Digital twins for safe and secure industrial systems

Bastien Sultan, Ludovic Apvrille, Philippe Jaillon
{bastien.sultan, ludovic.apvrille}@telecom-paris.fr
philippe.jaillon@emse.fr
February 6, 2022

Plan

Introduction

Cyber-Physical Systems (CPS) are often...

- (highly) complex

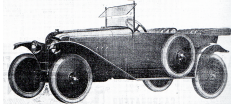
Introduction

San Diego Air and Space Museum Archives

Cyber-Physical Systems (CPS) are often...

- (highly) complex

1911 Encyclopædia Britannica, Vol. 24, pg. 898, Plate XIII

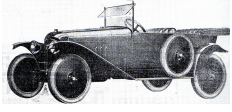


Le catalogue Citroën 1918-1960, Fabien Sabatès, Editions Massin

Introduction

Cyber-Physical Systems (CPS) are often...

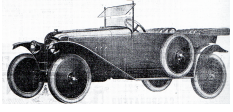
- (highly) complex
- safety-critical

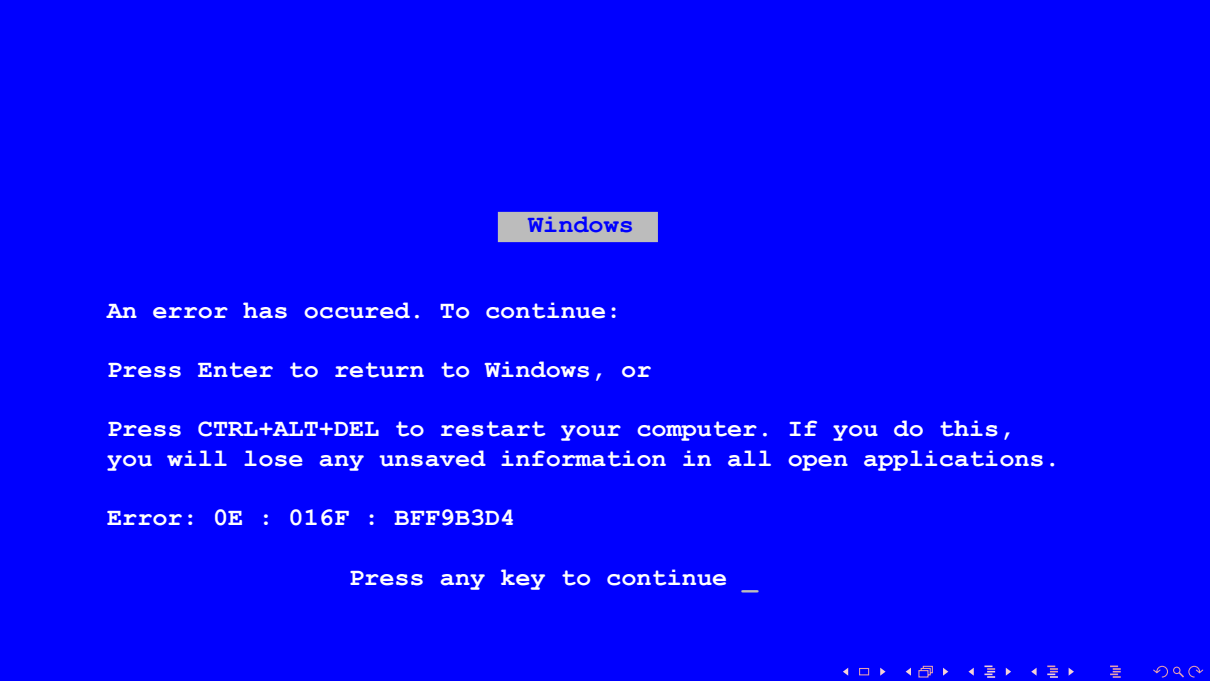


Introduction

Cyber-Physical Systems (CPS) are often...

- (highly) complex
- safety-critical
  - Cyberattacks on CPS can result in intolerable human or environmental consequences...




Windows
An error has occured. To continue:
Press Enter to return to Windows, or
Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.
Error: 0E : 016F : BFF9B3D4
Press any key to continue _

Introduction

Cyber-Physical Systems (CPS) are often...

- (highly) complex
- safety-critical
  - Cyberattacks on CPS can result in intolerable human or environmental consequences...
  - ... so do badly chosen countermeasures!

We need a comprehensive assessment of security countermeasures in order to select among them:

- the **most efficient**
- and the **least side effect prone** ones.

Plan

W-Sec in a nutshell

Objectives

SPARTA

- Assessing the efficiency and impacts of security countermeasures on a system
- In terms of **safety**, **security** and **performance**

W-Sec in a nutshell

Objectives

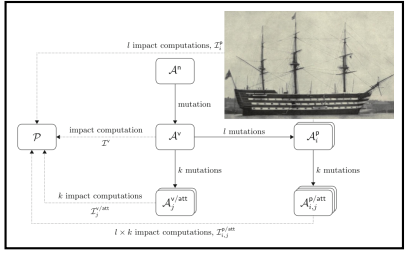
SPARTA

- Assessing the efficiency and impacts of security countermeasures on a system
- In terms of **safety**, **security** and **performance**

Verification

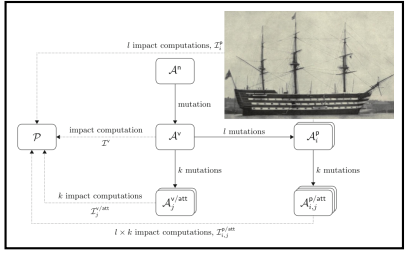
- Based on formal modeling with SysML-Sec
- Using formal verification and simulation for assessments

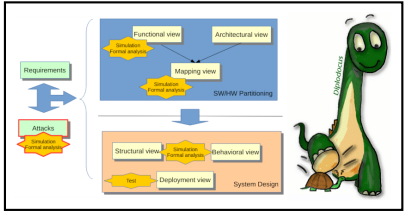
W-Sec in a nutshell



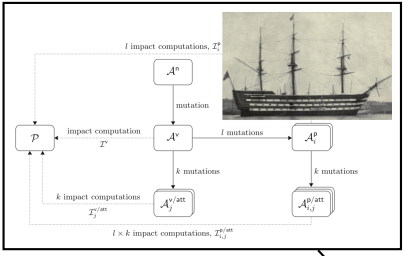
Reprinted by permission of
Springer, LNCS, [1], ©2018

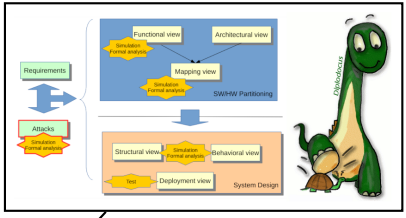
W-Sec in a nutshell

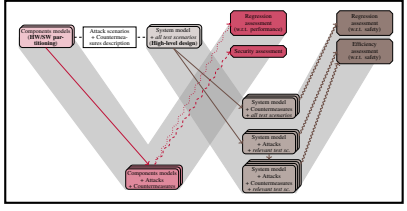




W-Sec in a nutshell







W-Sec in a nutshell

Two interwoven modeling and assessment cycles

Four stages

Modeling → Mutation → Verification and Simulation → Feedback

W-Sec in a nutshell

Two interwoven modeling and assessment cycles

Four stages

Modeling → Mutation → Verification and Simulation → Feedback

Two abstraction levels

- Components level, for **security** and **performance** assessment
- System level, for **safety** assessment
- Two distinct modeling views, reducing the complexity (of models and assessment operations): **HSW** and **System** view (two SysML profiles)

W-Sec in a nutshell

Two interwoven modeling and assessment cycles

Four stages

Modeling → Mutation → Verification and Simulation → Feedback

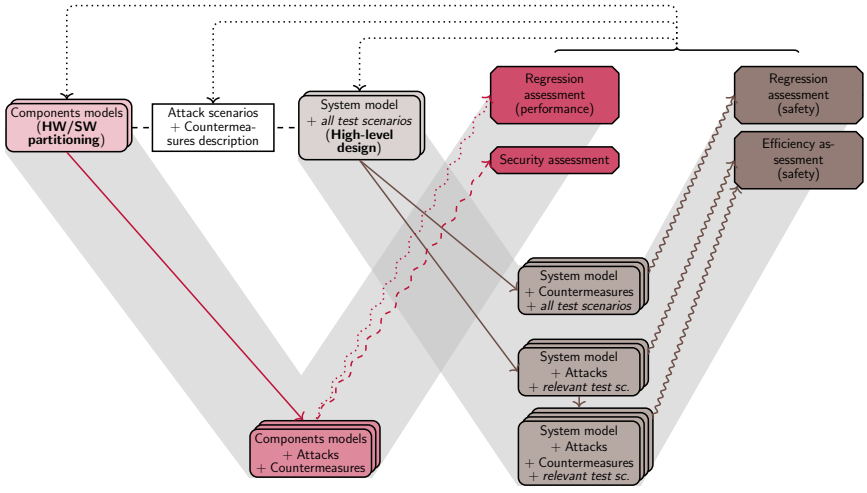
Two abstraction levels

- Components level, for **security** and **performance** assessment
- System level, for **safety** assessment
- Two distinct modeling views, reducing the complexity (of models and assessment operations): **HSW** and **System** view (two SysML profiles)

Ready to apply

W-Sec uses modeling and validation techniques already supported by TTool

W-Sec: Overview

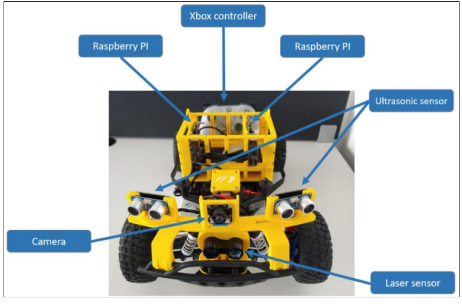


W-Sec: Application to SPARTA

SPARTA case-study: a swarm of rovers

- 4 attack scenarios, 4 platoon scenarios, 5 countermeasures
- 47 enriched models
- 110 safety property checks
- 12 security property checks
- 126 performance measurements

W-Sec provided an interesting basis for countermeasures comparison



Credits: Fortiss, SPARTA report D5.2

Plan

Industry of the Future

Specific features

- Complexity
- Diversity (IT, OT – including PLC –, sensors, actuators, etc.)
- Scalability
- Resilience
  - Operational maintenance
  - Patch and vulnerability management

Programmable Logic Controllers (PLC)

Architecture

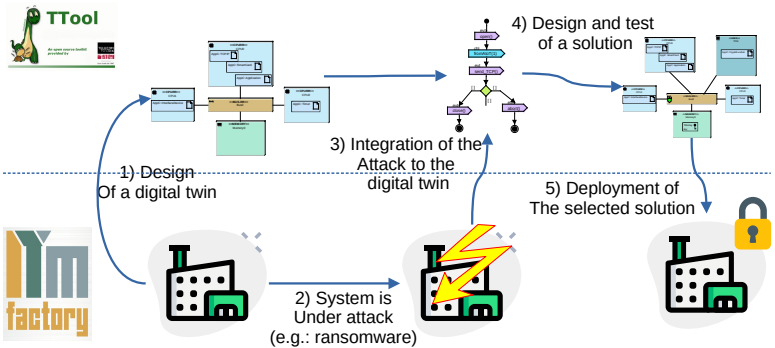
- Sensors | Input memory | CPU + RAM | Output memory | Actuators
- Dedicated networks (Profibus, RS-485, Direct command, etc.)
- Generic Ethernet/IP networks with specific features.

More time constraints

- Real time constraints
- Isochronous data communication

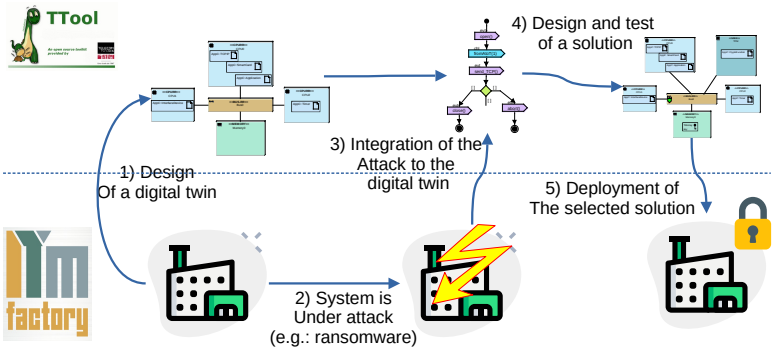
TTool will be used to model PLCs and their specificities (operating cycles, etc.)

Digital twins for safe and secure industrial systems



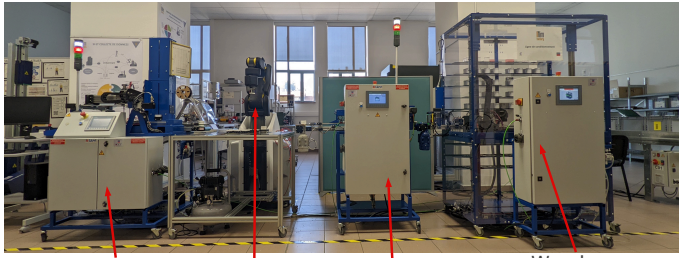
W-Sec applied to security, safety and performance evaluation in the context of the industry of the future.

Digital twins for safe and secure industrial systems



W-Sec applied to security, safety and performance evaluation in the context of the industry of the future.

IT'm Factory's packaging chain



Our goal

Design the digital twin of the packaging chain with TTool so that we can check, thanks to formal verification, if the safety, security and performance properties of the system are still ensured after an upgrade.

IT'm Factory's packaging chain

Physical topology

- Warehouse → Filling machine → Cobot → Packer
- Integration with the platform LAN
- Integration with WAN/Internet/Cloud (through MES and MindSphere)

Data flows

- Supervision console → (warehouse, filling machine, cobot, packer)
- (warehouse, filling machine, packer) → (supervision console, MES, MindSphere)

IT'm Factory as a Testbed

Use-case #1: MindConnect

- TWIST project (InterCarnot 2022, TP/MSE)
- Integrate the packaging chain with a MindConnect, an equipment dedicated to the monitoring of the system through Cloud-based services
- Evaluate the impact of this integration

Use-case #2: Moving Target as remediation method

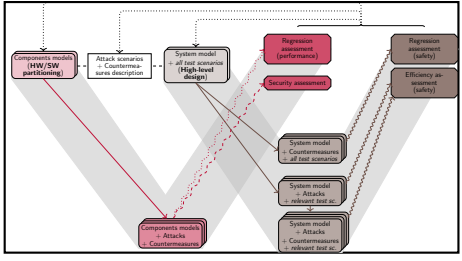
- MTD (Carnot TSN 2002, TP/TSP/MSE)
- Ensure that the properties of the packaging chain remain verified when performing the Moving Target remediation method

Plan

Conclusions (1/2)

W-Sec

- Developed in the scope of SPARTA
- Three kinds of assessment (safety, security, performance)
- Two sets of models (SHW, System)
- Based on SysML-Sec and TTool: ready-to-use, easy-to-use



Conclusions (2/2)

Future Works

- Automate the models enrichment task
- Investigate the links between HSW and System views
- Design comparison metrics
- Evaluate W-Sec in the industy of the future context (IT'm Factory)

Plan

Bibliographie I

[1] Sultan, B., Dagnat, F., and Fontaine, C.
A methodology to assess vulnerabilities and countermeasures impact on the missions of a naval system.
In *Computer Security* (Cham, 2018), S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, and S. Gritzalis, Eds., Springer International Publishing, pp. 63–76.