INSTITUT
POLYTECHNIQUE
DE PARIS

Safe and secure robots

Prof. Ludovic Apvrille, Dr Bastien Sultan, Prof. Tullio Tanzi
ludovic.apvrille@telecom-paris.fr

Seminar at ISAE-SUPAERO, July 7th, 2022

Outline

Outline

Introduction

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

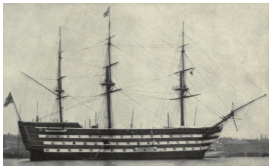
- (Highly) complex

Introduction

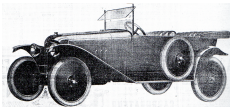
San Diego Air and Space Museum Archives

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

- (Highly) complex



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

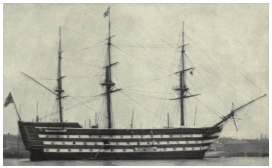


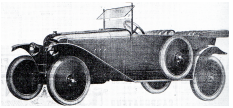
Le catalogue Citroën 1918-1960, Fabien Sabatès, Editions Massin

Introduction

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

- (Highly) complex
- Safety-critical

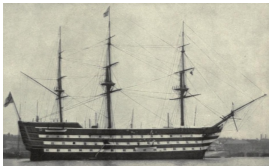


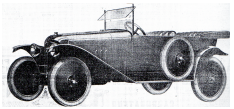


Introduction

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

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





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!

Assessment of security countermeasures:

- The **most efficient**
- The ones with the less important side effects

Why not use SysML-Sec? (1/2)

Talk at ISAE-SUPAERO, July 2018:

Model-Driven Engineering for Safety,

Security and Performance:

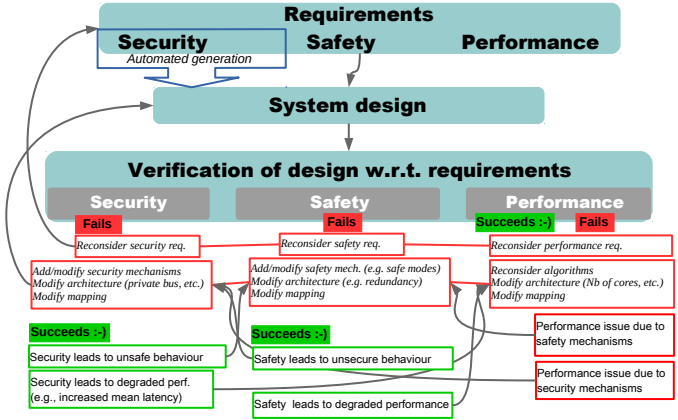
SysML-Sec

Ludovic APVRILLE
ludovic.apvrille@telecom-paristech.fr

Invited talk - ISAE Supaero

[SYSML-SEC] *Ludovic Apvrille, Yves Roudier, "Designing Safe and Secure Embedded and Cyber-Physical Systems with SysML-Sec", Chapter in Model-Driven Engineering and Software Development, p293–308, Springer International Publishing, 2016.*

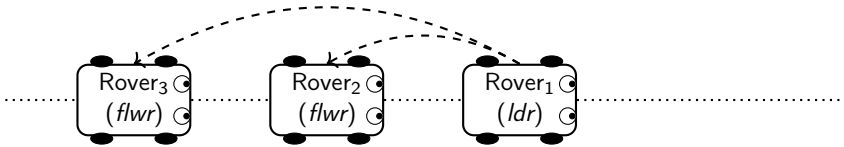
Why not use SysML-Sec? (2/2)



Fully supported by TTool

Outline

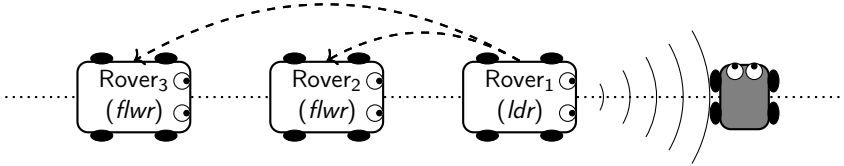
Rover #1. SPARTA platoon



Update messages from the leader

- Speed update messages

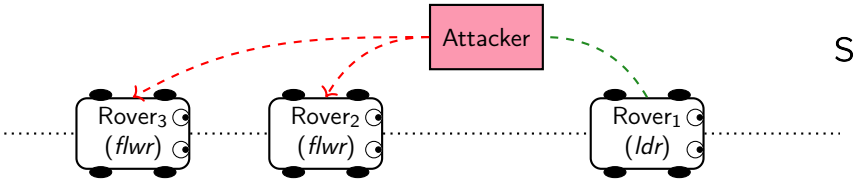
Rover #1. SPARTA platoon



Update messages from the leader

- Speed update messages
- Emergency brake message if an obstacle is detected

Rover #1. SPARTA platoon

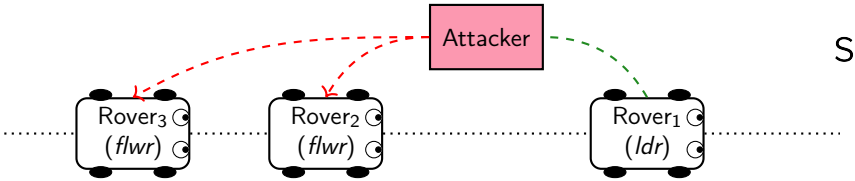


Attack scenarios

att1 speed $\leftarrow$ legitimate speed $\times$ 1.2

att2 speed $\leftarrow$ legitimate speed $\times$ 5

Rover #1. SPARTA platoon



Attack scenarios

att1 speed $\leftarrow$ legitimate speed $\times$ 1.2

att2 speed $\leftarrow$ legitimate speed $\times$ 5

Countermeasures

c1 plausibility check: $|\frac{speed}{mean}| \overset{?}{<} 1.3$

c2 symmetric encryption and nonce

Outline

Rover #2. Context: disasters

- Disaster means chaotic scenario
- Lives in danger → time matters
  - Chance to survive strongly decreases after 72 h

Rover #2. Problematic and our proposal

Mission

- Intervention in large devasted areas
  - Global and quick mapping
- Detection of victims
  - Use of EM from personal objects
  - GPR — Ground Penetration Radar
- Handling of hostile environments
  - Fire, heat, water. . . and attackers!

Our idea: rover with (fast) mission-configurable payload

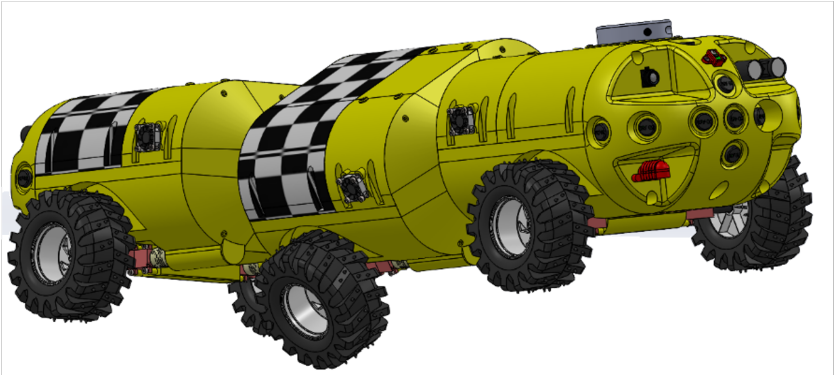
- Autonomous
- Many positioning sensors (Optical, IR, sonars, etc.)
- Electromagnetic features (radars, including GPR)

TECHNISCHE UNIVERSITÄT CHEMNITZ

Prof. Madhu Chandra

Rover #2. Let's welcome ArcTurius!

- **Modular**
- **Configurable payload**
  - Configurable slots for custom sensor
- **Embedded power**: from 1 to 3 kWh
- **Weight**: 10 kg for classical configuration, up to 15 kg

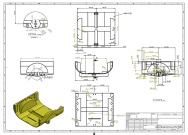


Rover #2. Typical sensors

- Inertial unit
- Temperature, pressure, humidity
  - Internal (LiPo, motors), external (environment)
- Magnetometer
- Surroundings capture (LIDAR, Sonar, camera, etc.)
- Wheel rotation control for better traction control
  - 3592 ticks per wheel revolution, 2 encoders per wheel
- Power consumption tracking
- Attitude (anti-overturn control)
- ...

Rover #2. Design approach

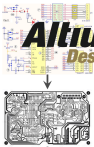
3D design



Mechanical Validation

3D Print

HW design



Embedded system

SW design

SysML Model

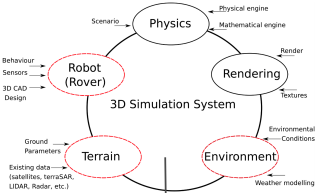
Safety &Cyber-Security verification

Code Generation

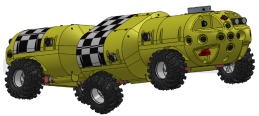
C/C++

Supervisory SW

System Simulation

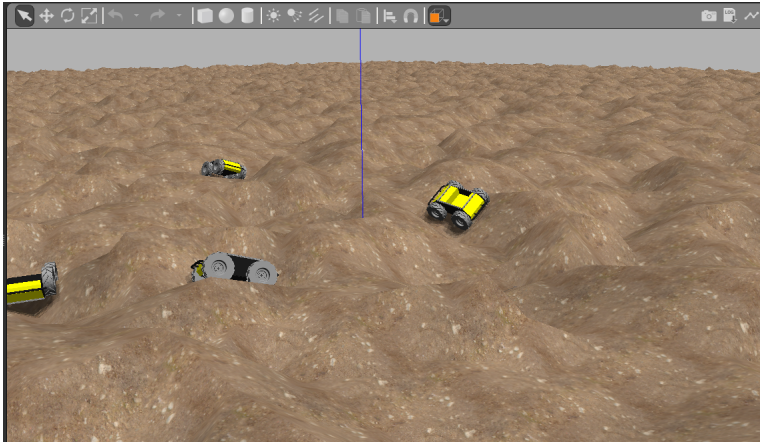


Configuration



Mission-specific system

Rover #2. Design approach (Gazebo)



Tullio Tanzi, Matteo Bertolino. 3D Simulation to Validate Autonomous Intervention Systems Architecture for Disaster Management. 4th International Conference on Information Technology in Disaster Risk Reduction (ITDRR), Oct 2019, Kyiv, Ukraine. pp.196-211.

Outline

TELECOM Paris

IP PARIS

Will my rovers be attacked?

Yes!

Cyber-criminals target all systems of interest

- Pranggono, B, Arabo, A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters. 2021; 4:e247.
  This paper emphasizes that there is a correlation between the pandemic and the increase in cyber-attacks targeting sectors that are vulnerable.
- Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care. 2021 Feb 20;33(1):mzaa117.
  . . . cyber-attacks during COVID-19, recognizing that a growing number of cyber-criminals are seeking to capitalize on the vulnerabilities of the healthcare sector during this period . . .

Typical safety and security properties

Safety

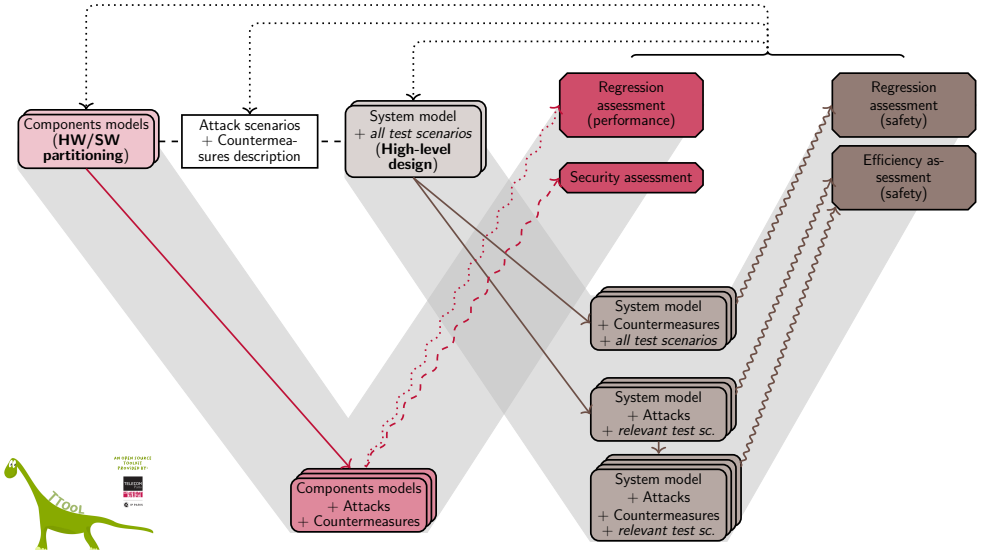
- Resilience to external event
- Mission fulfilment without extra damages and casualties
  - Internal, external
- Absence of deadlocks, livelocks
- Variables always in their definition domain
- ...

Cyber-security

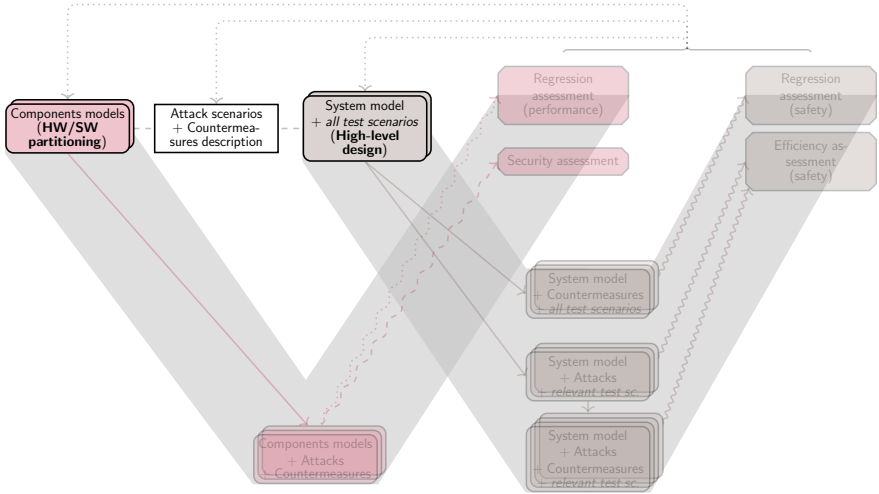
- Man-in-the-Middle between control station and robots, or between robots
- DoS
- Ransomware
- Environment manipulation
- Spying on confidential data
- ...

Yaacoub, JP.A., Noura, H.N., Salman, O. et al. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 21, 115–158 (2022).

W-Sec: a method to design safe and secure systems



W-Sec, 1/4: modeling



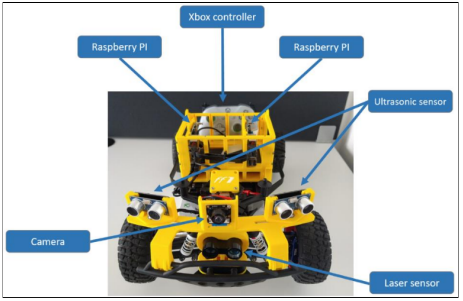
W-Sec, 1/4: models

Modeled system

A swarm of Fortiss rovers

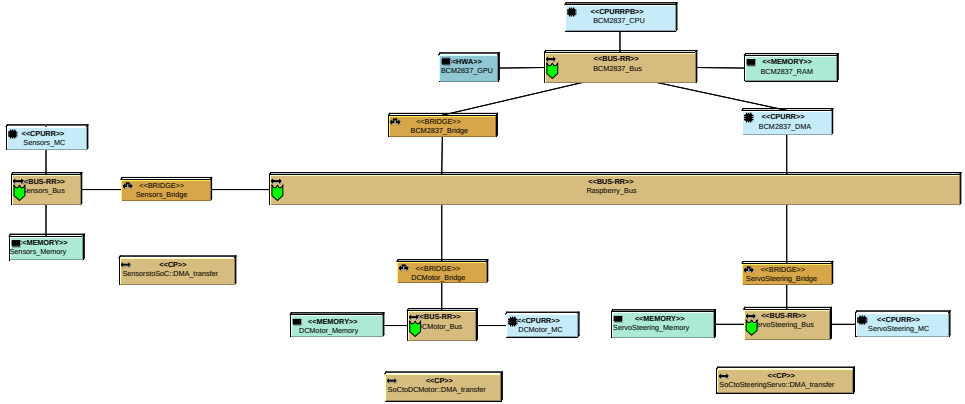
Chosen modeling granularity

- **Components**: rovers, with a focus on the Raspberry Pi executing the algorithms
  - Hardware components
  - Communications between components
  - Application components
- **System**: platoon

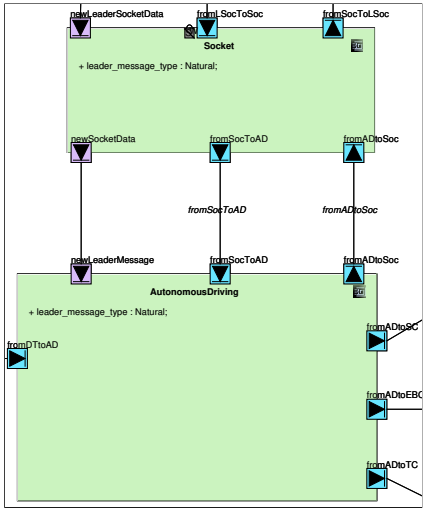


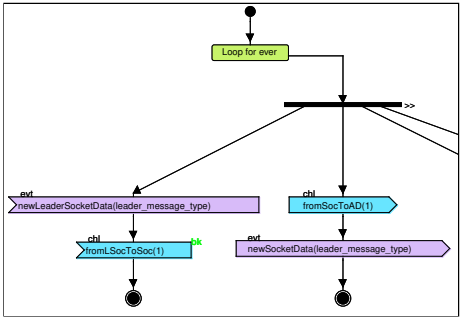
Credits: Fortiss, SPARTA deliverable D5.2

W-Sec, 1/4: modeling

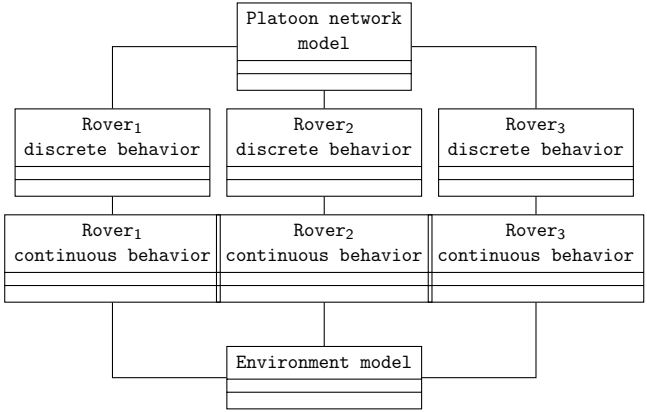


W-Sec, 1/4: modeling



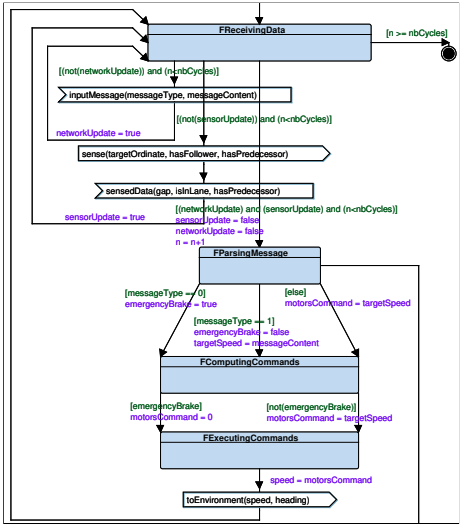


W-Sec, 1/4: modeling



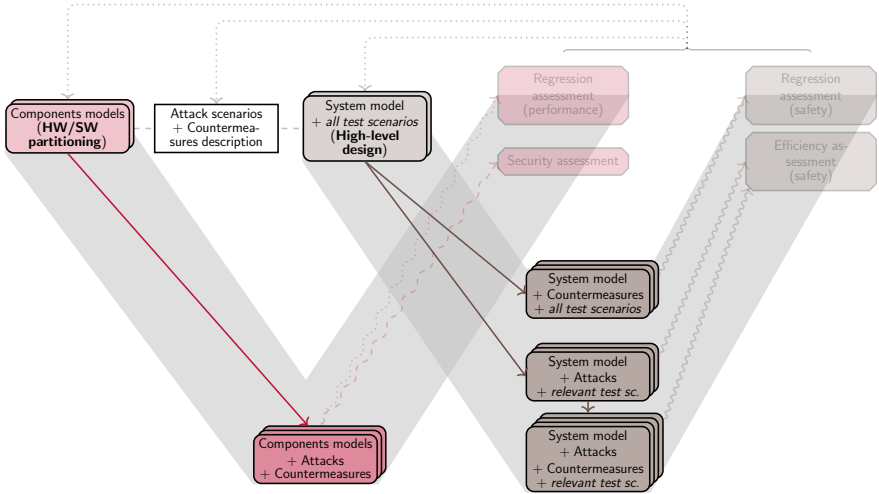
- SysML-Sec blocks
- Associations depict port connections and signal associations
- Software and dynamics blocks instantiate SysML-Sec librairies

W-Sec, 1/4: modeling

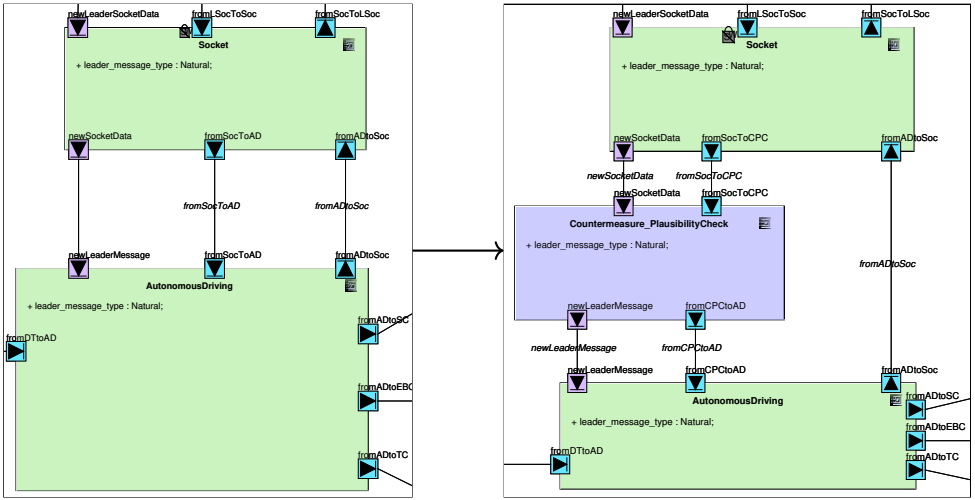


- High-level behavior
- Follower:
  - HSW view: 10 blocks
  - System view: 2 blocks

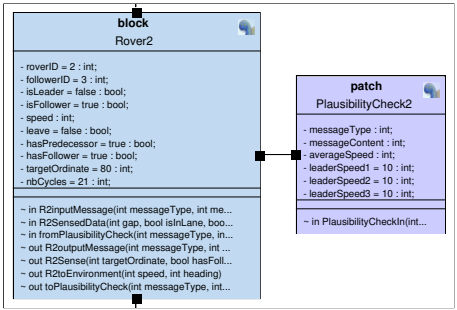
W-Sec, 2/4: enriching the models

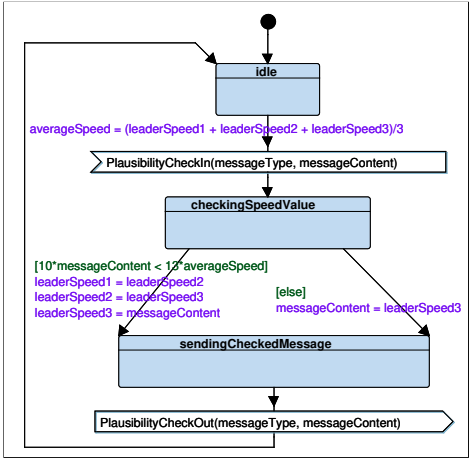


W-Sec, 2/4: enriching the models

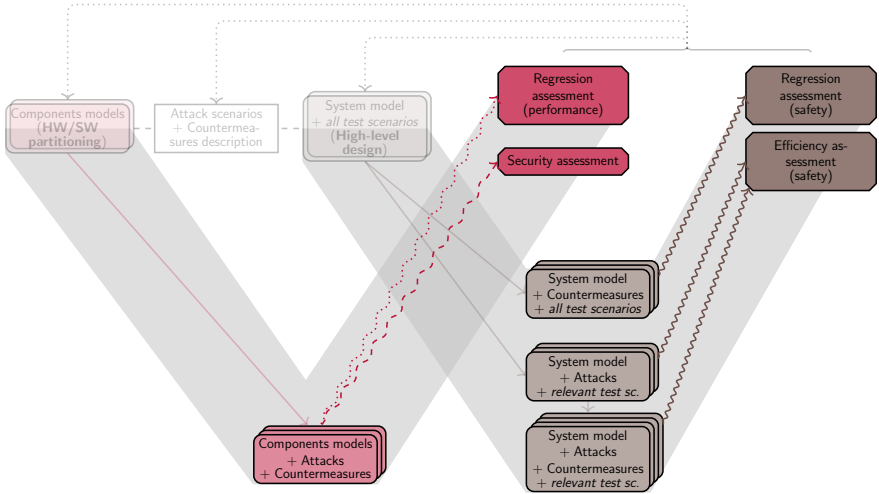


W-Sec, 2/4: enriching the models





W-Sec, 3/4: assessing the countermeasures



W-Sec, 3/4: assessing the countermeasures

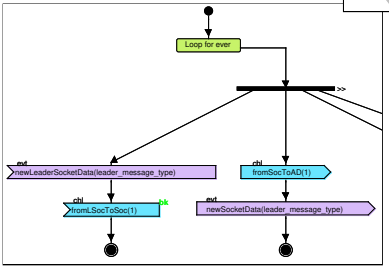
Three kinds of assessments

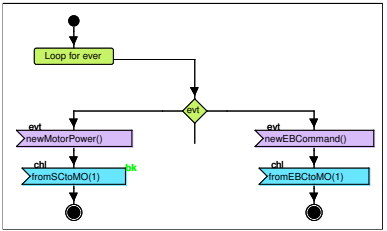
- Performance of the targeted component(s)
  - Simulation with TTool internal simulator, HSW view
- Security of the targeted component(s)
  - Formal verification with ProVerif, HSW view
- Safety at system level
  - Formal verification with TTool internal model checker, System view

W-Sec, 3/4: assessing the countermeasures

Performance assessment

- Two breakpoints in the activity diagrams, placed at the input/output actions of the targeted application(s)
- The "difference" between the elapsed times at bp no. 2 and bp no. 1 enables to evaluate the computational overhead





W-Sec, 3/4: assessing the countermeasures

Countermeasures (reminder)

c1 plausibility check: $|\frac{speed}{mean}| \overset{?}{<} 1.3$

c2 symmetric encryption and nonce

W-Sec, 3/4: assessing the countermeasures

Countermeasures (reminder)

- c1 plausibility check: $|\frac{speed}{mean}| \overset{?}{<} 1.3$
- c2 symmetric encryption and nonce

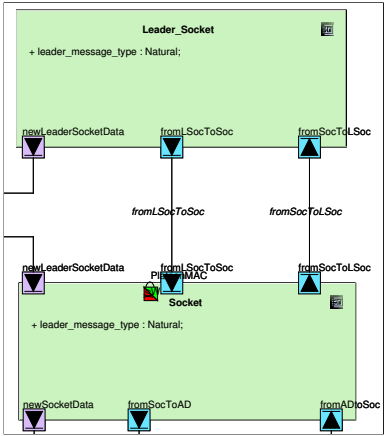
Simulation results

- no 274 ns
- c1 357 ns (+**30%**)
- c2 646 ns (+**136%**)

W-Sec, 3/4: assessing the countermeasures

Security assessment

- "Ask" ProVerif to check security properties on selected data channels of the targeted application
- Evaluate the integrity, authenticity and confidentiality of sensitive data
- Evaluate if the countermeasures targeting data security are properly implemented



W-Sec, 3/4: assessing the countermeasures

Countermeasures (reminder)

c1 plausibility check: $|\frac{speed}{mean}| \overset{?}{<} 1.3$

c2 symmetric encryption and nonce

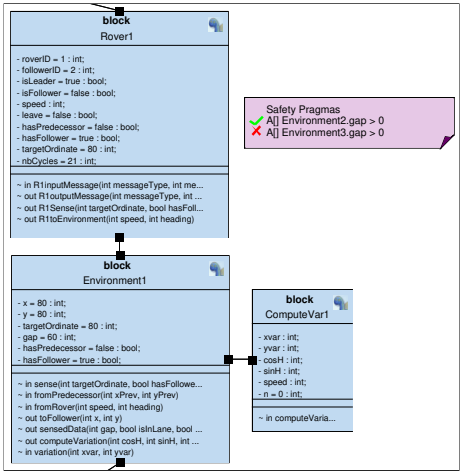
Verification results

Contermeasure \ *Property*	*Weak auth.*	*Strong auth.*
No countermeasure	✗	✗
c1	✗	✗
c2	✓	✓

W-Sec, 3/4: assessing the countermeasures

Safety assessment

- Evaluate the liveness/reachability of properties defined by the user
- CTL* queries (+ observer blocks if needed)
- Evaluate the safety regression/recovery induced by the countermeasures at system level



W-Sec, 3/4: assessing the countermeasures

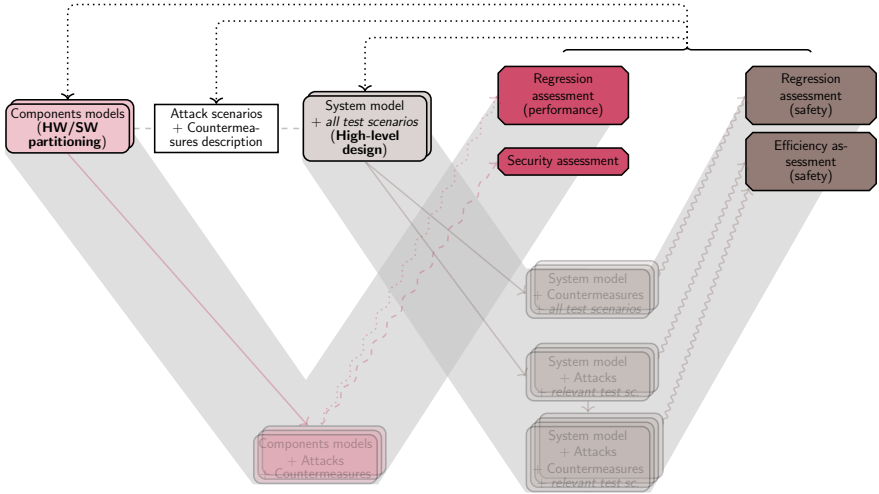
Checked property

A[] Rover_1.x-Rover_2.x > 0 && Rover_2.x-Rover_3.x > 0

Verification results

Countermeasure \ Attack	No att.	att1	att2
No countermeasure			
c1			
c2			

W-Sec, 4/4: feedback

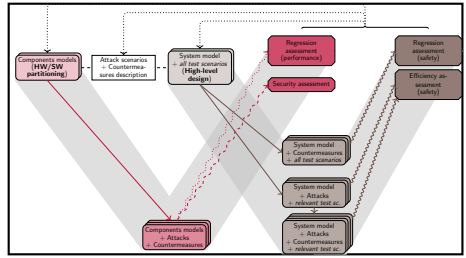


Outline

Conclusions (1/3)

W-Sec

- Method for safe and secure systems
- Successfully applied to two systems
  - An existing system (Fortiss rovers)
  - A system under development (ArcTurius)
- Vulnerabilities identified and patched
- Based on SysML-Sec and TTool: ready-to-use

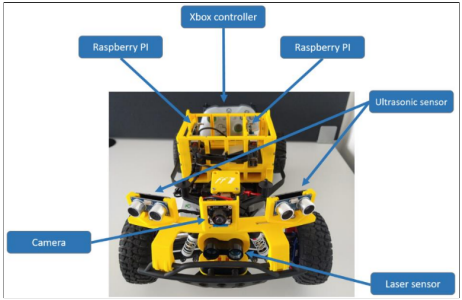


Conclusions (2/3)

SPARTA Case-study

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

W-Sec helps comparing countermeasures



Credits: Fortiss, SPARTA report D5.2

Conclusions (3/3)

Future Works

- Automate the models enrichment task (mutations)
- Investigate the links between HSW and System views
- Design comparison metrics
- Evaluate W-Sec on other case studies
- ArcTurius in action!

Questions?

Download TTool!

- http://ttool.telecom-paris.fr/

- *B. Sultan, L. Apvrille, P. Jaillon, "Safety, Security and Performance Assessment of Security Countermeasures with SysML-Sec", in the Proceedings of the 10th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2022).*
- *T. Tanzi, L. Apvrille, "3D Simulation for Disaster Management: toward a new approach", Proceedings of the 3rd URSI Atlantic / Asia-Pacific Radio Science Meeting, Maspalomas, Spain, May-June 2022.*