Securing Cyber-Physical Systems

Sabah Suhail

University of Tartu
Information Security Research Group

September 17, 2021

Outline

Table of Contents

Introduction (1/2)

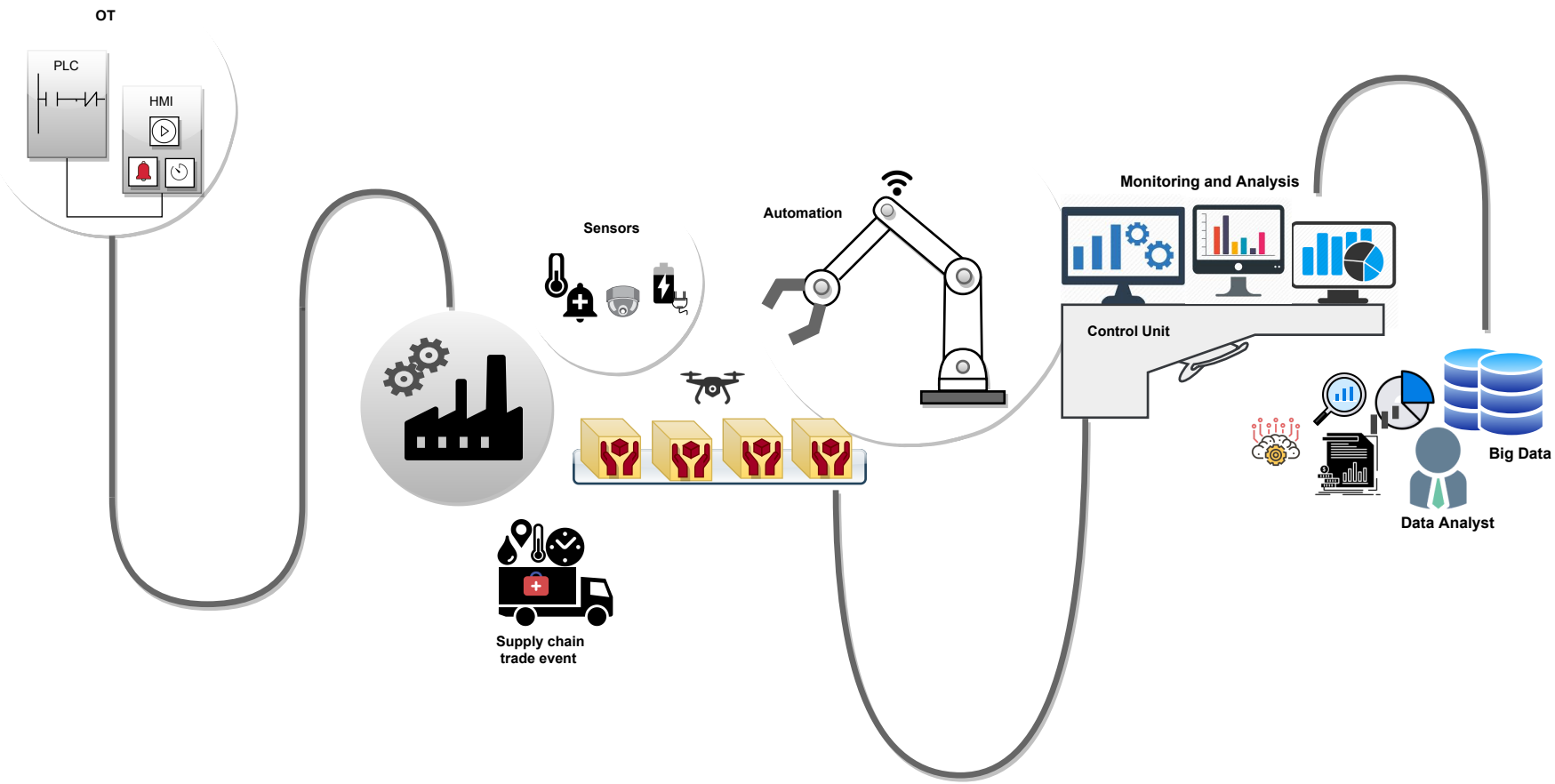


Figure: CPSs: Connecting physical and digital worlds

Introduction (2/2)

- What are the consequences of integrating IT & OT systems in CPSs?

Cyber-attacks

  - Reasons:
    - Operational functionality outweighs security
    - Loopholes in infrastructure enable attackers to launch attacks
    - Trustworthy data-generating sources?

Table of Contents

Motivation

- Essential measures to secure CPSs:
  - evaluating functionality
  - assessing security level by conducting attacks
  - PROBLEM: Availability
- Reflecting CPS in operation while avoiding interference
  - **Solution I**: *IDSs*
    - hard to reproduce attack scenarios
  - **Solution II**: *testbeds*
    - time- and cost-intensive setup/maintenance
- **Problems**:
  - delayed countermeasures
  - not covering entire product lifecycle

Motivation

- Essential measures to secure CPSs:
  - evaluating functionality
  - assessing security level by conducting attacks
  - PROBLEM: Availability
- Reflecting CPS in operation while avoiding interference
  - **Solution I**: *IDSs*
    - hard to reproduce attack scenarios
  - **Solution II**: *testbeds*
    - time- and cost-intensive setup/maintenance
- **Problems**:
  - delayed countermeasures
  - not covering entire product lifecycle

Motivation

- Essential measures to secure CPSs:
  - evaluating functionality
  - assessing security level by conducting attacks
  - PROBLEM: Availability
- Reflecting CPS in operation while avoiding interference
  - **Solution I**: *IDSs*
    - hard to reproduce attack scenarios
  - **Solution II**: *testbeds*
    - time- and cost-intensive setup/maintenance
- **Problems**:
  - delayed countermeasures
  - not covering entire product lifecycle

Table of Contents

Research Objective

How to secure CPSs?

- data trustworthiness
- predictive maintenance
- cyber situational awareness

Table of Contents

Proposed Framework: Overview

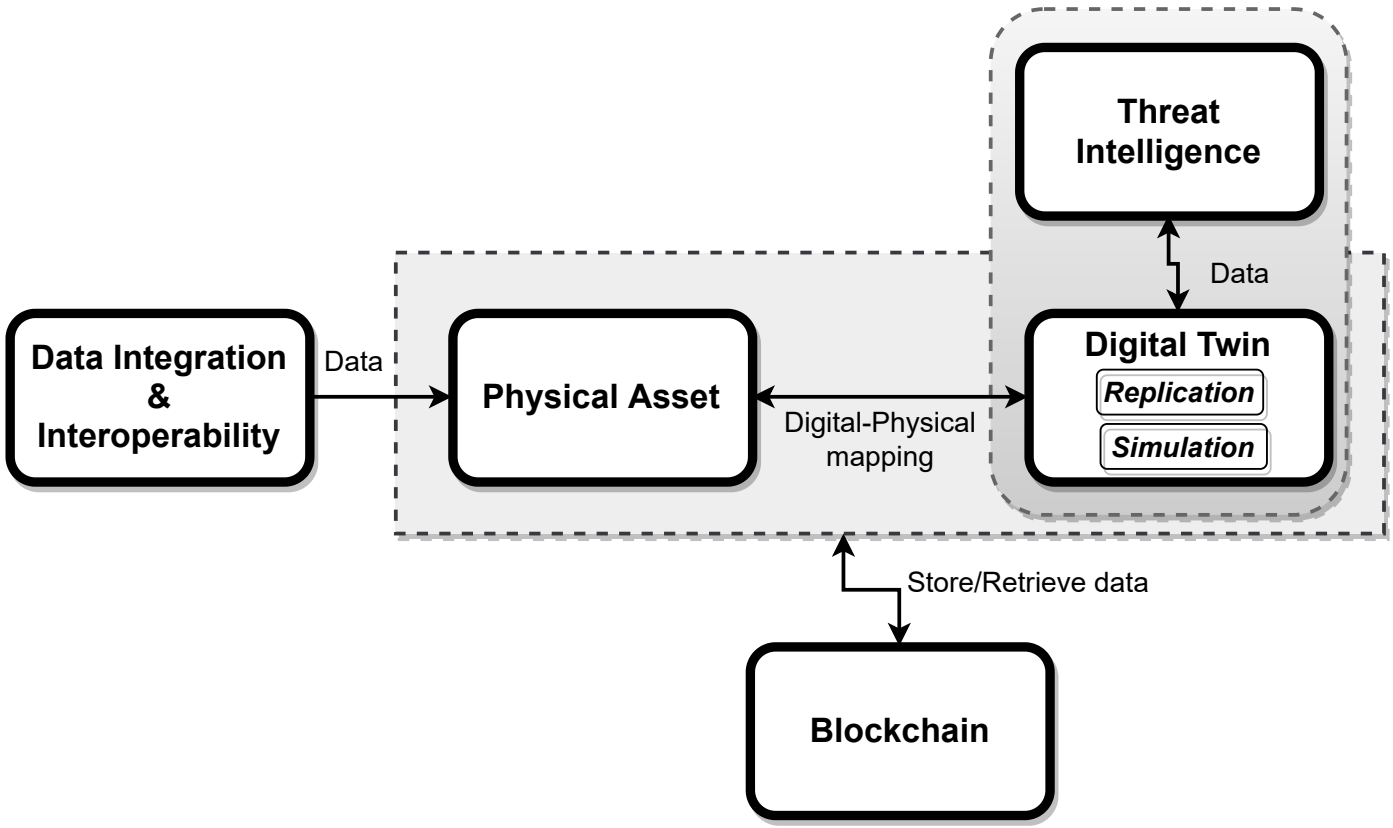


Figure: Overview [5].

Securing CPSs: TI-aided blockchain-based DT framework

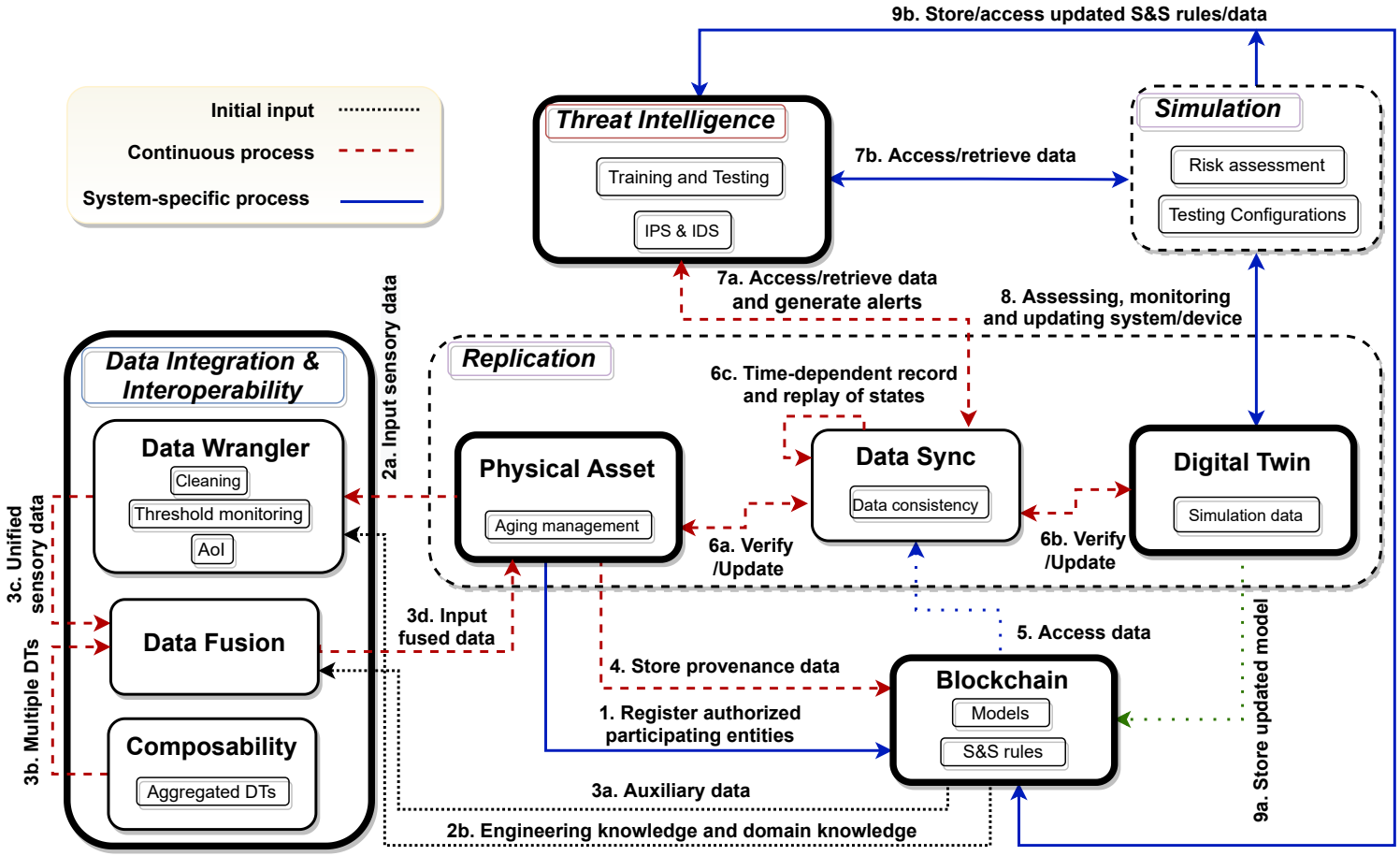
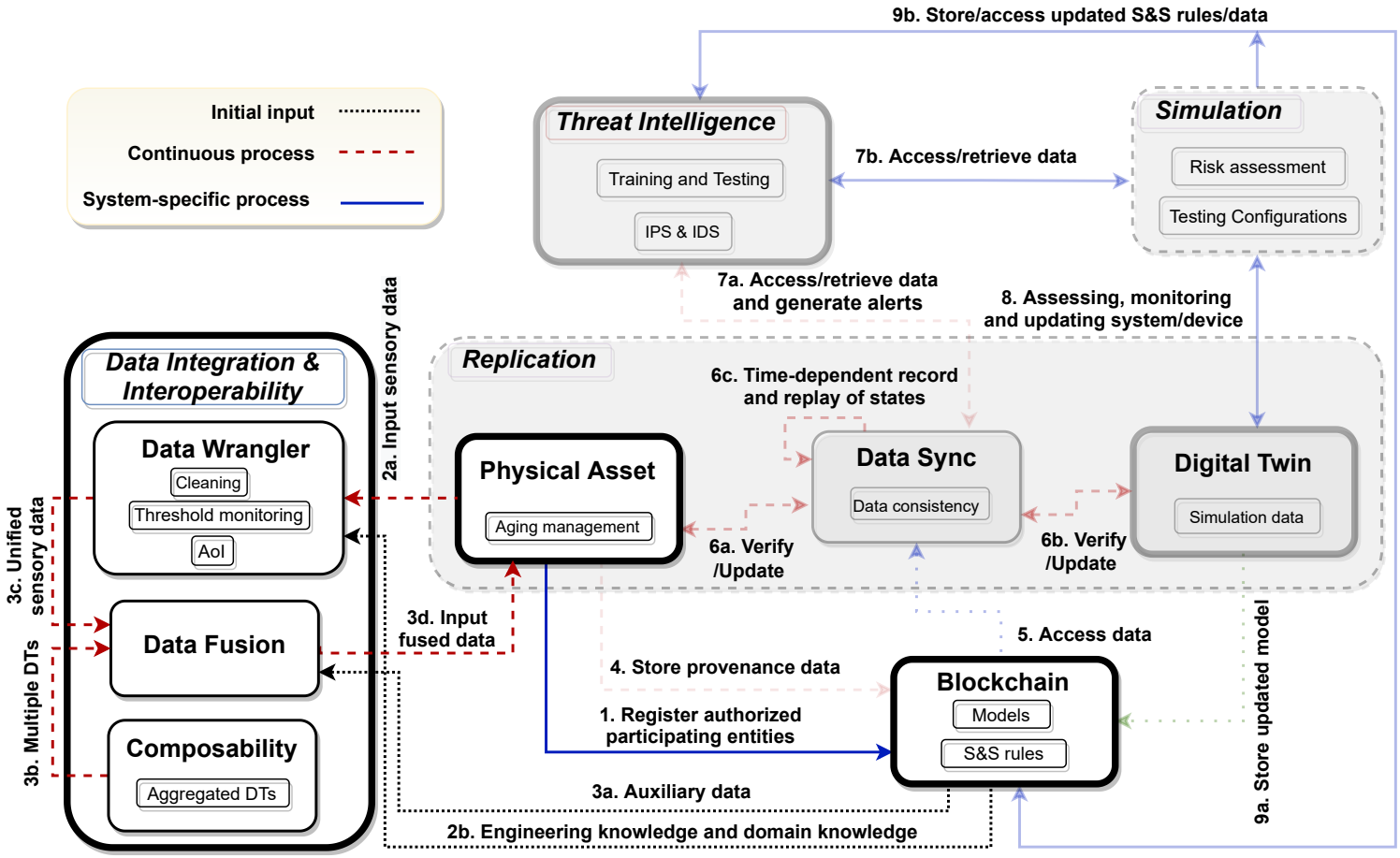


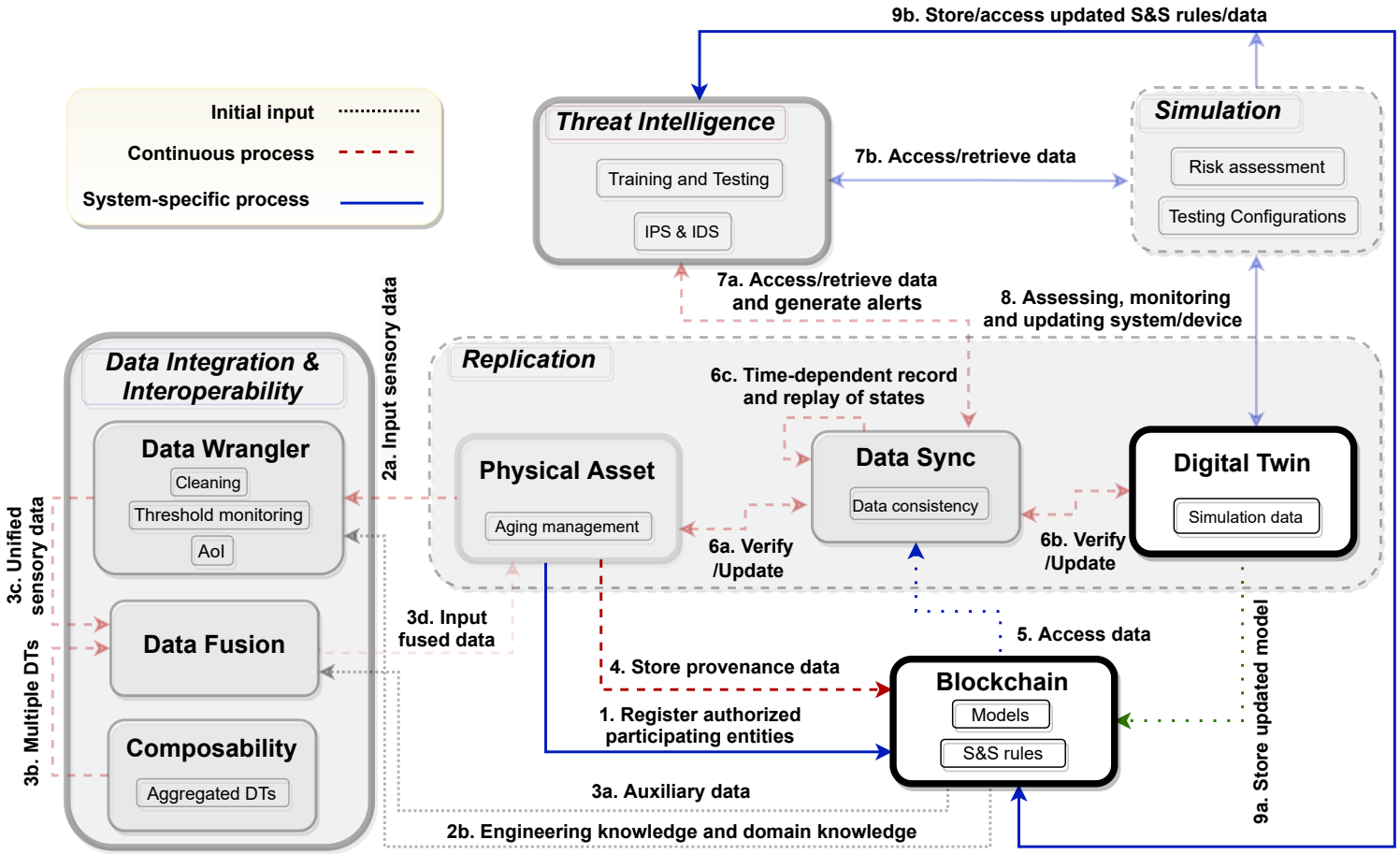
Figure: Securing CPSs: A Framework [5].

Securing CPSs: TI-aided blockchain-based DT framework



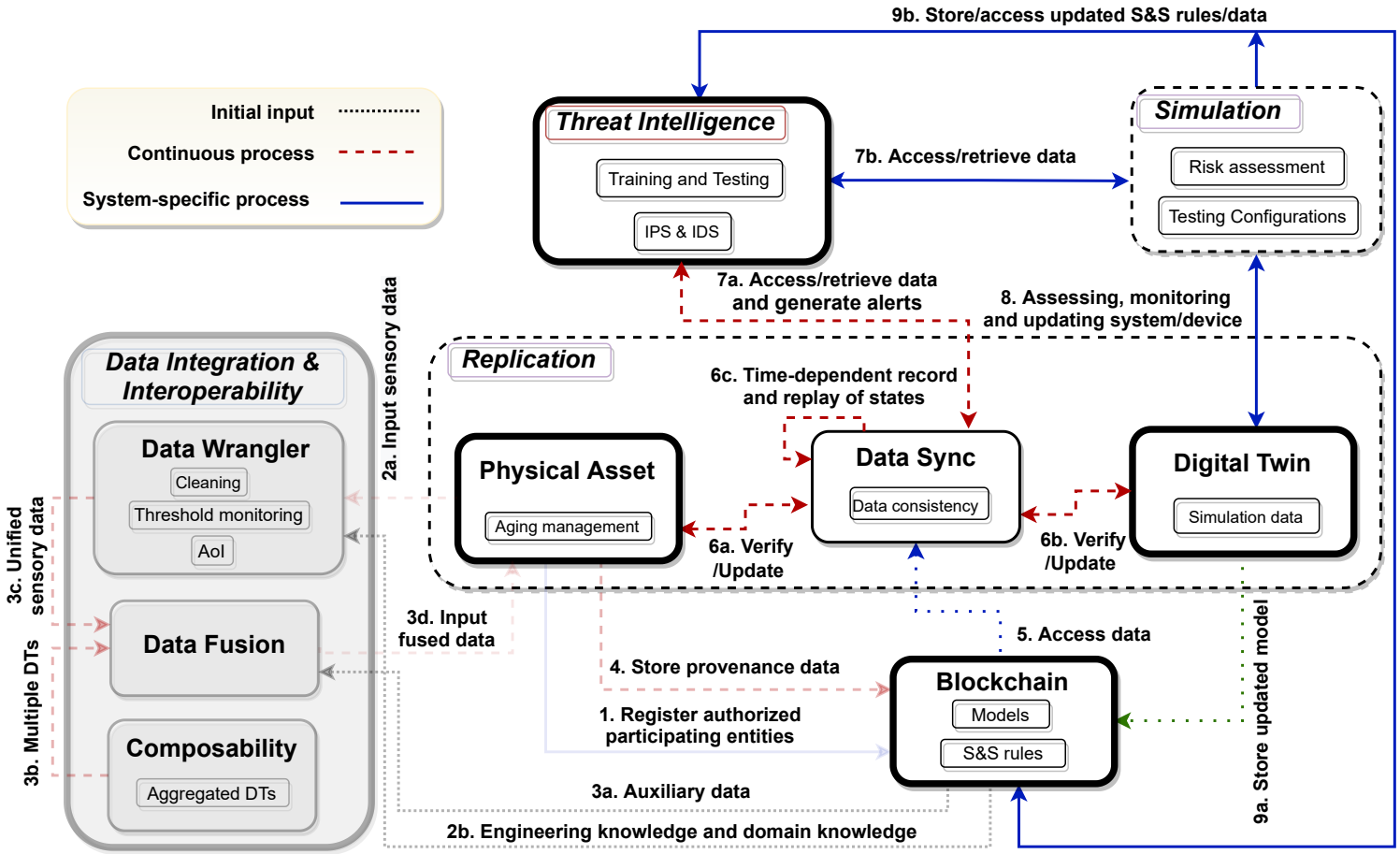
DDI

Securing CPSs: TI-aided blockchain-based DT framework



Blockchain-based DTs

Securing CPSs: TI-aided blockchain-based DT framework



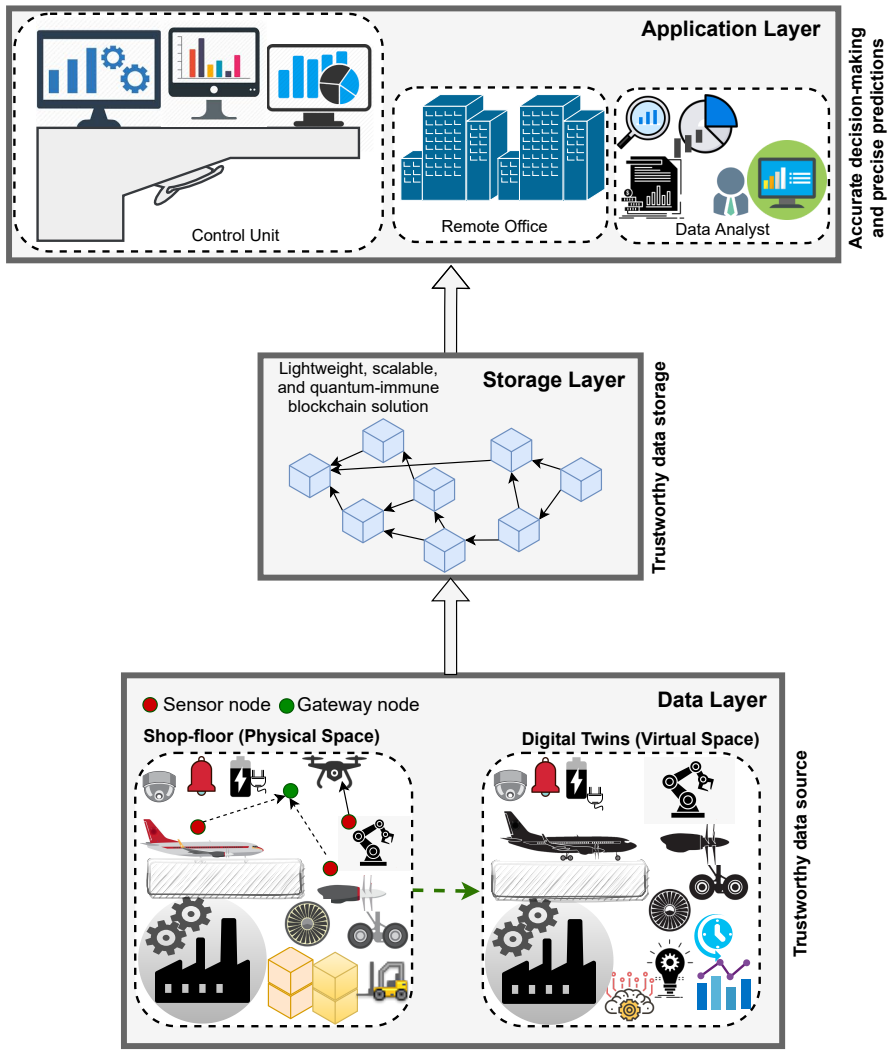
Significance of Data

Errors using inadequate data are much less than those using no data at all.

(Charles Babbage)

Data Integration and Interoperability (1/2)

- ★ Trustworthy data-generating sources ⇒ GIGO
- ★ Data quality



Data Integration and Interoperability (2/2)

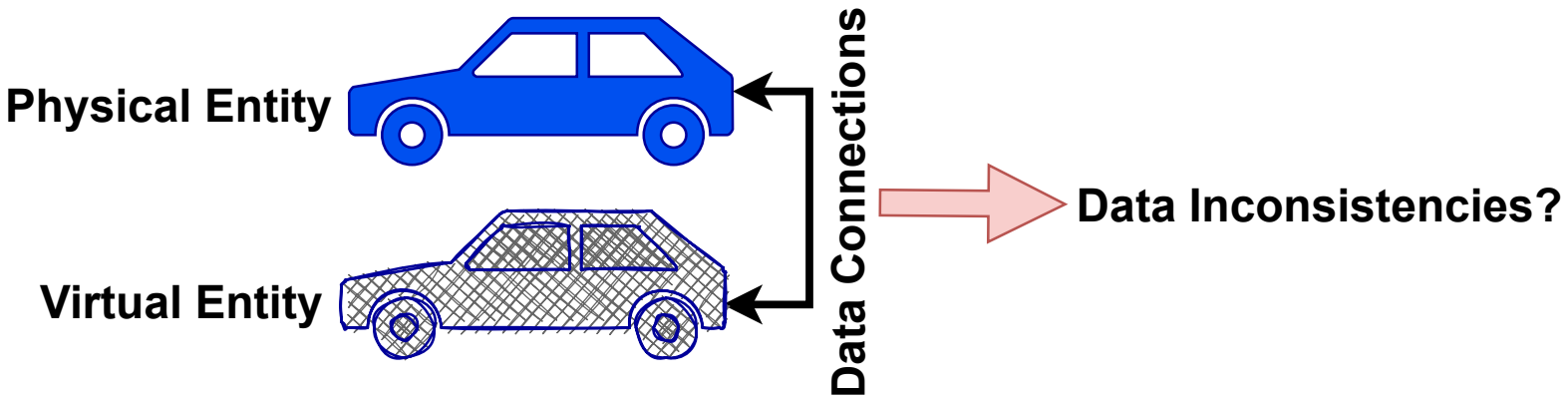
- *Data Wrangler*
  - Cleaning invalid, duplicate, or missing data
    - improve data quality through AI-enabled data curation
  - Integrity Checking Mechanisms (ICMs)
    - *Engineering knowledge* [1]
    - *Domain knowledge*
- *Composability*
  - Aggregates data from multiple DTs or replicas.
- *Data Fusion*
  - Integrate data from *data wrangler* and *composability*

▸ **Framework**

[1] why wee need specifications of CPS?

Digital Twins (1/5)

What are DTs and how they operate?



Suggested reading: What are DTs? [1, 6]
Suggested reading: DTs in the Information Security Domain: [3]
Gartner Hype Cycle for Emerging Technologies

Definition: Digital Twins (2/5)

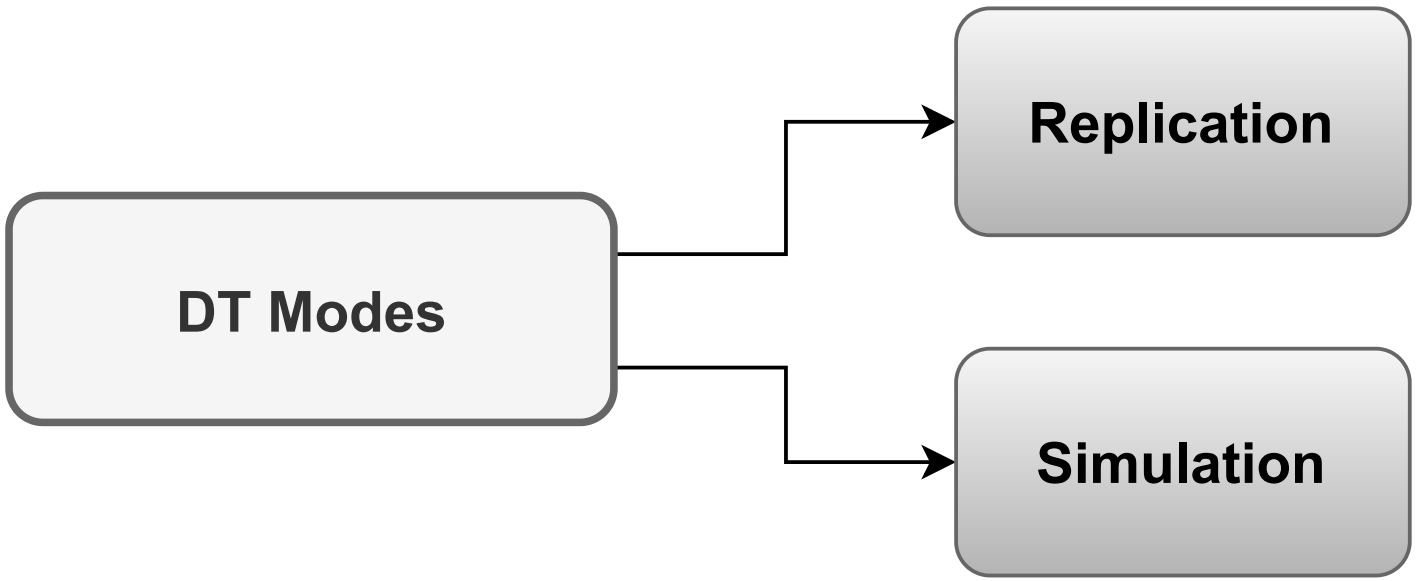
What is our objective of utilizing DTs?

> *A digital twin, which is used for the purpose of enhancing the security of a cyber-physical system, is a virtual replica of a system that accompanies its physical counterpart during phases of its lifecycle, consumes real-time and historical data if required, and has sufficient fidelity to allow the implementation of the desired security measure [3].*

Note: Process knowledge CAN BE obtained through DTs or Process knowledge CAN NOT obtained directly through DTs.

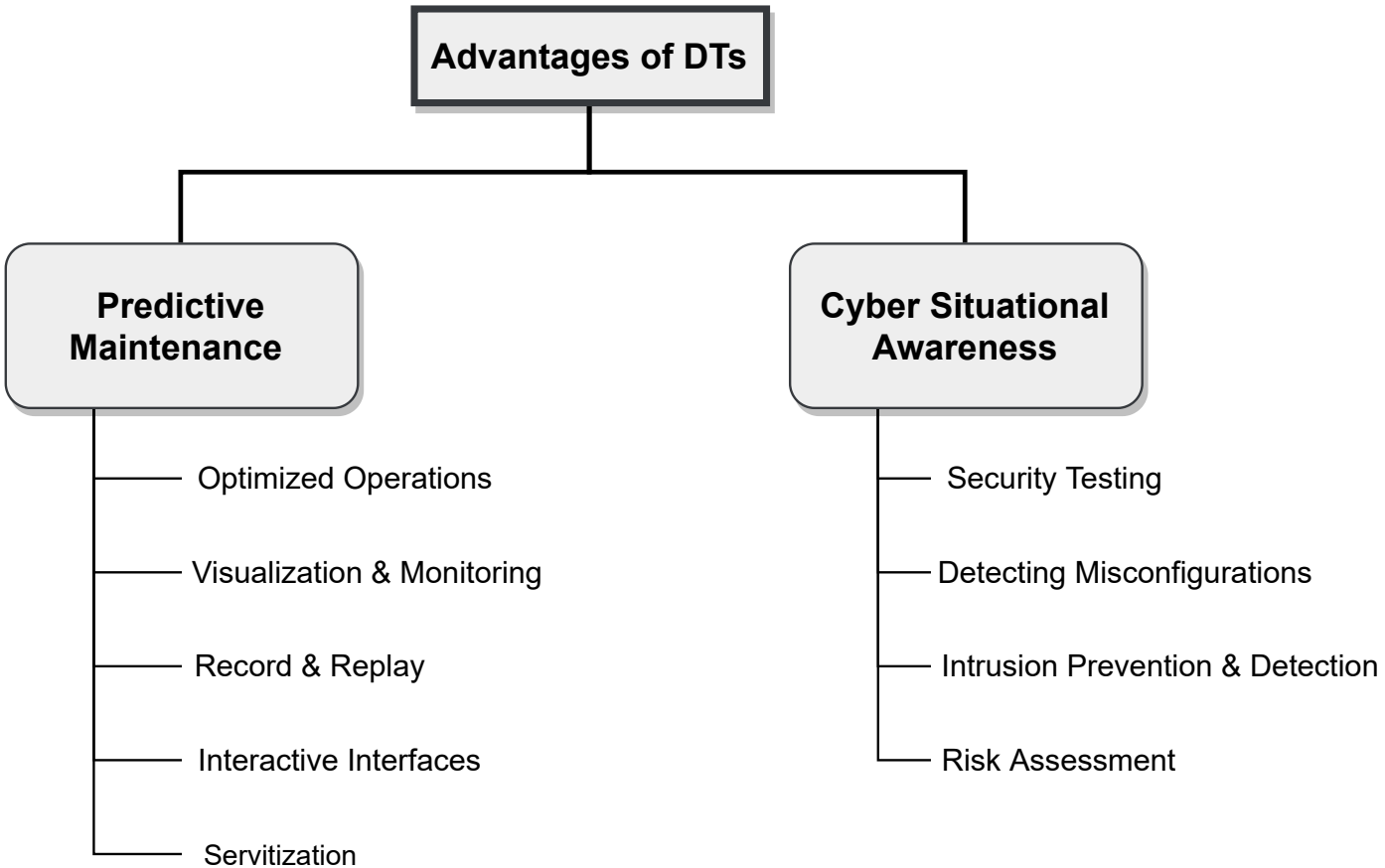
Digital Twins (3/5)

What are DT security-operation modes?



Digital Twins (4/5)

What are the advantages of DTs?



Digital Twins (5/5)

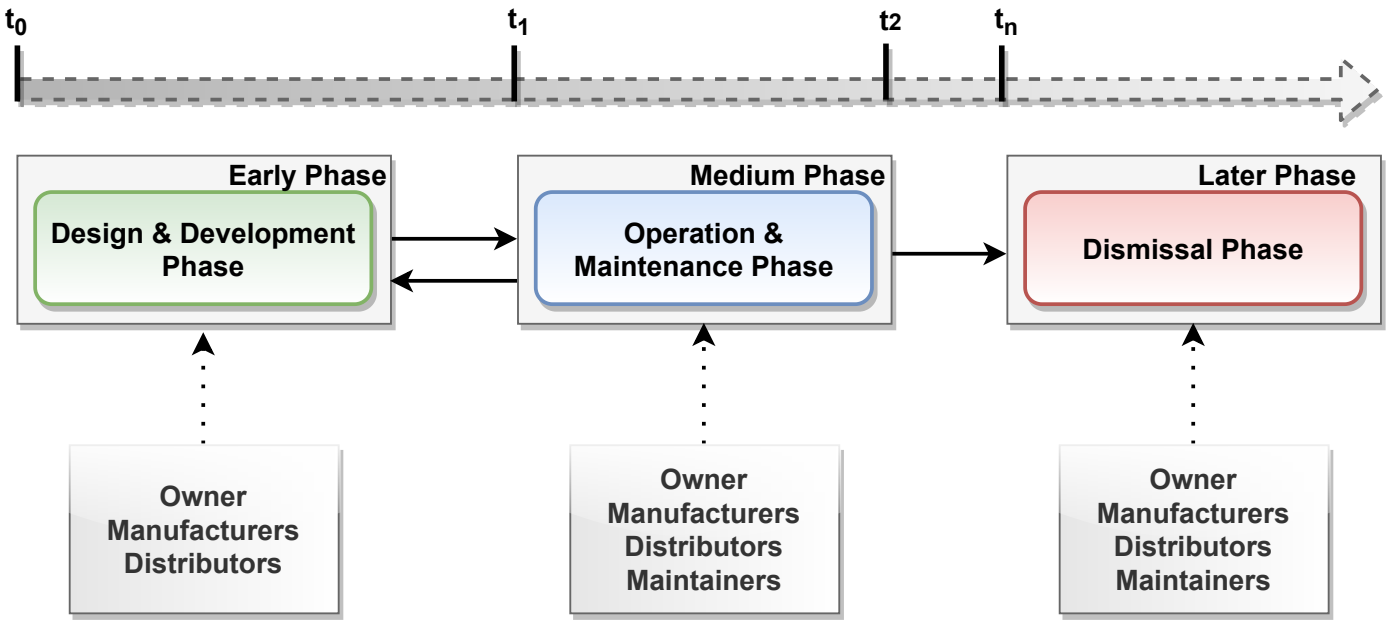
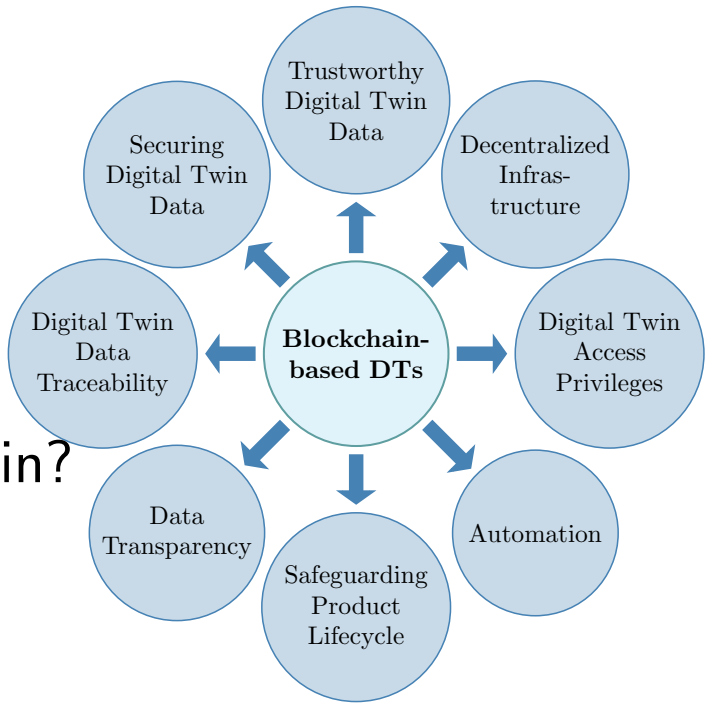


Figure: Lifecycle of DTs [4].

Blockchain Empowered Digital Twins (1/2)

- Do we really need *blockchain*? [2]
- What should be stored on blockchain?
  - critical data
  - sources that can provide *track & trace*
  - separating *dynamic* & *static* data
- What are the design solutions for blockchain?

▸ **Framework**



[2] Suggested reading [4, 9, 8].

Blockchain Empowered Digital Twins (2/2)

- What are S&S?
- Why we need S&S?
- When S&S should be deployed?
- Why we need to store S&S on blockchain?

Framework

How DTs can secure ICS from APT: Stuxnet? [2]

Threat Intelligence (1/4)

- Why we need TI?
- How to analyze volume of data for actionable insights in real-time?

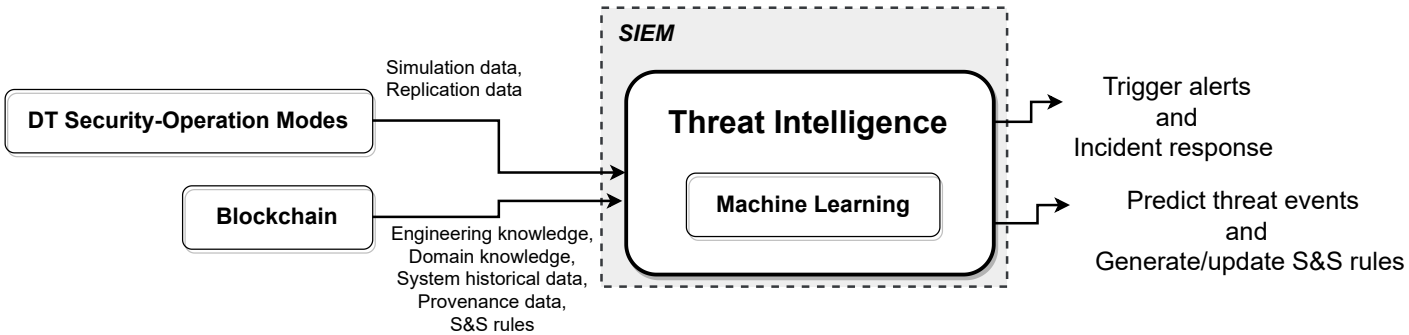


Figure: Overview of TI [5].

Threat Intelligence (2/4)

DTs Replication mode and TI (1/2)

- How replication mode operates?
  - DT and its physical counterpart are constantly connected [3]
- What is the role of replication mode?
  - serve as *training & testing* platform
  - operate virtually disjointed from live systems
  - simulate attack scenarios to analyze system behavior
    - red-blue team exercises
    - DTs and cyber ranges [7]

▸ Framework

[3] log files, sensor measurements, network communication, etc.

Threat Intelligence (3/4)

DTs Replication mode and TI (2/2)

- How TI supports replication mode?
- **Problem**:
  - time-dependent *record & replay* of states
  - state *replication accuracy*
- **Solution**:
  - ML predictive capability provided by TI supports DTs
- How TI responds to *known* and *unknown* threats/attacks?

▸ Framework

Threat Intelligence (4/4)

DTs Simulation mode and TI

- How simulation mode operates?
  - runs independently of its physical counterparts
- What is the role of simulation mode in risk assessment?
  - allows running tests repeatedly under range of conditions
  - support *security by design* approach
- How simulation mode supports TI?
  - predict possibility of attacks or system malfunctioning
  - carry out what-if and cost-benefit analysis

▸ Framework

Table of Contents

Automotive Industry: A CPS Use Case (1/3)

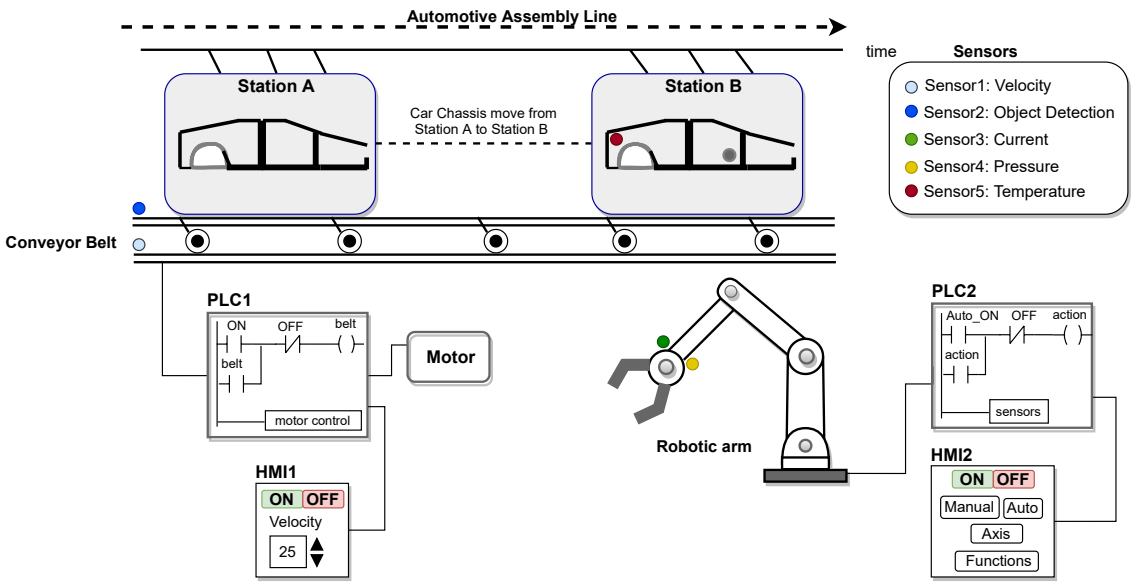
Before production process:

- Retrieving data from blockchain:
  - ICMs
  - application- user-specific data

Automotive Industry: A CPS Use Case (2/3)

During production process:

- Role of DT-based intelligent manufacturing:
  - Predictive Maintenance
  - Cyber Situational Awareness



Simulations and attack scenarios at GitHub

Automotive Industry: A CPS Use Case (3/3)

After production process:

- Collect data from sensors
  - Reasons?
    - fed data to DTs which self-adapts to asset
    - extracts new knowledge for next production processes
    - study adversarial space to update S&S rules for advanced attacks

Table of Contents

Research Challenges

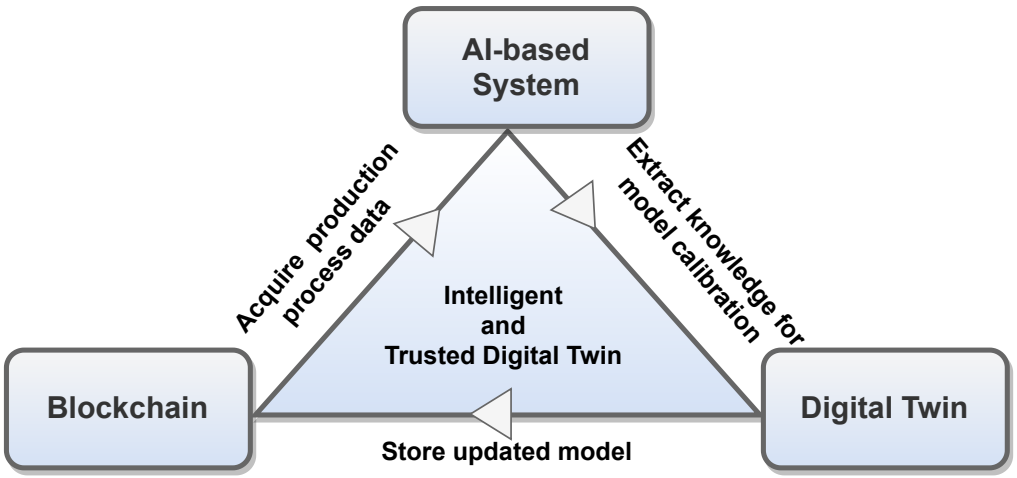
- Accurate representation of DTs
  - Trade-off b/w budget and fidelity
  - State replication accuracy
- Data-related challenges
  - Trade-off b/w excessive and limited data volumes
  - Data storage
  - Merging of disparate data types
- Democratizing AI
  - Need for explainable AI
  - Adversarial inputs

For more details on *challenges for AI in blockchain-based DTs* check [4].

Table of Contents

Conclusion

- Securing CPSs
- Propose a *TI-aided blockchain-based DT* framework
- *Future work*: implementing replication mode and integrating TI



References I

[1] B. R. Barricelli, E. Casiraghi, and D. Fogli.
A survey on digital twin: Definitions, characteristics, applications, and design implications.
IEEE Access, 7:167653–167671, 2019.

[2] M. Dietz and G. Pernul.
Unleashing the digital twin's potential for ics security.
IEEE Security & Privacy, 18(4):20–27, 2020.

[3] M. Eckhart and A. Ekelhart.
Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook, pages 383–412.
Springer International Publishing, Cham, 2019.

[4] S. Suhail, R. Hussain, R. Jurdak, A. Oracevic, K. Salah, and C. S. Hong.
Blockchain-based digital twins: Research trends, issues, and future challenges, 2021.
arXiv: 2103.11585. [Online]. Available: https://arxiv.org/abs/2103.11585.

[5] S. Suhail, R. Jurdak, R. Matulevičius, and C. S. Hong.
Securing cyber-physical systems through blockchain-based digital twins and threat intelligence, 2021.
arXiv: 2105.08886. [Online]. Available: https://arxiv.org/abs/2105.08886.

[6] F. Tao, H. Zhang, A. Liu, and A. Y. Nee.
Digital twin in industry: State-of-the-art.
IEEE Transactions on Industrial Informatics, 15(4):2405–2415, 2018.

[7] M. Vielberth, M. Glas, M. Dietz, S. Karagiannis, E. Magkos, and G. Pernul.
A digital twin-based cyber range for soc analysts.
In K. Barker and K. Ghazinour, editors, *Data and Applications Security and Privacy XXXV*, pages 293–311, Cham, 2021.
Springer International Publishing.

References II

[8] K. Wüst and A. Gervais.
Do you need a blockchain?
In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54, Zug, Switzerland, jun 2018. IEEE.

[9] I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar, and M. Imran.
Blockchain for digital twins: Recent advances and future research challenges.
IEEE Network, 34(5):290–298, 2020.

Thank You!

Q & A

Contact:

sabah.suhail@ut.ee

Thesis Topics:

- ⋆ Blockchain-based Digital Twins
- ⋆ Digital Twins for Cyber-Physical Systems Security