective 3 Detect and predict cyber attacks based on side channel

Open Issues

Issues

Issue 1 How to standardize DT conception and development?

Issue 2 How to measure DT impact in a system rather than traditional methods?

Summary

My presentation in a nutshell

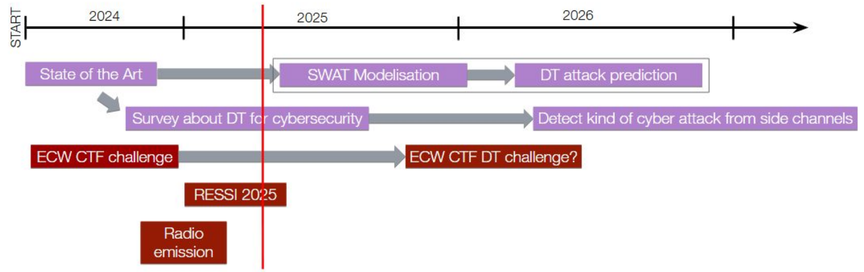
Goals

Goal 1 Developing a metric for the realism of a DT.

Goal 2 Using DTs for more comprehensive risk analysis.

Goal 3 Using DTs for simulating side-channel measurements for better attack detection.

Timeline



Next Steps

Long term

Objective 1 Create a DT challenge for ECW

Objective 2 Implement a SWAT System

Objective 3 Detect and predict cyber attacks based on side channel

Experimentation with Digital Twin

Definition

Aim: Consequence prediction

Target: SWAT

Context: Cyber-physical system