Une école de l'IMT

SysML Model Transformation for Safety and Security

Florian Lugou, Rabéa Ameur-Boulifa,
Ludovic APVRILLE
ludovic.apvrille@telecom-paristech.fr

université PARIS-SACLAY

ISSA'2018 - Barcelona

Outline

Examples of Threats

Transport systems

- Use of exploits in Flight Management System (FMS) to control ADS-B/ACARS [Teso 2013]
- Remote control of a car through Wifi [Miller 2015] [Tecent 2017]

(C) Wired - ABC News

Medical appliances

- Infusion pump vulnerability, April 2015. http://www.scip.ch/en/?vuldb.75158

(C) Hospira

How to Identify Vulnerabilities?

Investigations

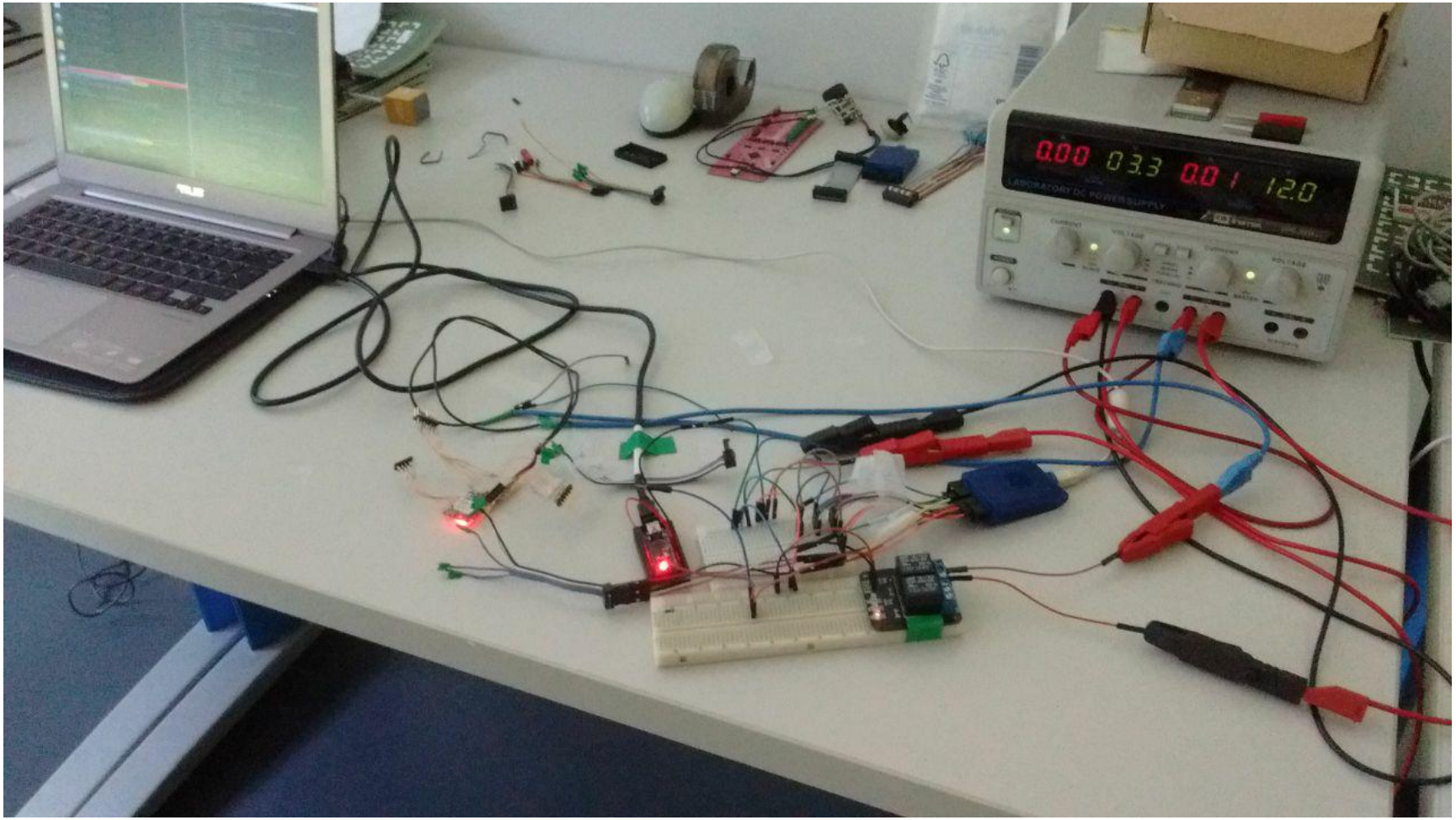
- Testing ports (JTAG interface, UART, . . .)
- Firmware analysis
- Memory dump
- Side-channel analysis (e.g. power consumption, electromagnetic waves)
- Fault injection
- . . .

Secure your systems!

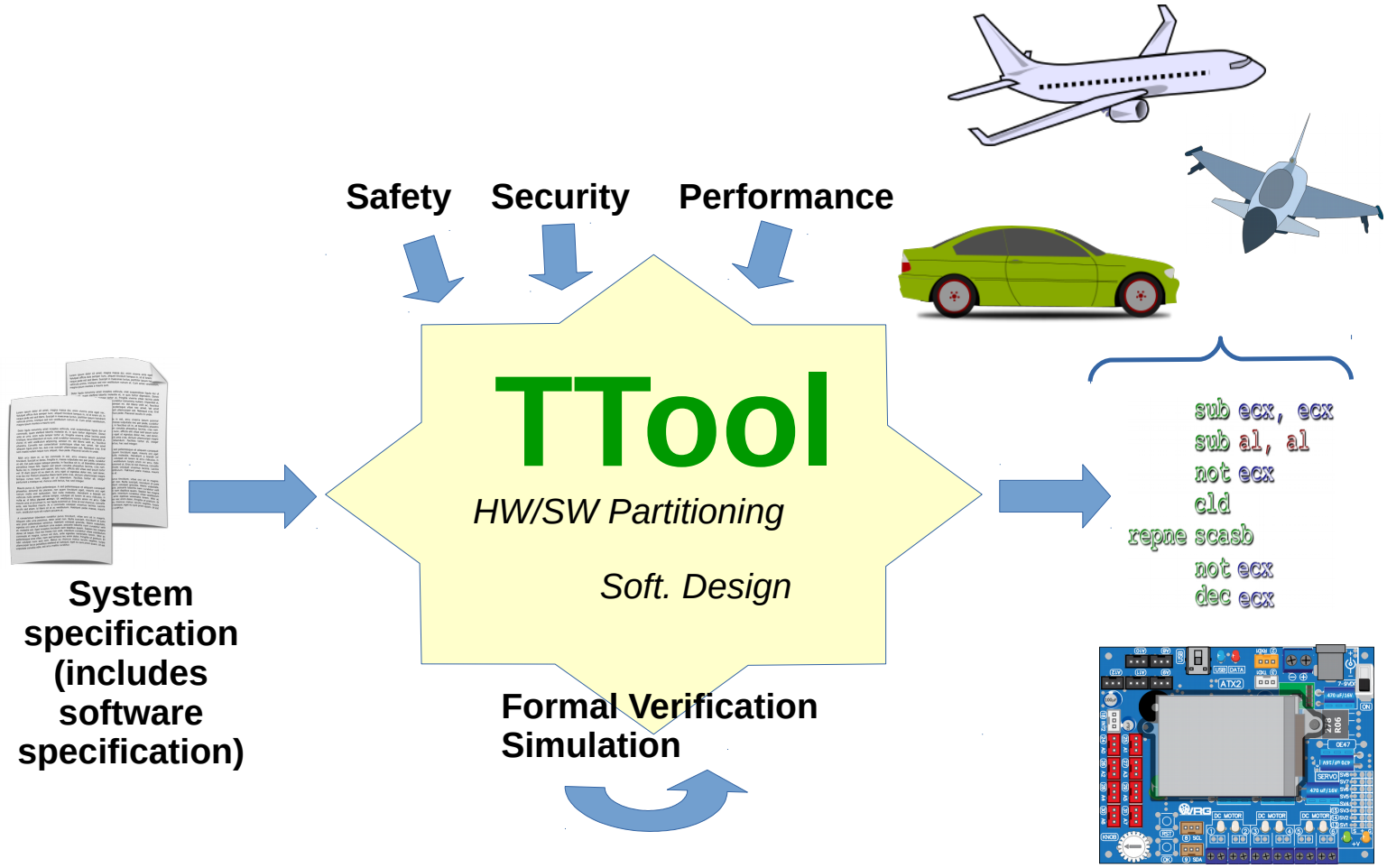
Develop your system with security in mind from the very beginning

Our solution: SysML-Sec, supported by TTool

Firmware Dumping



Goal: Designing Safe and Secure Embedded Systems



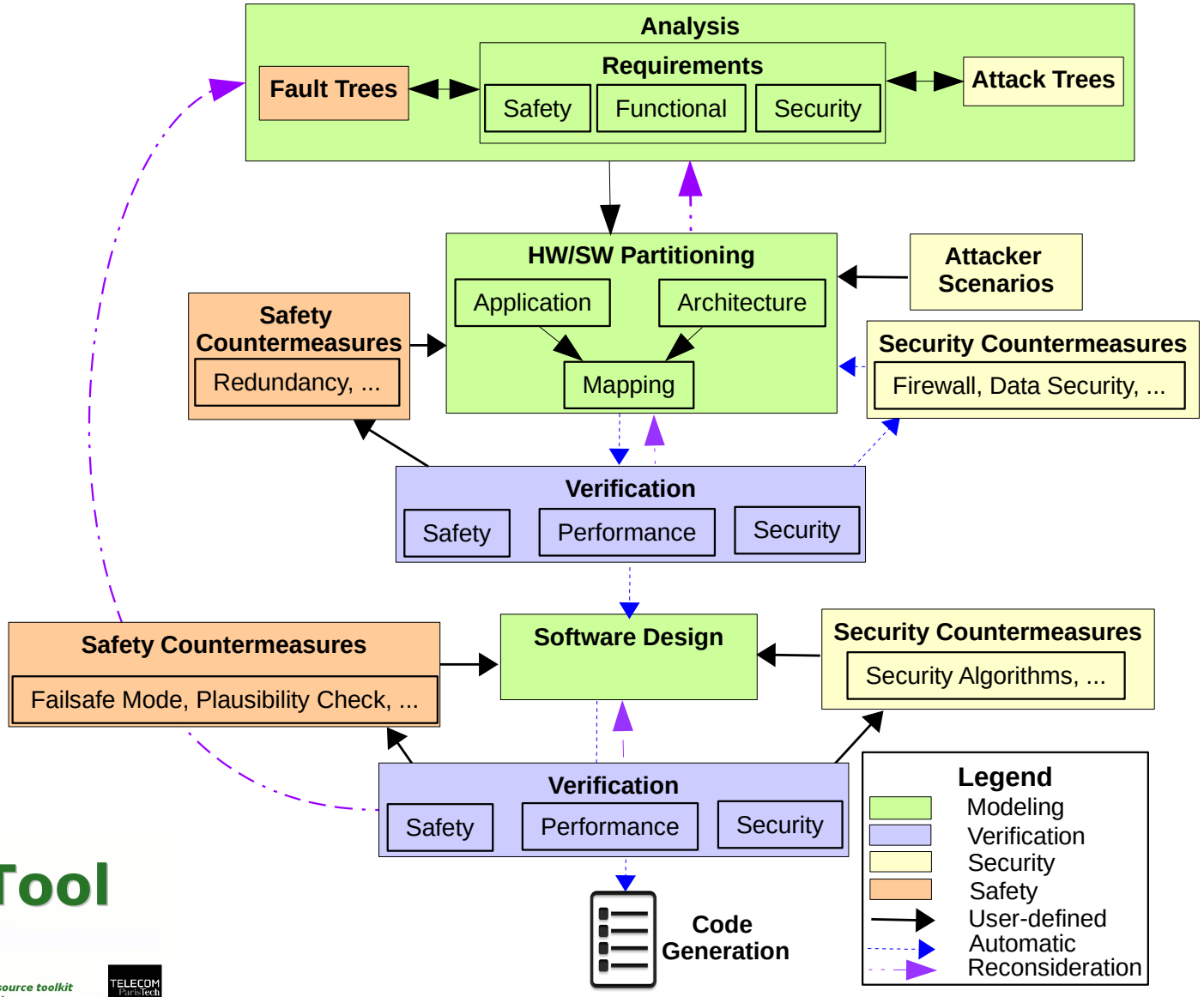
TTool: Key Features

- Model-Driven Engineering tool
- Free and Open-Source
  - Plug-in can be used to insert private/commercial features
- Easy to use
- **Focus on safety, security and performance**
- **Formal verification at the push of a button**

SysML-Sec

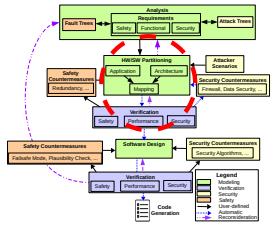
Common issues (addressed by SysML-Sec):

- Adverse effects of security over safety/real-time/performance properties
  - Commonly: only the design of security mechanisms
- Hardware/Software partitioning
  - Commonly: no support for this in tools/approaches in MDE and security approaches



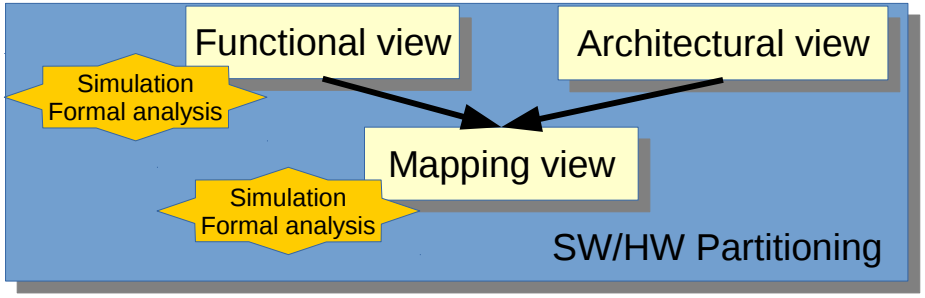
Fully supported by TTool

Partitioning



Before mapping

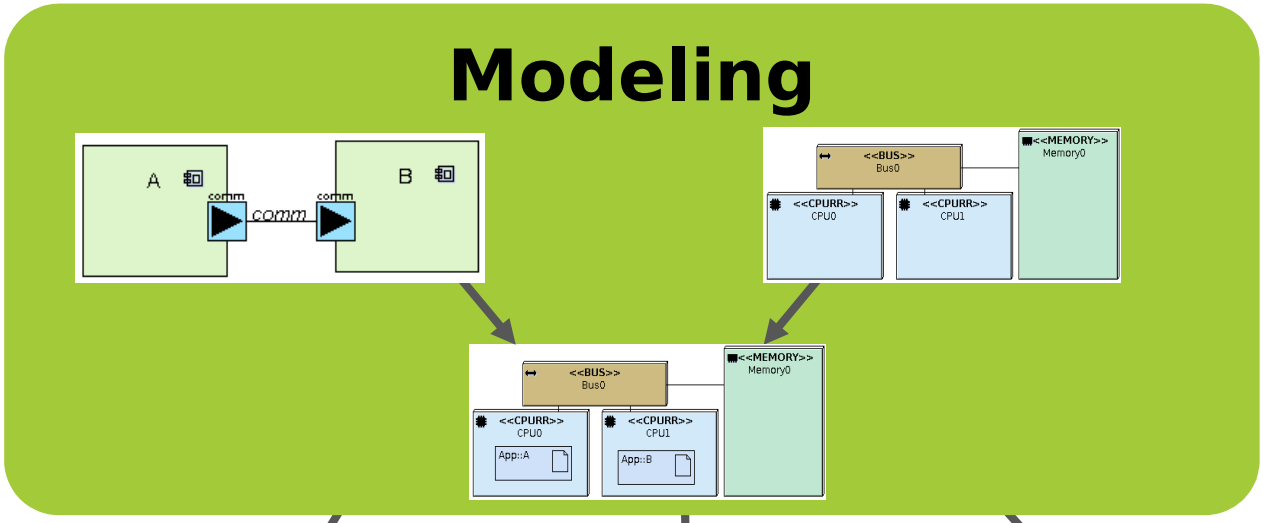
- Security mechanisms can be captured but not verified



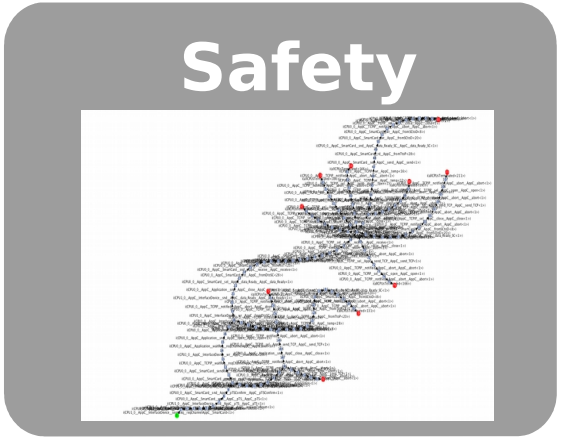
After mapping

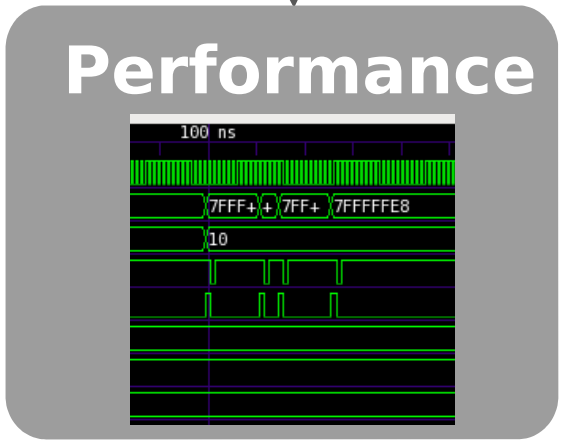
- Verify security (confidentiality, authenticity) according to attacker capabilities
  - Whether different HW elements are or not on the same die
  - Where are stored the cryptographic materials (keys)
  - Where are performed encrypt/decrypt operations
- Impact of security mechanisms on performance and safety
  - e.g. increased latency when inserting security mechanisms

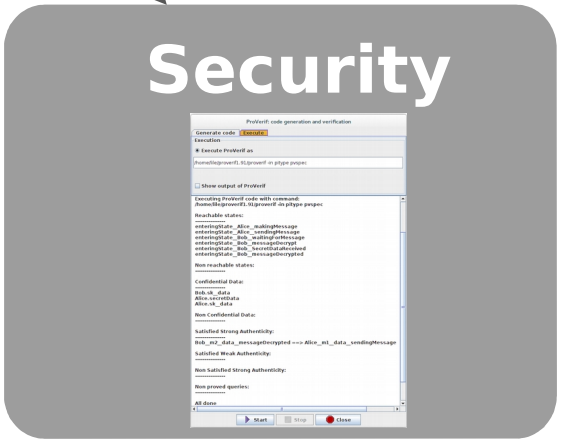
Partitioning Verification



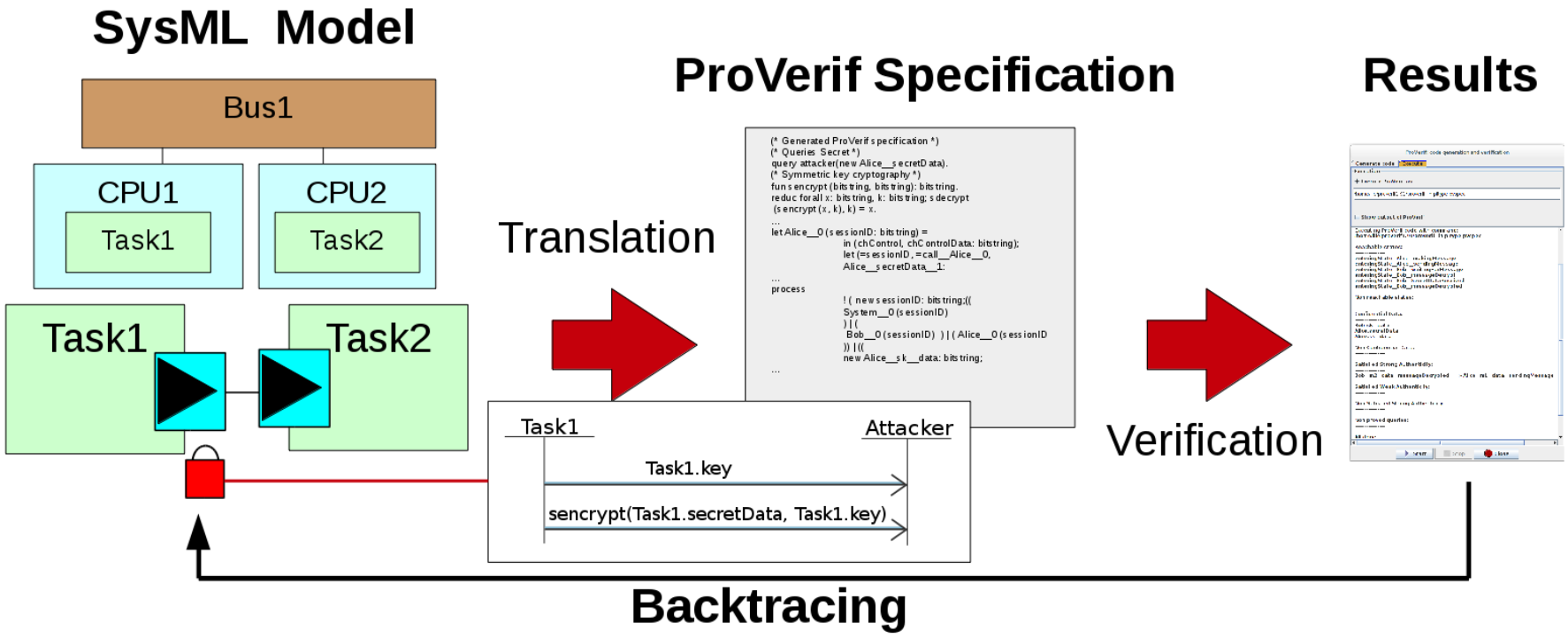
Automatic Verification







Security Verification



Automated Proverif Specification Generation

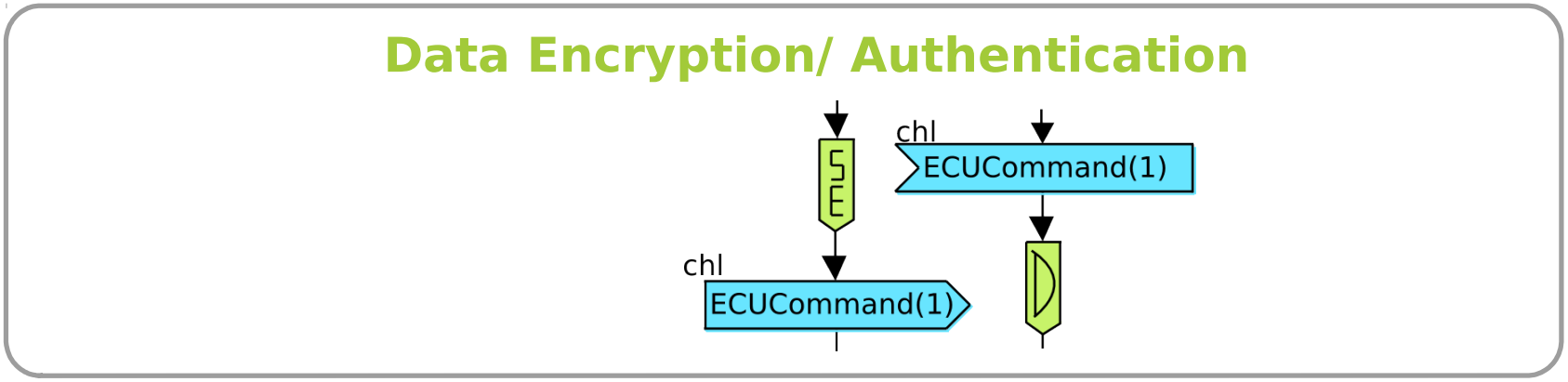
- Main idea
  - Decompose SysML-Sec behaviors into a set of *basic blocks*
  - Generate Proverif code
- The semantic function for generating the code:
  - Processes generation

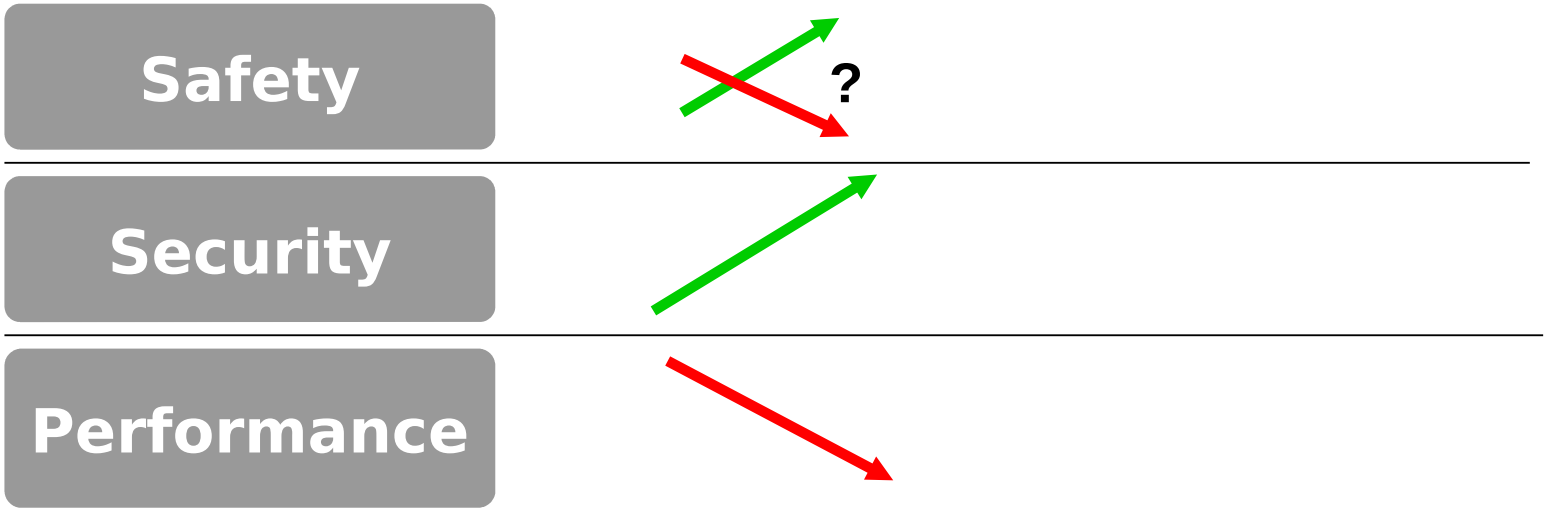
$$[\![.]\!]^{p}_{\mathcal{E}} : \mathit{Basic\_block} \rightarrow \mathit{Proverif\_process}$$

  - Main process generation

$$[\![.]\!]_{\mathcal{E}} : \mathit{SysML\_components} \rightarrow \mathit{Proverif}$$

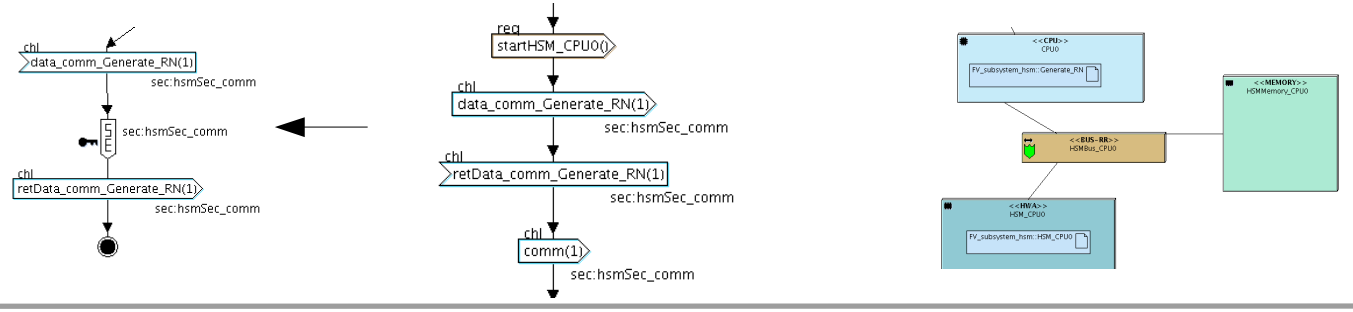
Safety and Security Mechanisms





Safety and Security Mechanisms (Cont.)

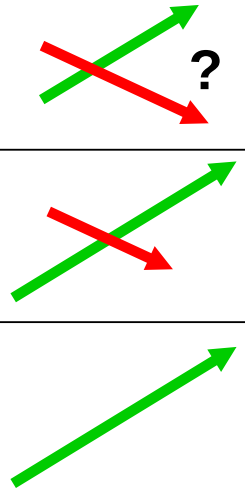
Data Security with Hardware Security Module



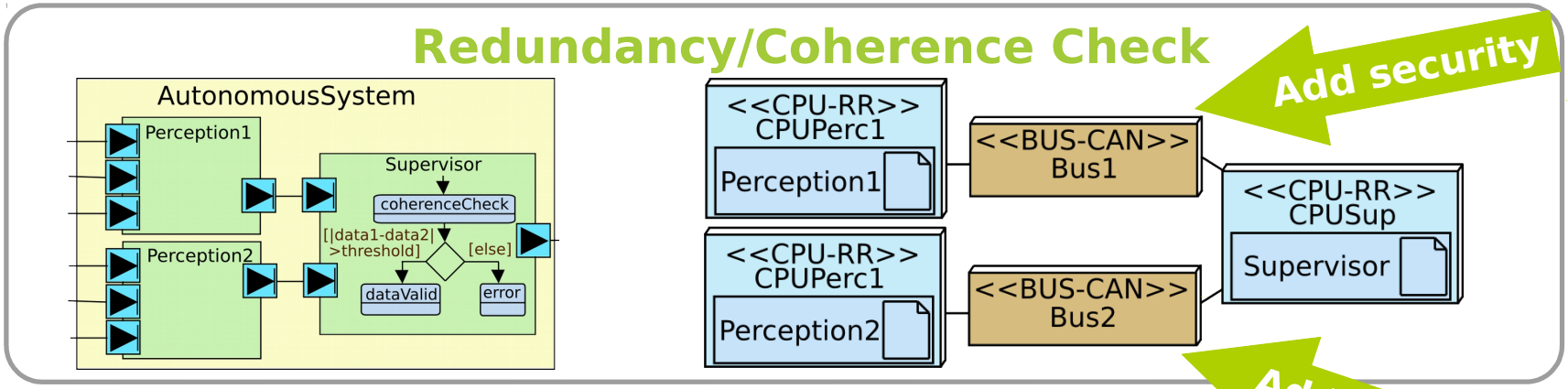
Safety

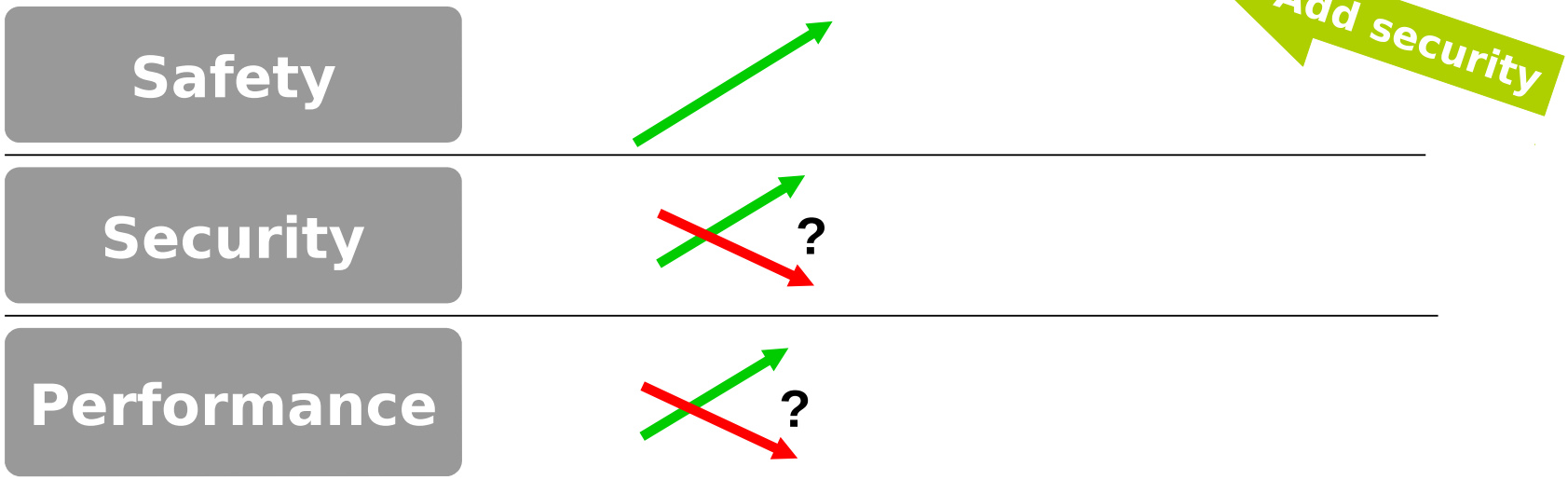
Security

Performance

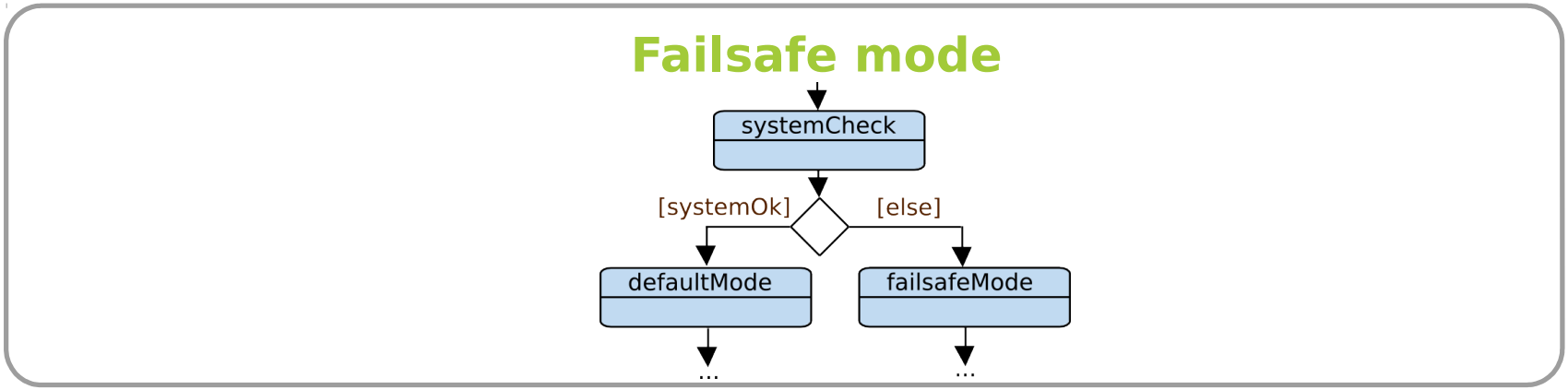


Safety and Security Mechanisms (Cont.)





Safety and Security Mechanisms

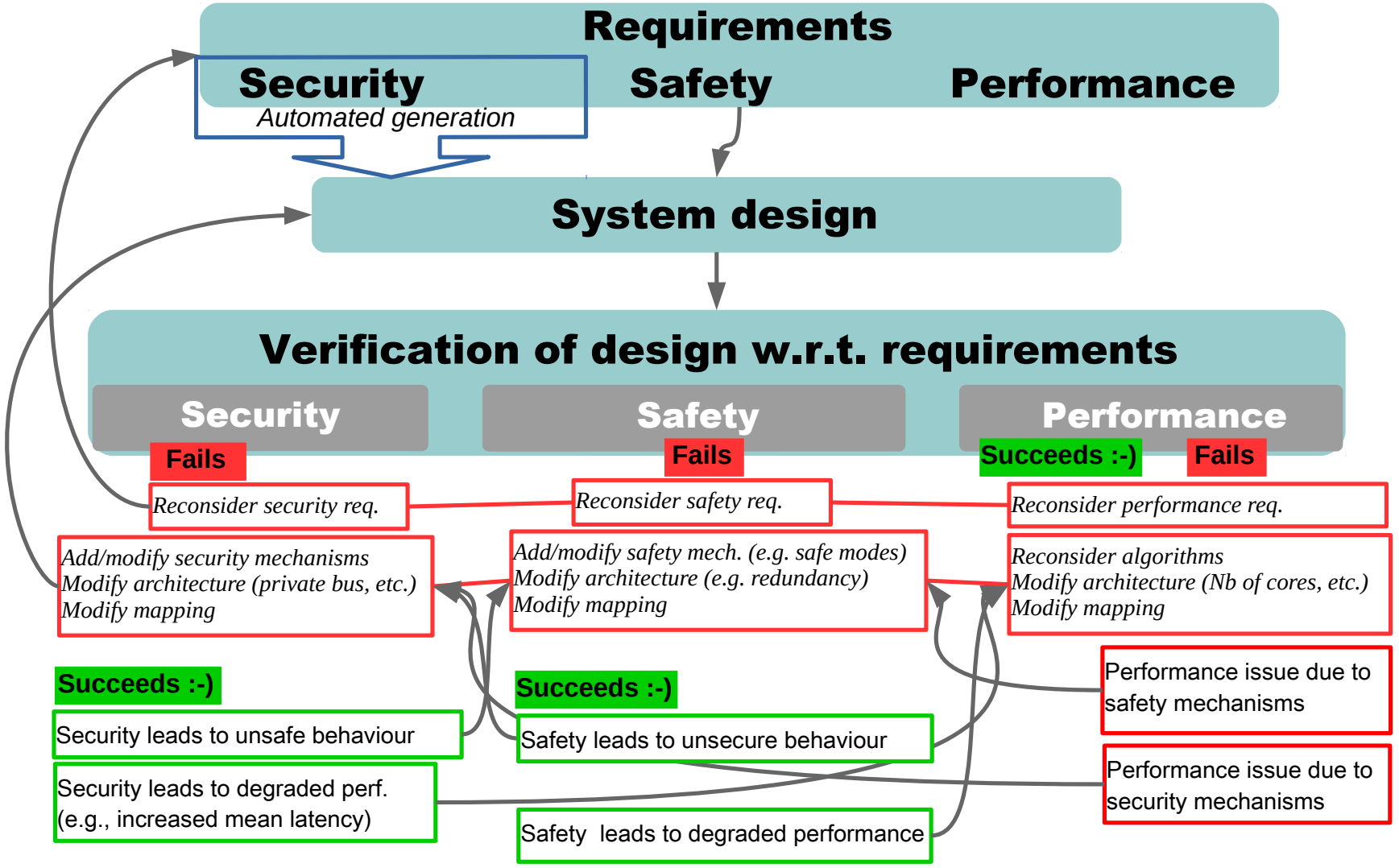


Safety

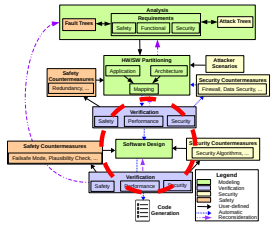
Security

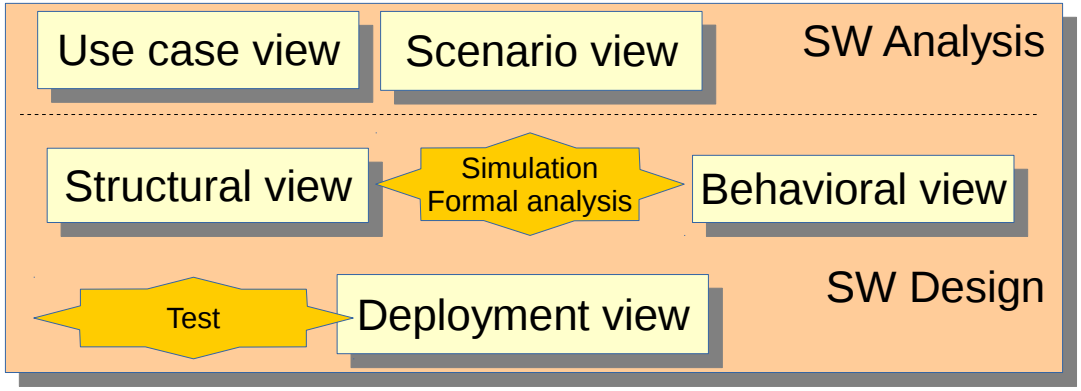
Performance

Safety/Security/Performance



SysML-Sec: SW Design





- Precise model of security mechanisms (security protocols)
- Proof of security properties : confidentiality, authenticity
- Channels between software blocks can be defined as private or public
  - This should be defined according to the hardware support defined during the partitioning phase

Case Studies

Cyber security of connected vehicles

- Safety/Security/Performance
- EVITA FP7 Partners: Continental, BMW, Bosch, ...
- VEDECOM

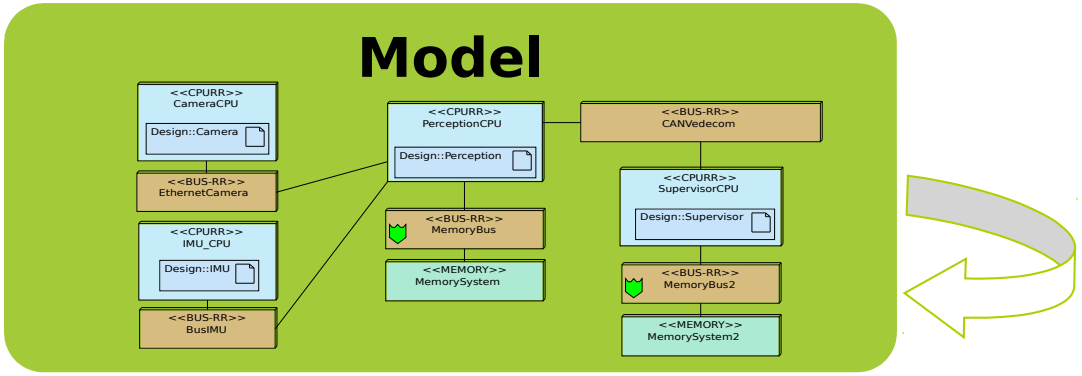
H2020 AQUAS

- Automated train sub-systems (ClearSy): Safety/Security/Performance
- Industrial Drives (Siemens): Safety/Security/Performance

Nokia

- Digital architectures for 5G networks (Safety/Performance)

Case Study: VEDECOM Autonomous Vehicle



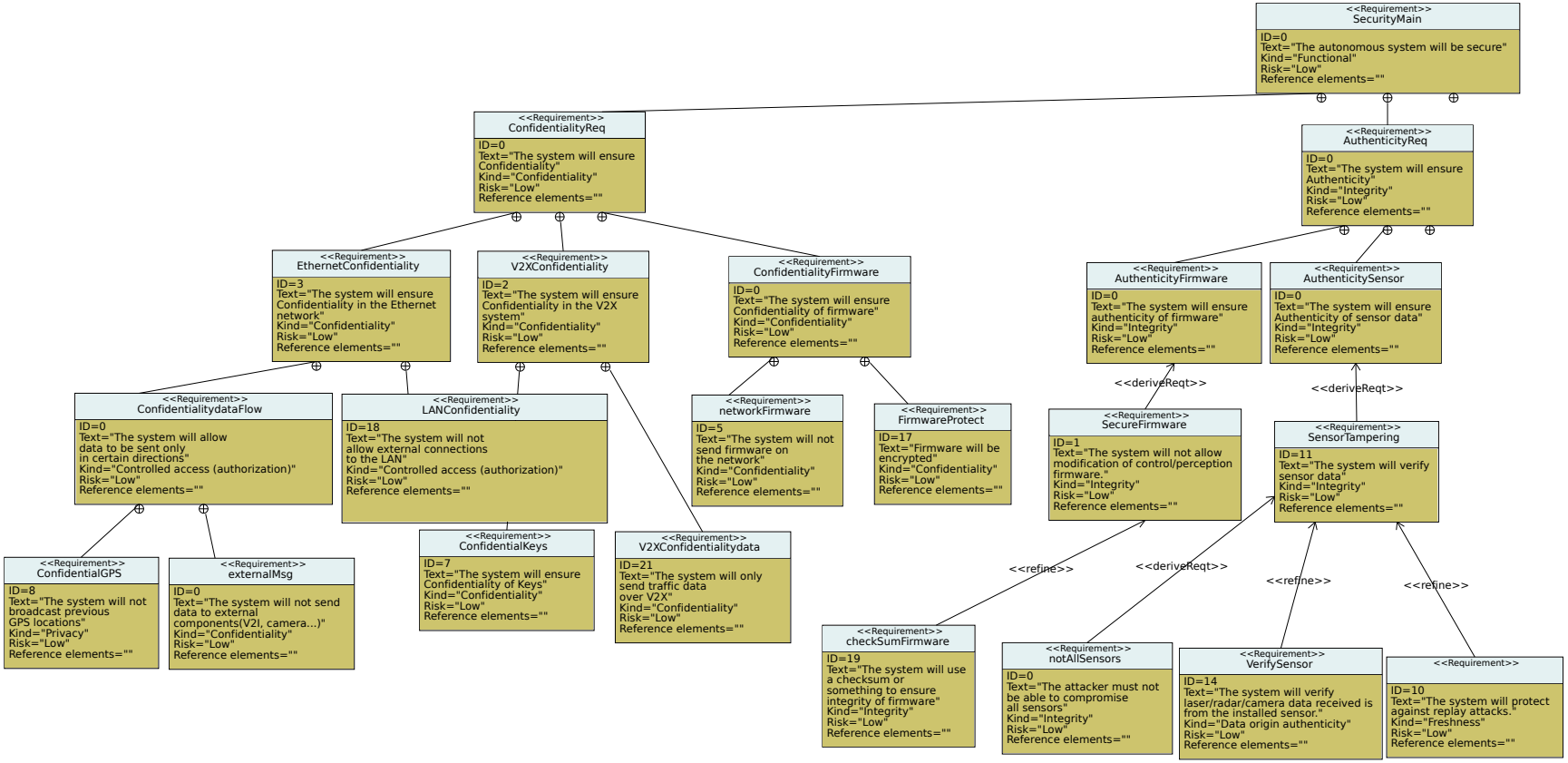
Verification

Tests

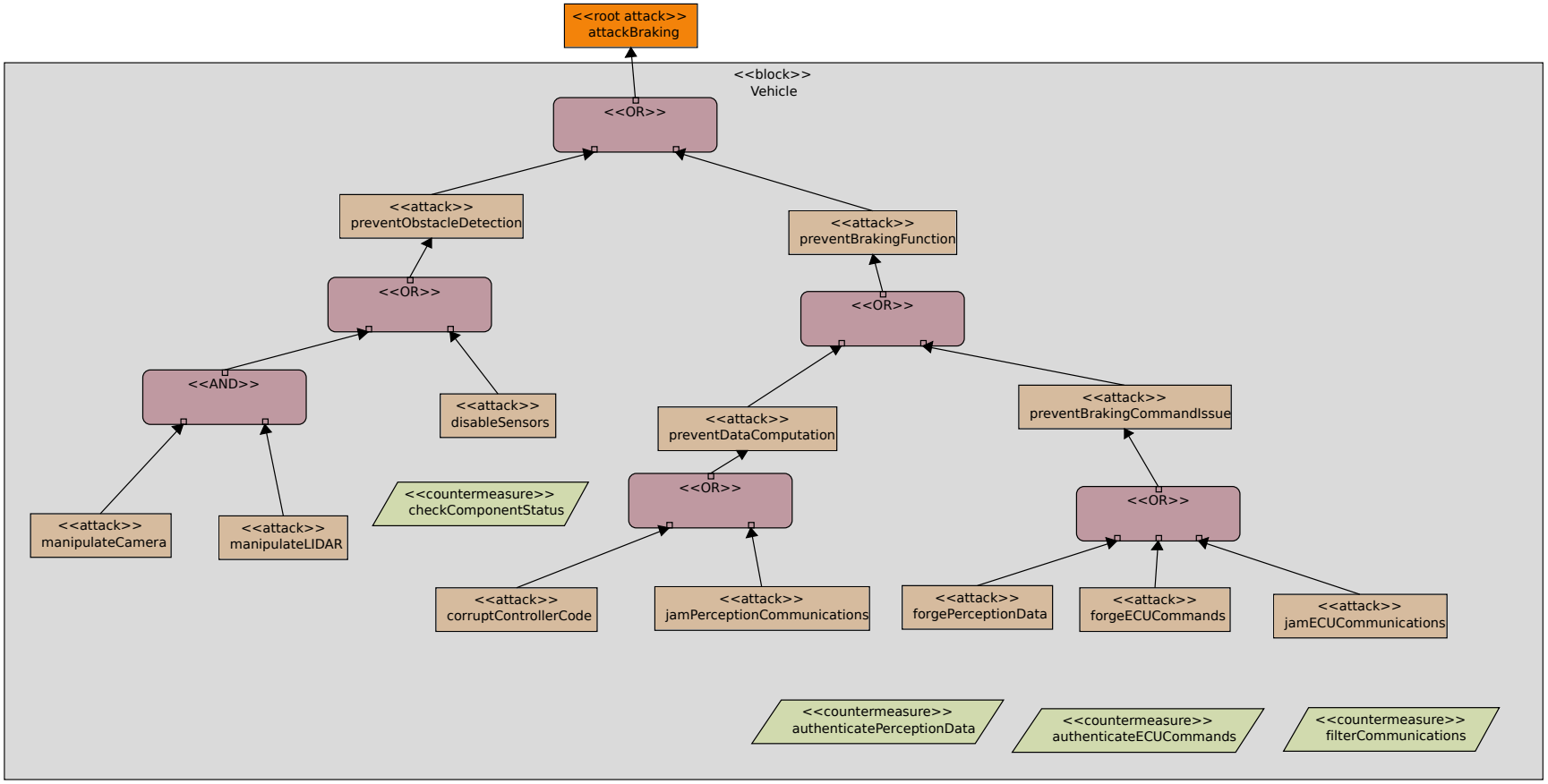
Constraints

- Standard: ISO26262
  - SOTIF: Safety Of The Intended Function
- Security: impact of potential attacks on safety

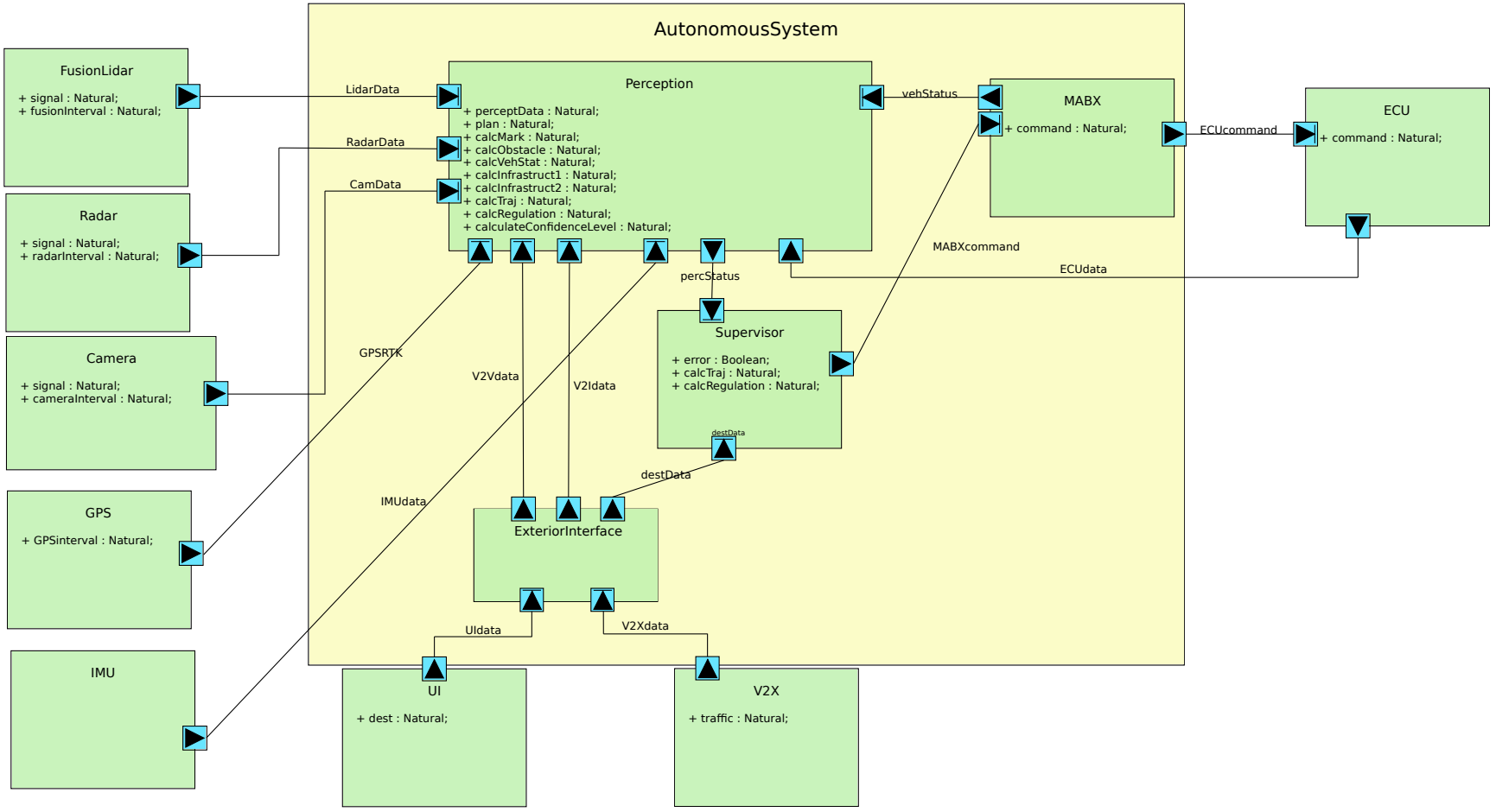
Requirements



Attacks

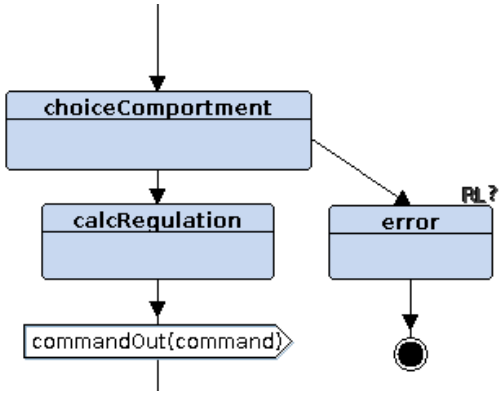

<<root attack>>
attackBraking
<<block>>
Vehicle
<<OR>>
<<attack>>
preventObstacleDetection
<<attack>>
preventBrakingFunction
<<OR>>
<<OR>>
<<AND>>
<<attack>>
disableSensors
<<attack>>
preventDataComputation
<<attack>>
preventBrakingCommandIssue
<<countermeasure>>
checkComponentStatus
<<OR>>
<<OR>>
<<attack>>
manipulateCamera
<<attack>>
manipulateLIDAR
<<attack>>
corruptControllerCode
<<attack>>
jamPerceptionCommunications
<<attack>>
forgePerceptionData
<<attack>>
forgeECUCommands
<<attack>>
jamECUCommunications
<<countermeasure>>
authenticatePerceptionData
<<countermeasure>>
authenticateECUCommands
<<countermeasure>>
filterCommunications

Functional View



Safety Verification (Before Mapping)

Reachability/Liveness

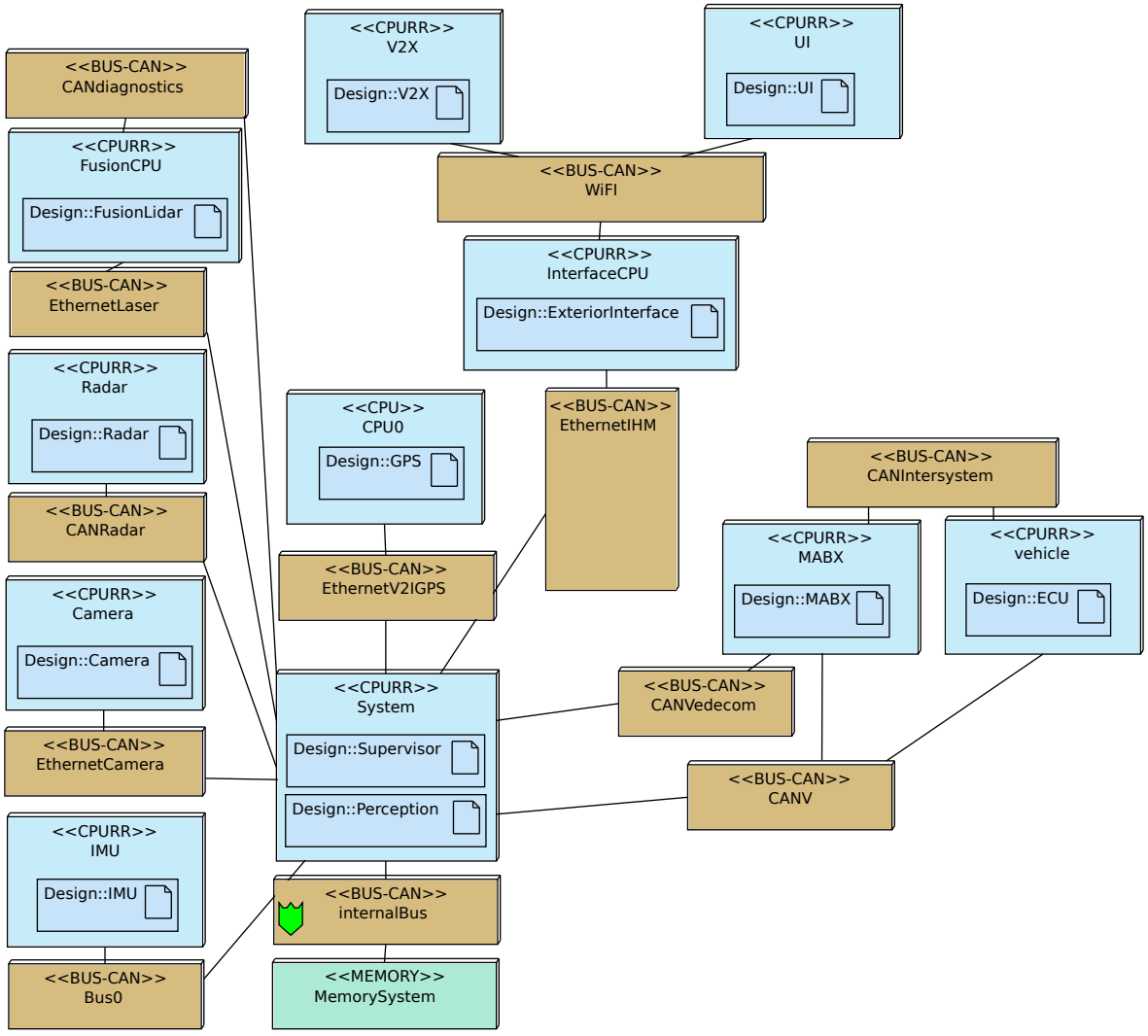


Queries

Safety Pragma

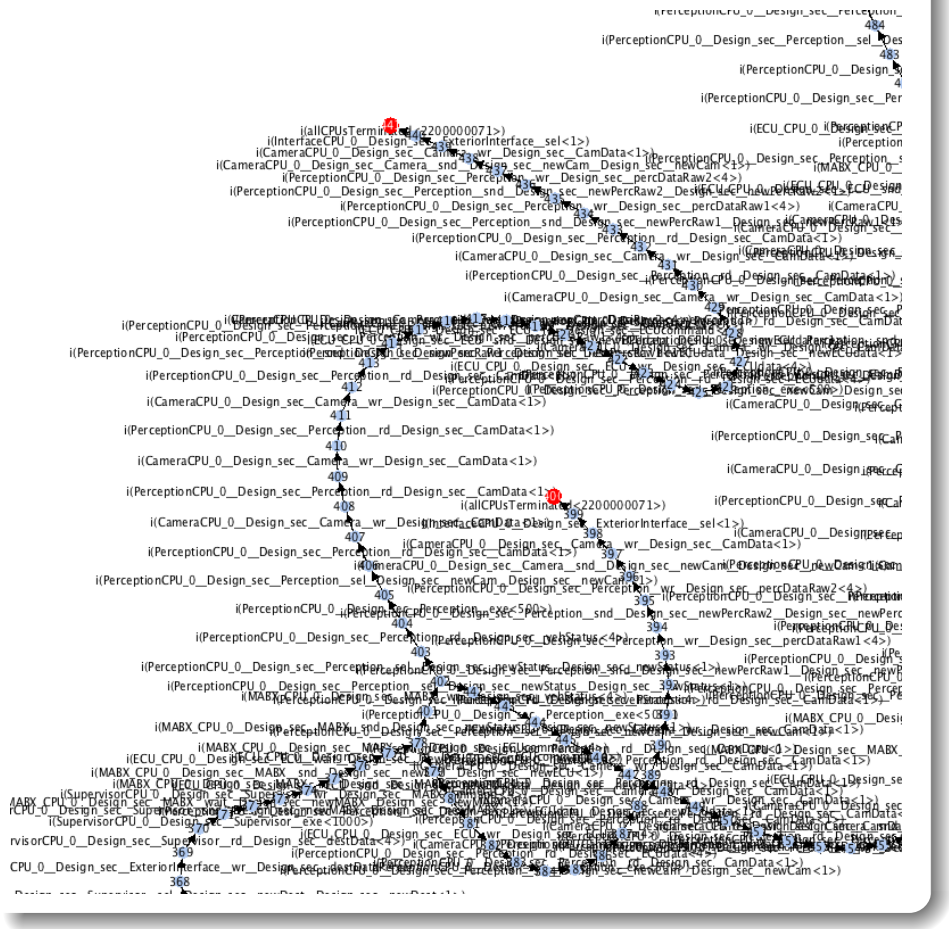
A[] Supervisor.running
Perception.distance<threshold -->
Supervisor.brakingOrder

Architecture and Mapping Views

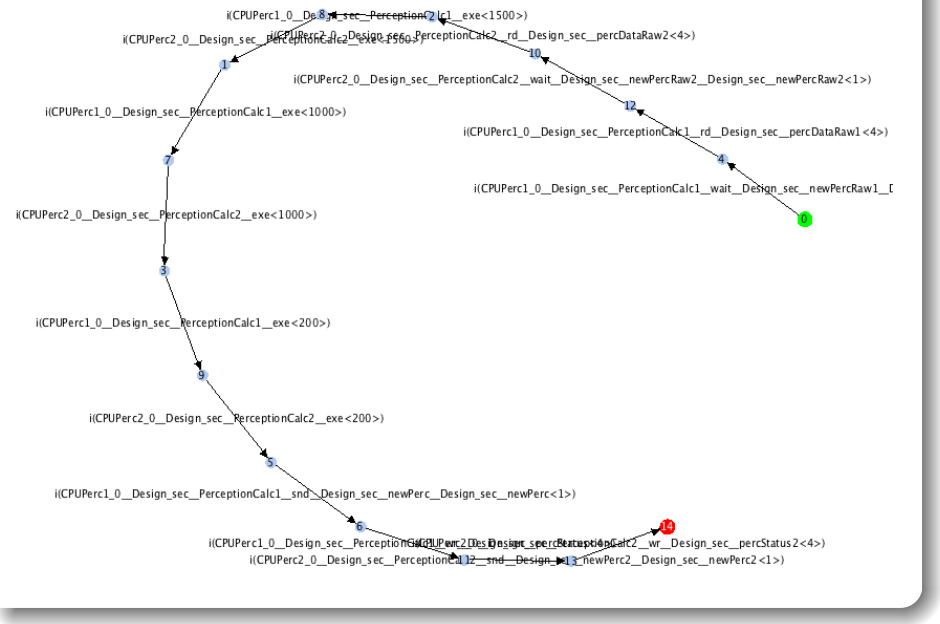


Safety Verification (After Mapping)

Reachability Graph

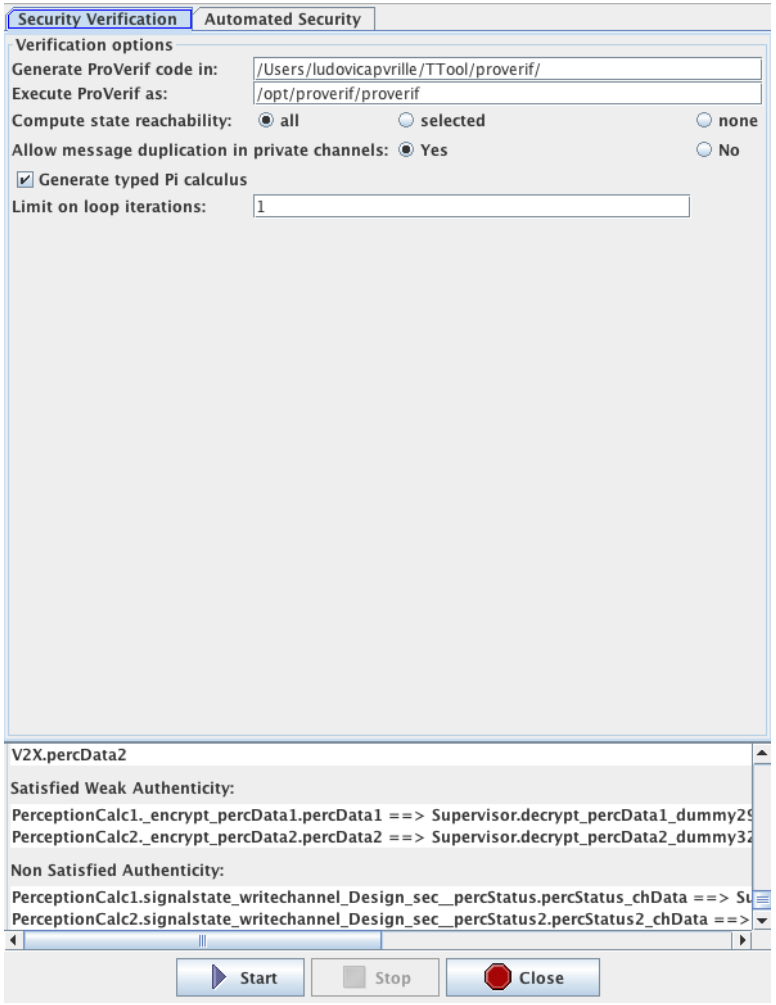


Minimized RG

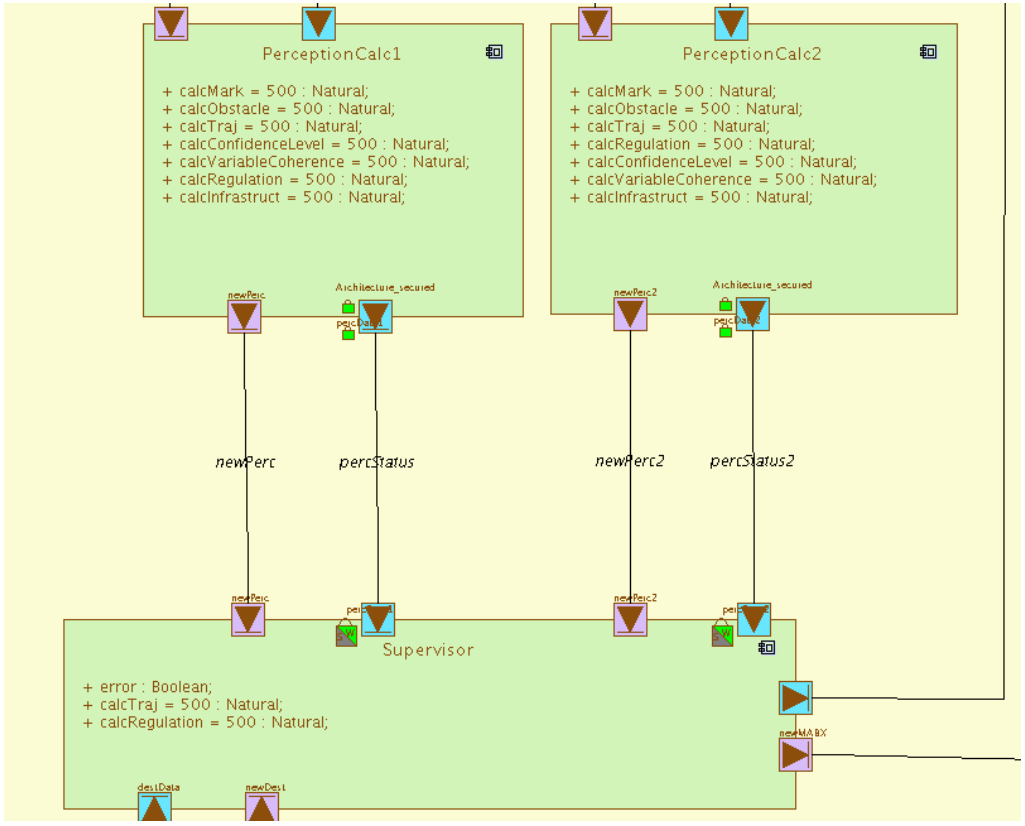


Security Verification

Dialog window

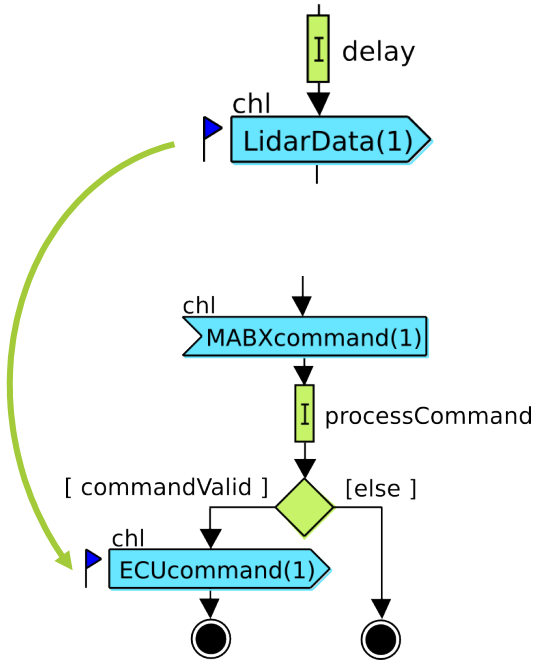


Backtracing

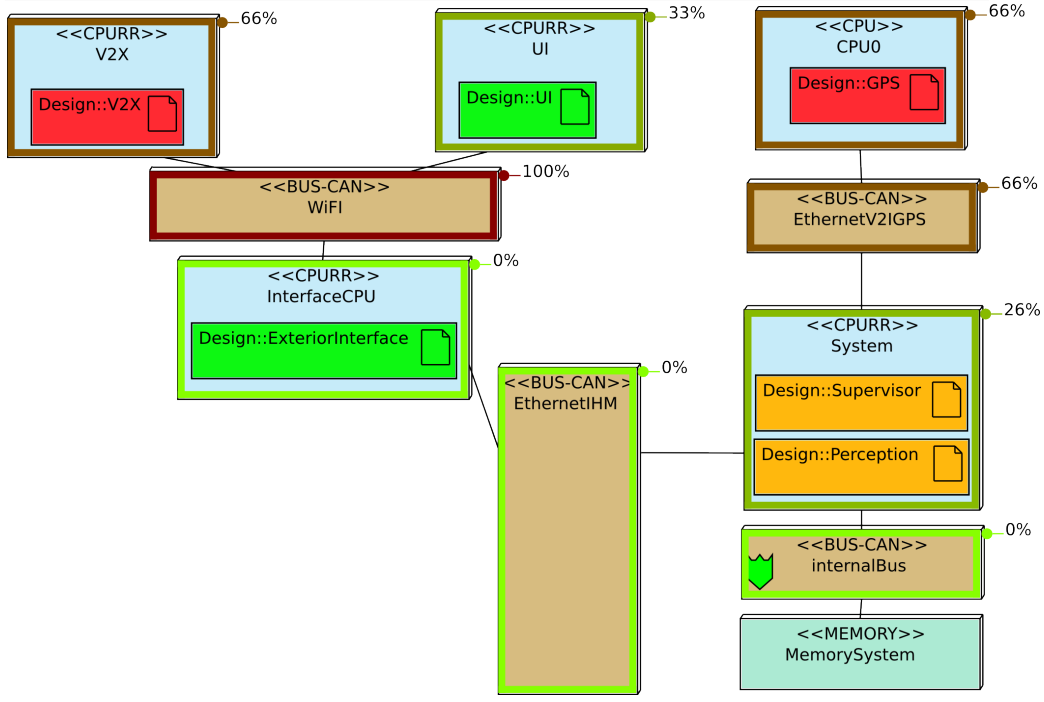


Performance Verification

Latency

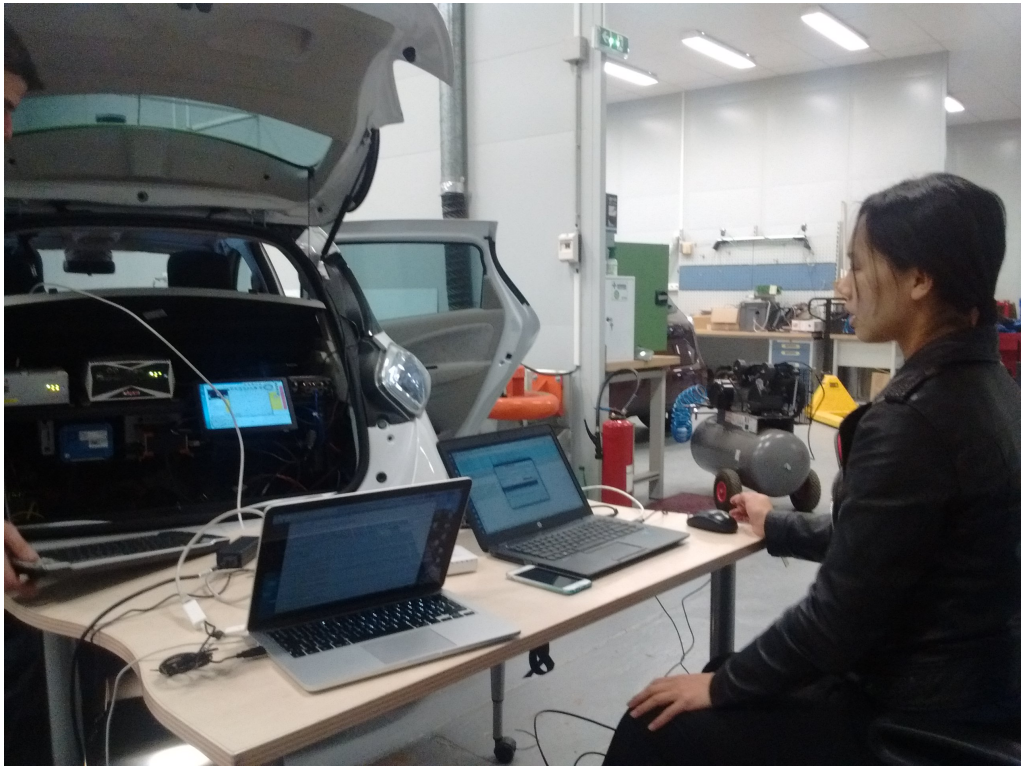


Bus/CPU Load



SW Design, Code generation, Test

- First SW model from mapping models
- SW model refinement
- SW model verification (safety, security)
- Code generation
  - (Virtual) Prototyping, test



Conclusion and Future Work

Achievements: SysML-Sec

- Methodology for designing safe and secure embedded systems
- Fully supported by TTool
- Applied to different domains, e.g., automotive systems, IoTs, malware

Future work

- Security risk assistance and backtracing
- Assistance to handle conflicts between security/safety/performance
  - Design space exploration

To Go Further ...

Web sites

- https://sysml-sec.telecom-paristech.fr
- https://ttool.telecom-paristech.fr

References

- Ludovic Apvrille, Yves Roudier, "SysML-Sec: A SysML Environment for the Design and Development of Secure Embedded Systems", Proceedings of the INCOSE/APCOSEC 2013 Conference on system engineering, Yokohama, Japan, September 8-11, 2013.
- 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, 2015