Enhancing CyberSecurity with Digital Twins and AI

Hugo BOURREAU*, Marc-Oliver PAHL*, Fabien DAGNAT*
*{prénom.nom}@imt-atlantique.fr

CHAIRE CYBER CNI Sécurité des infrastructures critiques

cyberCNI.fr/

Context of the thesis

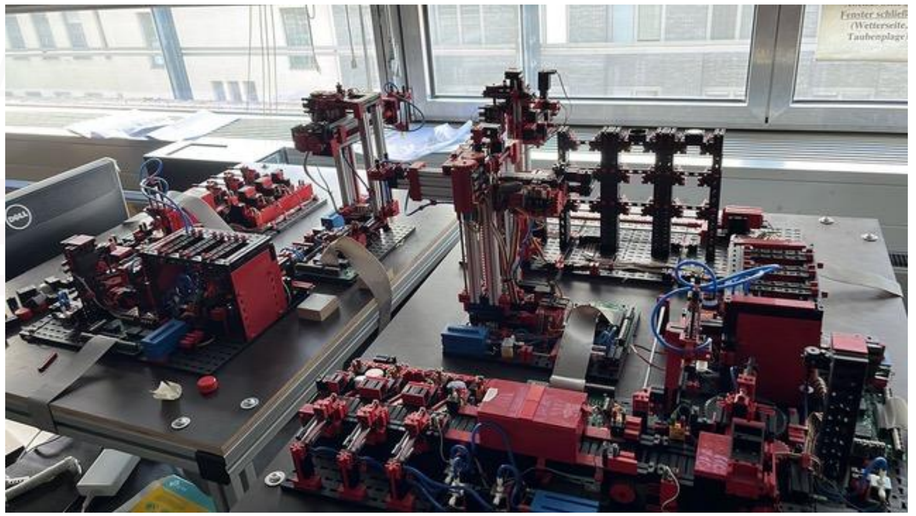
Chair

- Partners:
  - State of the art
  - Users stories

- CyberCNI:
  - Fishertechnik
  - CyberRange

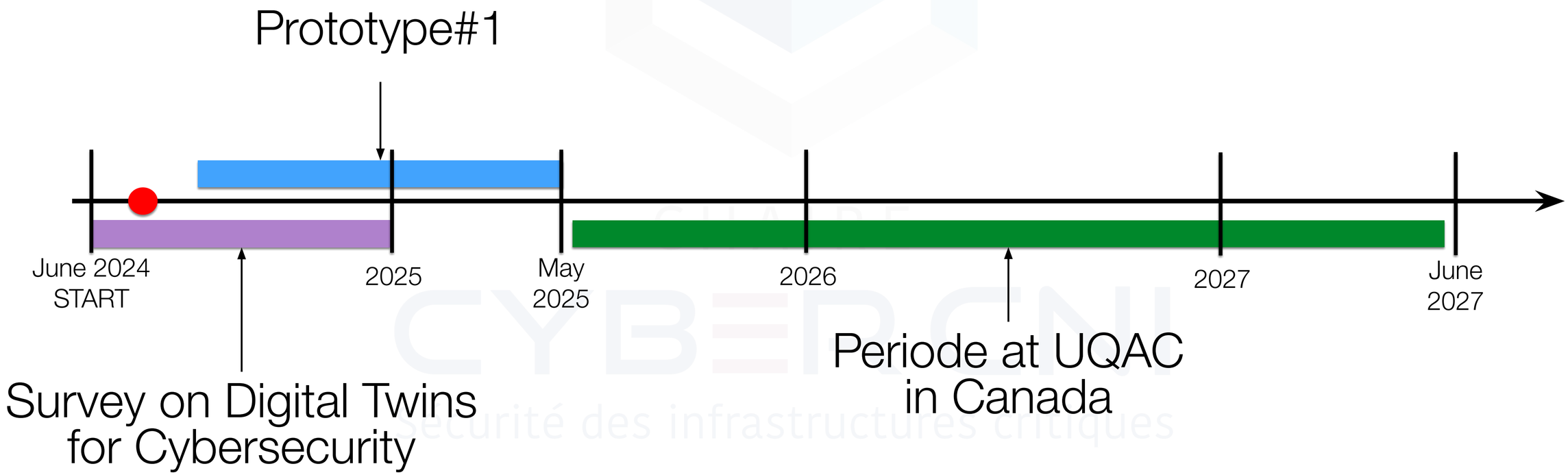
Cotutelle

- UQAC:
  - International PoV
  - IoT lab



Context of the thesis

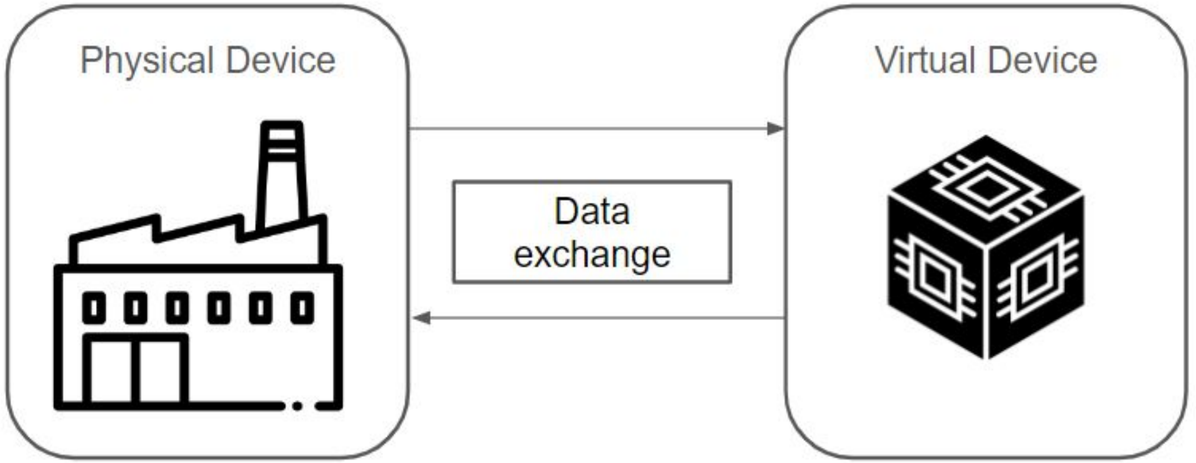
Timeline



Digital Twins

Digital Twins

Definition

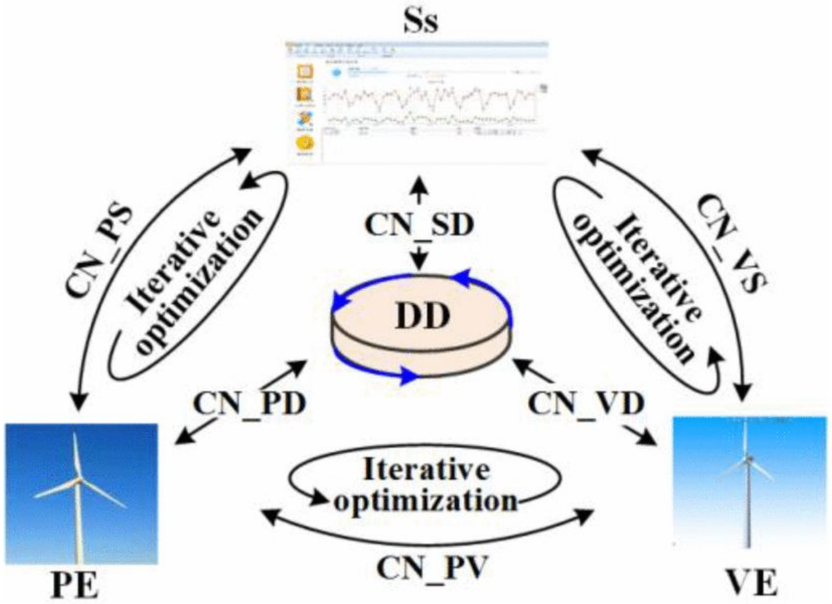


Holmes, David, Maria Papathanasaki, Leandros Maglaras, Mohamed Amine Ferrag, Surya Nepal, and Helge Janicke. “Digital Twins and Cyber Security – Solution or Challenge?” In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, 1–8, 2021. https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277.

Liang, Kaixin, Yuehong Chen, and Qi Zhang. “A Digital Twin Model Construction Method for Ships.” In *2023 IEEE 11th International Conference on Computer Science and Network Technology (ICCSNT)*, 402–5, 2023. https://doi.org/10.1109/ICCSNT58790.2023.10334571.

Digital Twins

Definition



Five-dimension model for the DT[1]

PE : Physical Entity
VE : Virtual Entity
Ss: Services
DD : DT Data
CN_PD : Connexion Physical Data
CN_VD : Connexion Virtual Data
CN_SD : Connexion Simulation Data
CN_PS : Connexion Physical Simulation
CN_VS : Connexion Virtual Simulation
CN_PV : Connexion Physical Virtual

1: Tao, Fei, He Zhang, Ang Liu, and A. Y. C. Nee. “Digital Twin in Industry: State-of-the-Art.” *IEEE Transactions on Industrial Informatics* 15, no. 4 (April 2019): 2405–15. https://doi.org/10.1109/TII.2018.2873186.

Digital Twins for Cybersecurity

Hugo BOURREAU, Marc-Oliver PAHL, Fabien DAGNAT | cyberCNI.fr

Digital Twins for Cybersecurity

General purpose

Aim: Create a Digital Twin for pentesting purposes

Target: OT Systems (Cyber-Physical Systems)

Context: Critical Infrastructures

CPHoneynet

Research topics

(T1) Survey of Digital Twins solutions for cybersecurity of CPS

- (T1.1) Looking for Digital Twin implementation in Industry and IT Systems
- (T1.2) Service simulation-based solutions
- (T1.3) AI-based solutions

(T2) Challenges of adapting DT for Cybersecurity in critical infrastructures

- (T2.1) Data acquisition and privacy concerns
- (T2.2) Model training and scalability

Digital Twins for Cybersecurity

Existing literature

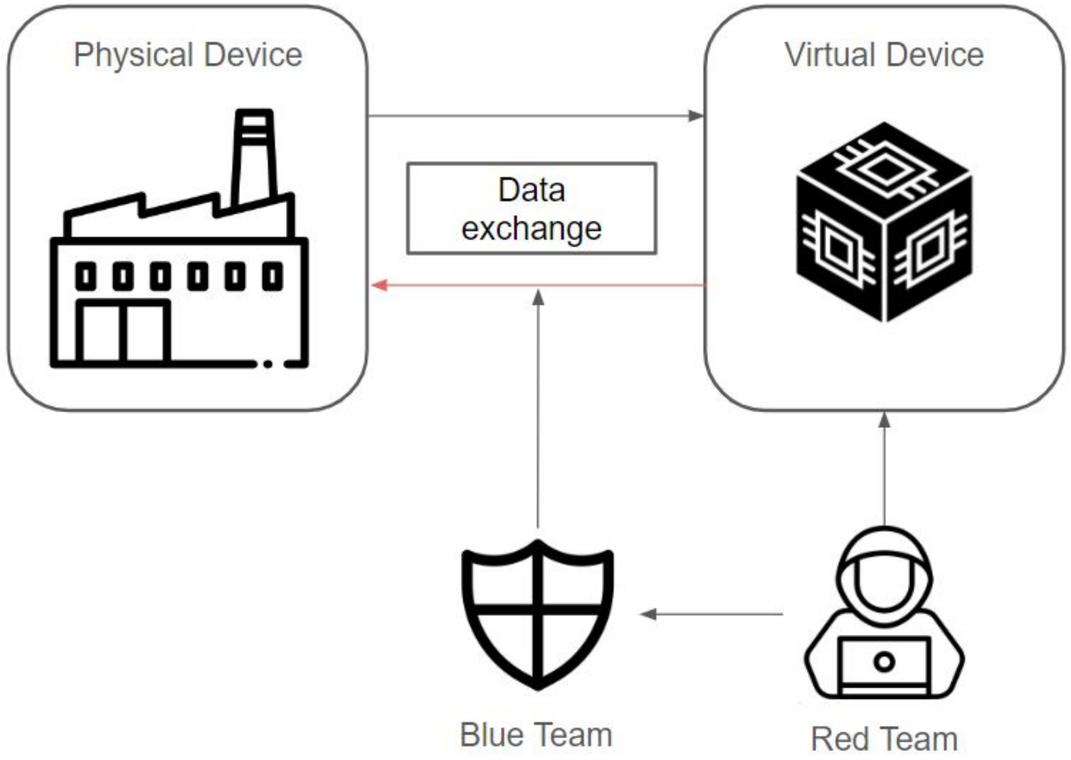
Keywords	Number of articles in this category
BIM	30
Digital twins	3
IOT	13
Security	26
BIM, DT	0
BIM, IOT	2
BIM, Security	12
DT, IOT	2
DT, Security	3
IOT, Security	14
BIM, DT, IOT	3
BIM, DT, Security	1
BIM, IOT, Security	5
DT, IOT, Security	3
BIM, DT, IOT, Security	1
Random	6

Article distribution[1]

1: Alshammari, Kaznah, Thomas Beach, and Yacine Rezgui. “Cybersecurity for Digital Twins in the Built Environment: Current Research and Future Directions.” *Journal of Information Technology in Construction (ITcon)* 26, no. 10 (April 26, 2021): 159–73. https://doi.org/10.36680/j.itcon.2021.010.

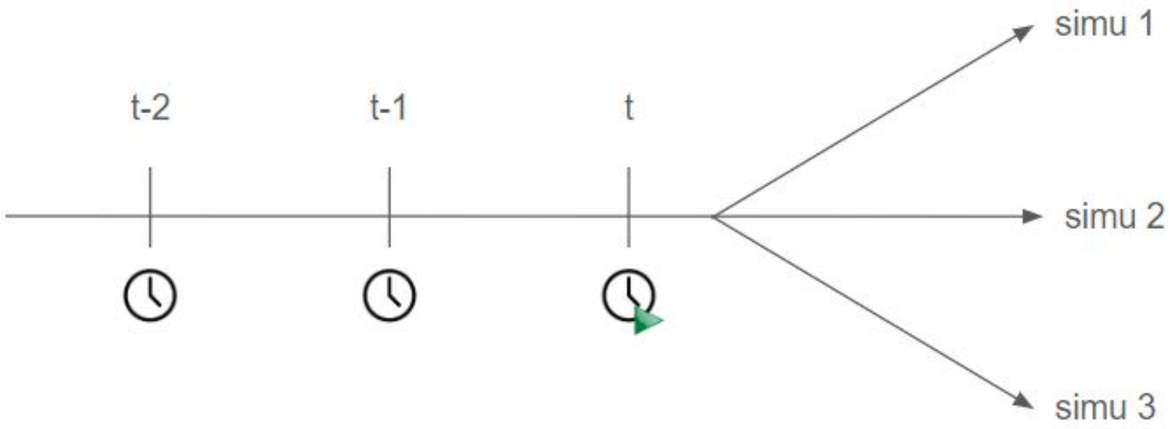
Digital Twins for Cybersecurity

Digital Twin Architecture



Digital Twins for Cybersecurity

Digital Twin Usage



Challenges identified

Challenge#1: Identify the state of the art

Challenge#2: Create a prototype of Digital Twin for Cybersecurity purposes

Challenge#3: Evaluate the feasibility of such an implementation in a critical infrastructure environment

Challenges identified

Challenge#1: Start writing the survey

Challenge#2: Look for concrete implementations

Challenge#3:

Challenges identified

Challenge#1: Provide relevant aspects, human in the loop

Challenge#2: Training of the model

Challenge#3: Complexity of cyber threats

Challenges identified

Challenge#1:

Challenge#2: Data Acquisition / Data from partners ?

Challenge#3: Scalability of the model

Currently being done

Survey: Beginning of writing

Digital Twin-based CTF: For ECW

Thank you for your attention.

Question time!

hugo.bourreau@imt-atlantique.fr