Une école de l'IMT

Harmonizing Safety, Security and Performance Requirements in Embedded Systems

Prof Ludovic APVRILLE, Dr Letitia LI
ludovic.apvrille@telecom-paristech.fr
letitia.li@baesystems.com

université PARIS-SACLAY

DATE'2019

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] [Tencent 2017]

(C) Wired - ABC News

Medical appliances

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

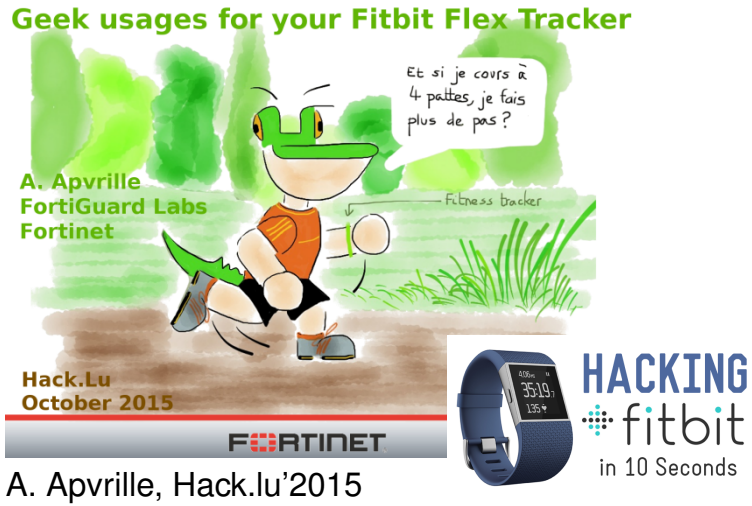
(C) Hospira

Examples of Threats (Cont.)

Internet of Things

- Proof of concept of attack on IZON camera [Stanislav 2013]

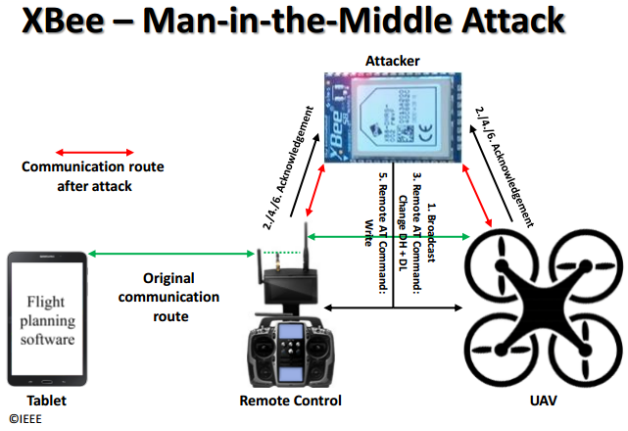
- Vulnerability on fitbit [Apvrille 2015]



A. Apvrille, Hack.lu'2015

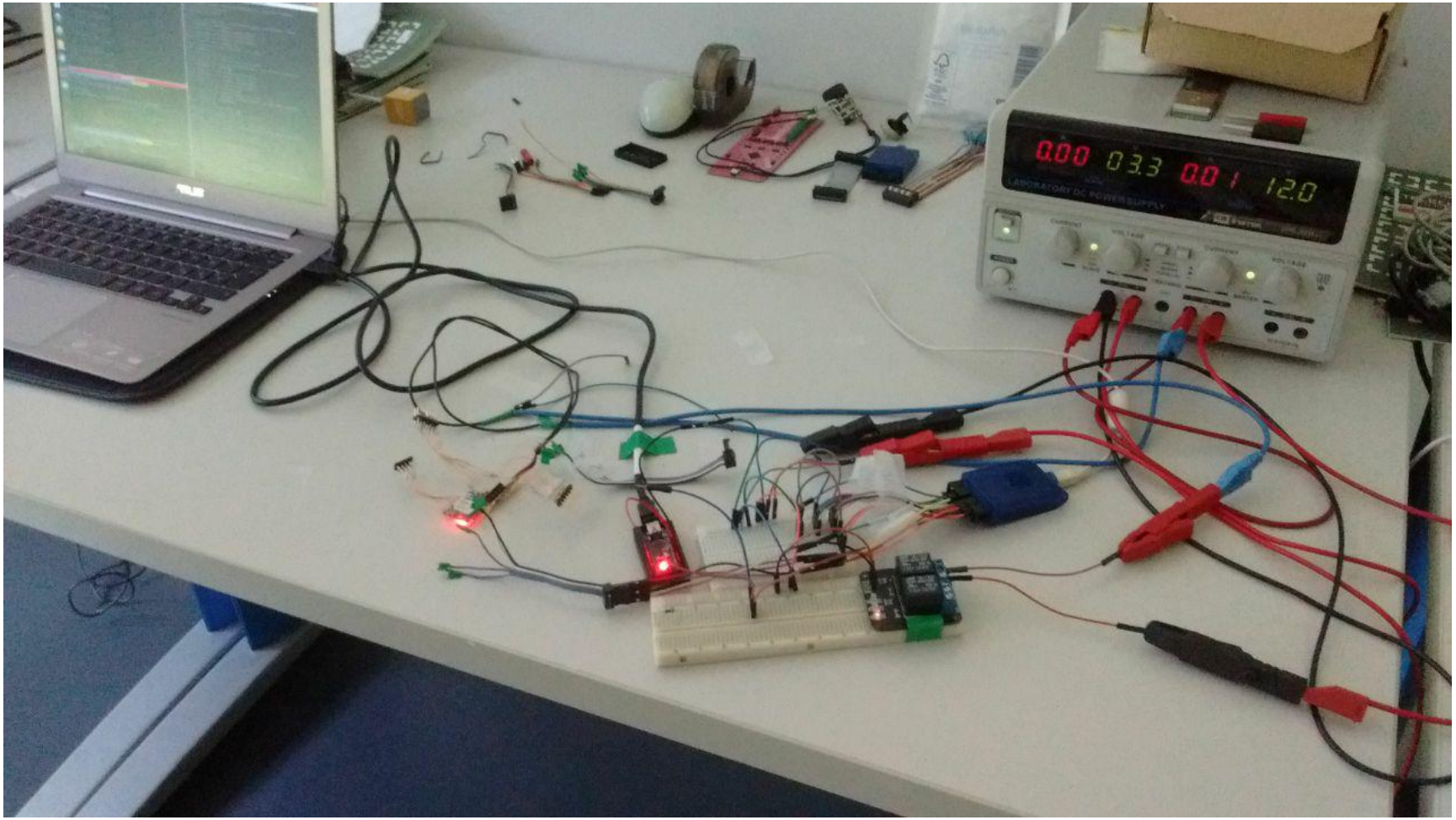
(C) beforeitnews

- Hacking a professional drone [Rodday 2016]



N. Rodday, BlackHat Asia'2016

Vulnerability Identification



Vulnerability Identification (Cont.)

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

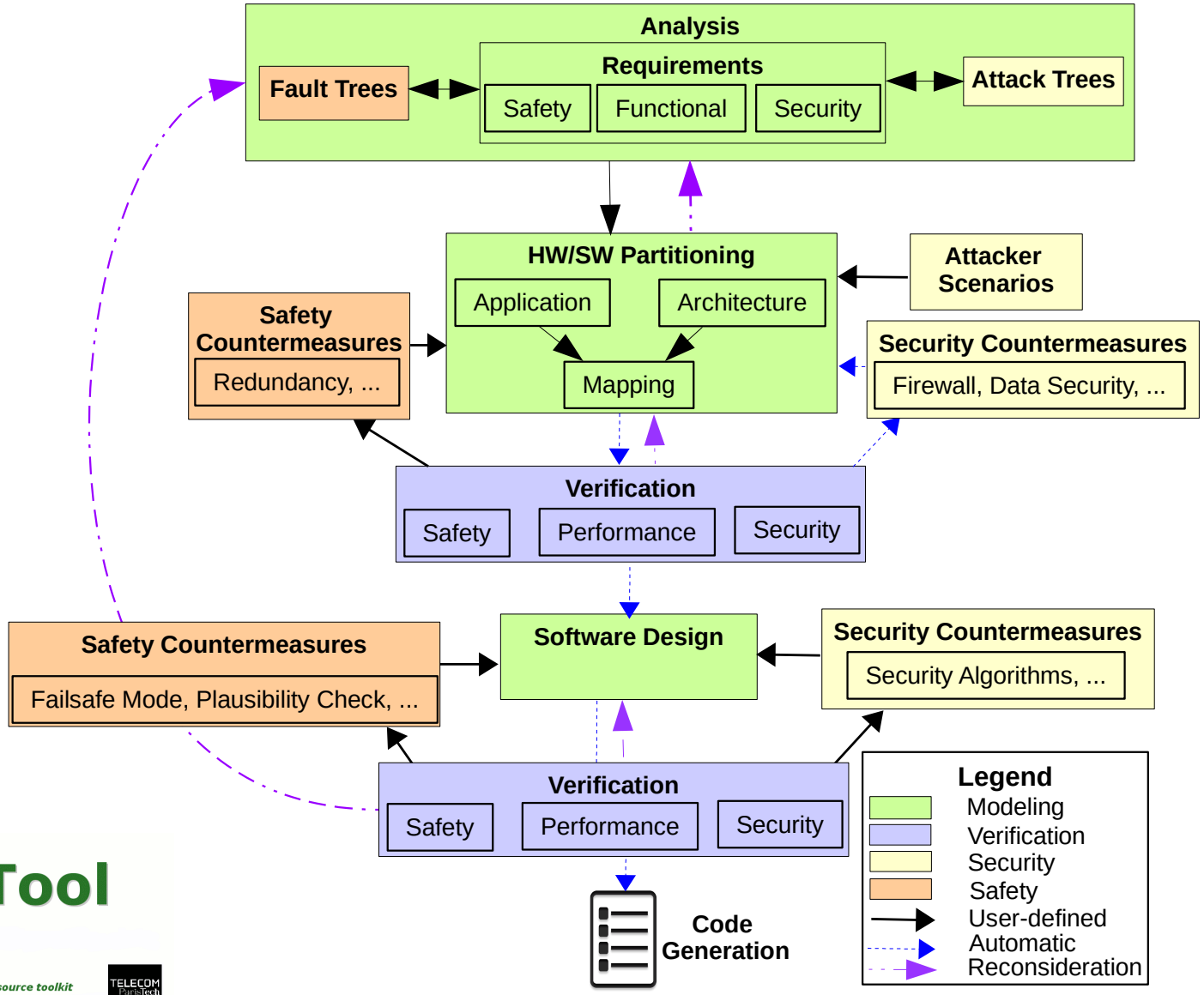
Designing Safe and Secure Embedded Systems: SysML-Sec

Main idea

- **Holistic approach**: bring together embedded system experts, system architects, system designers and security experts (with SysML)

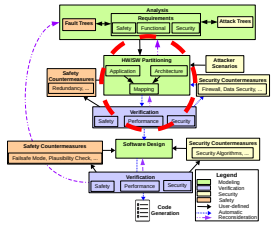
Common issues (addressed by SysML-Sec):

- Adverse effects due to security on safety/real-time/performance properties
  - Commonly: only the design of security mechanisms
- Hardware/Software partitioning and Design Space Exploration
  - Commonly: no support for security



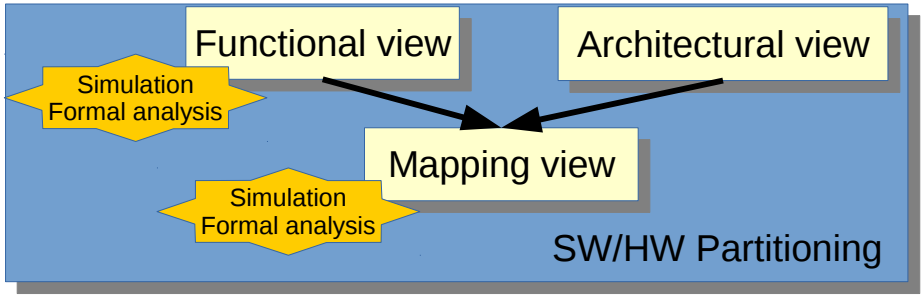
Fully supported by TTool

Partitioning



Before mapping

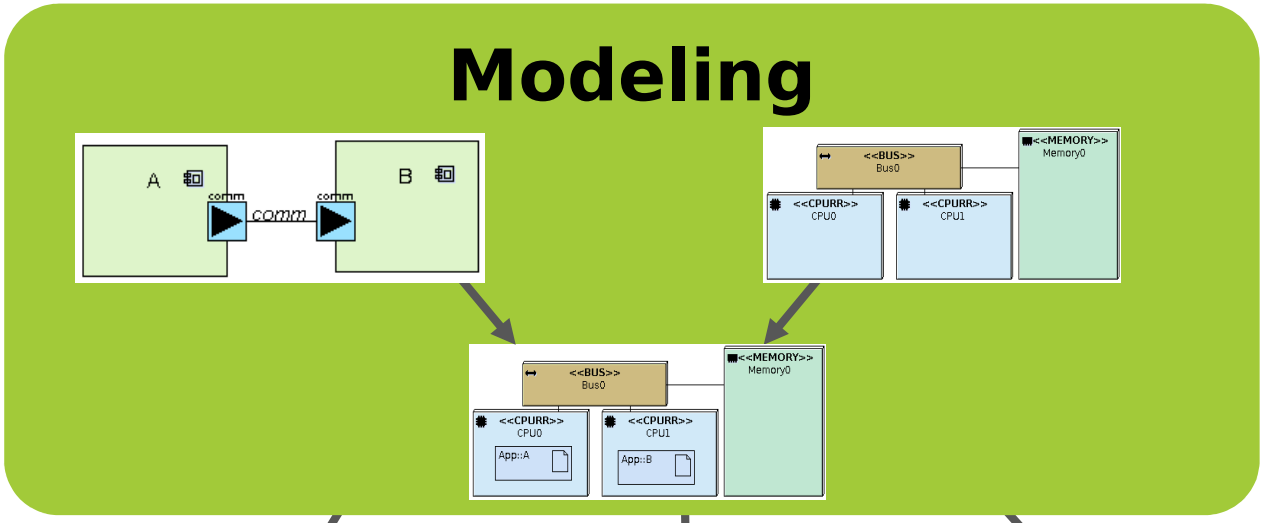
- Security mechanisms can be captured but not verified



After mapping

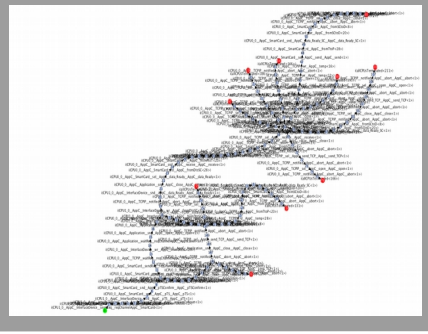
- Verify security (confidentiality, authenticity) according to attacker capabilities
  - Whether different HW elements are or are not on the same die
  - Where cryptographic materials (keys) are stored
  - Where encrypt/decrypt operations are performed
- Impact of security mechanisms on performance and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

Partitioning Verification

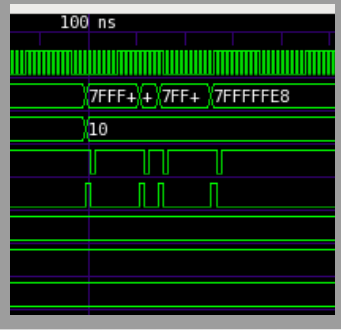


Automatic Verification

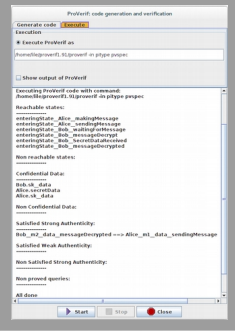
Safety



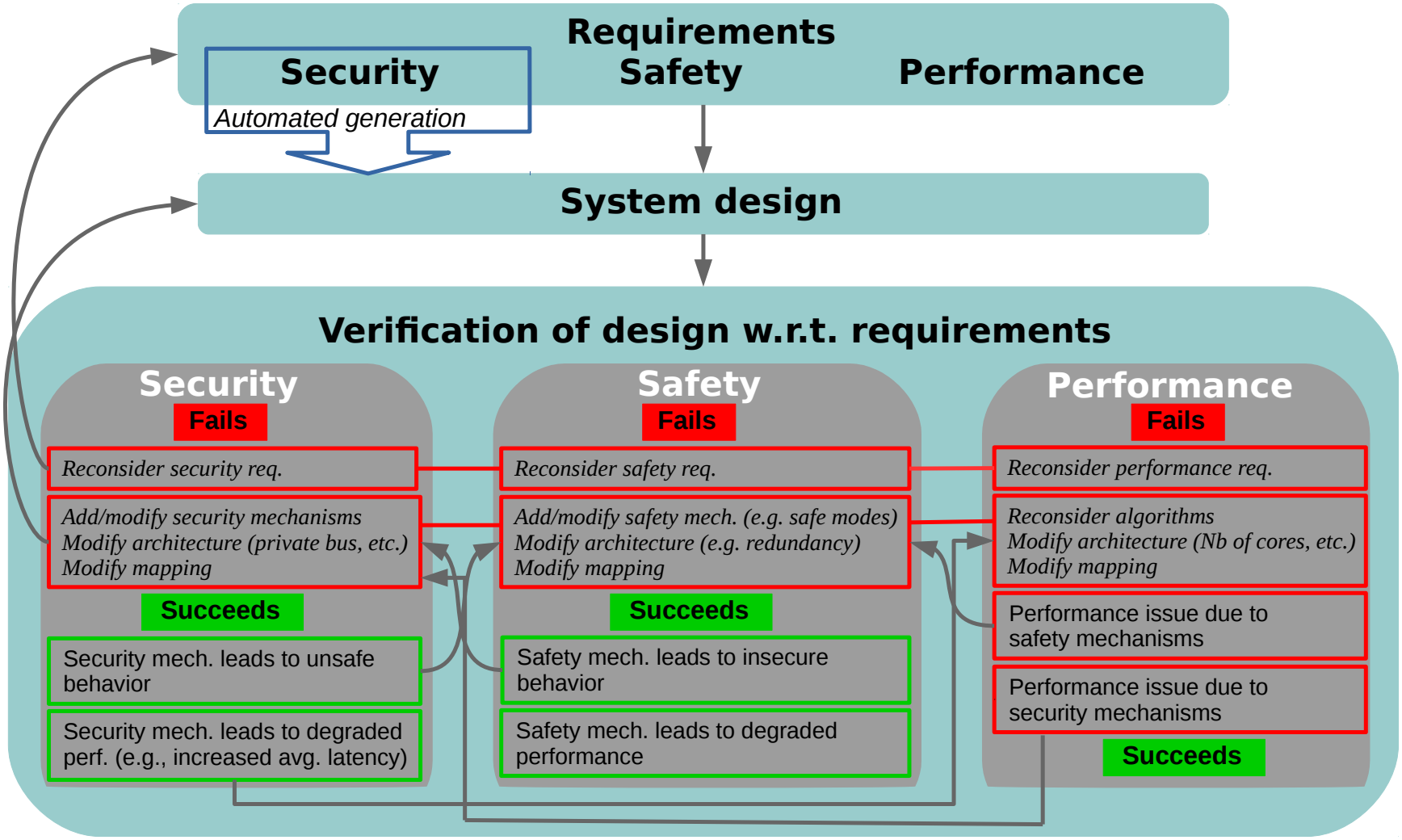
Performance



Security



Safety/Security/Performance



Safety, Security and Perf. Mechanisms

Safety

- Fail-safe mode
- Redundancy
- Resistance to external phenomenon
- System monitoring, event logging and watchdogs
- Plausibility check
- Anomaly detection
- RTOS (determinism)
- ...

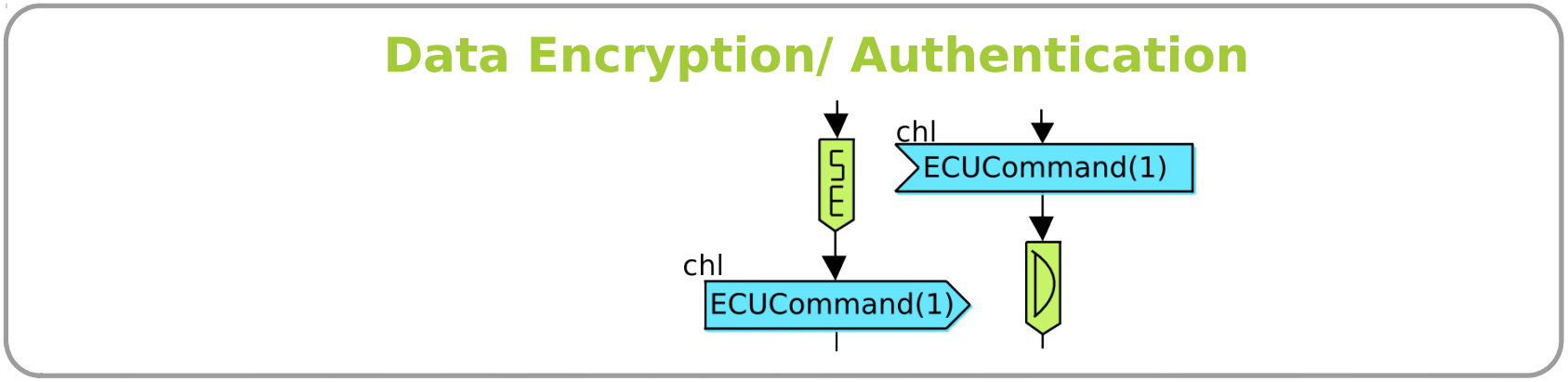
Security

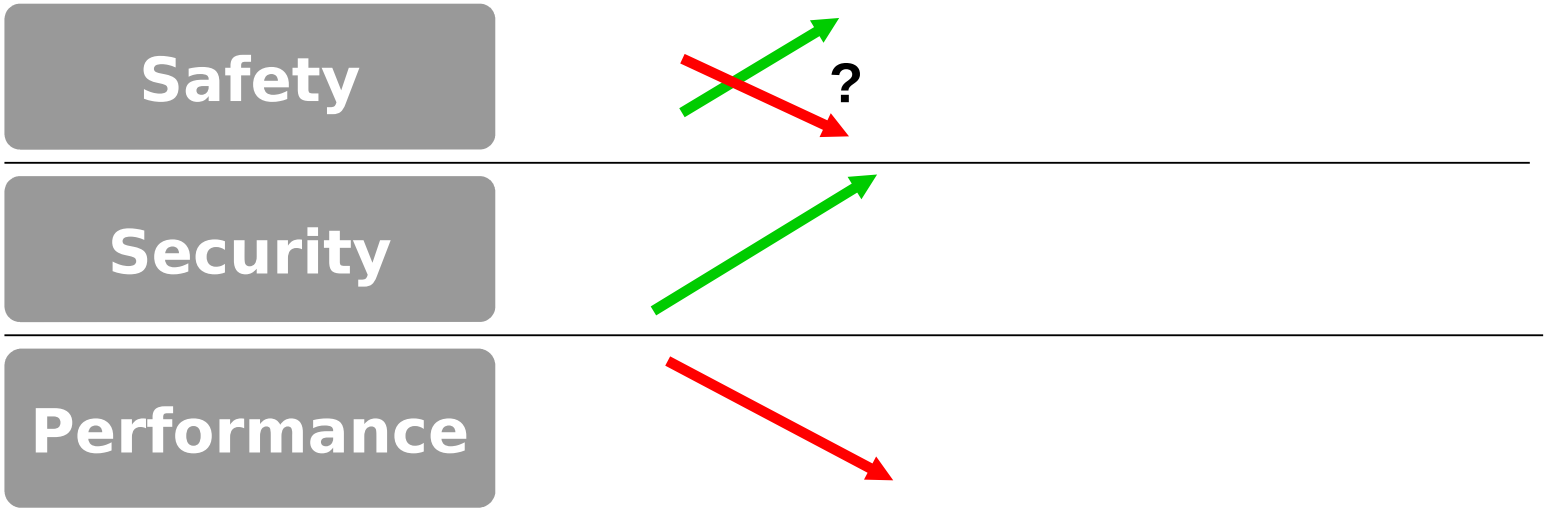
- TPMs
- Cryptography
- Security protocols
- Firewalls
- Intrusion detection Systems
- Secure boot
- ...

Performance

- Faster hardware
- Less complex versions of algorithms
- Move software functions to hardware
- ...

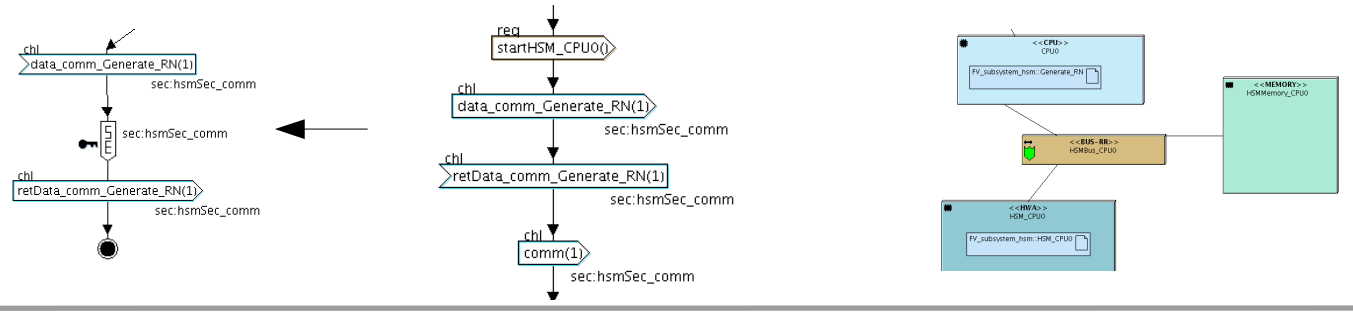
Safety and Security Mechanisms





Safety and Security Mechanisms (Cont.)

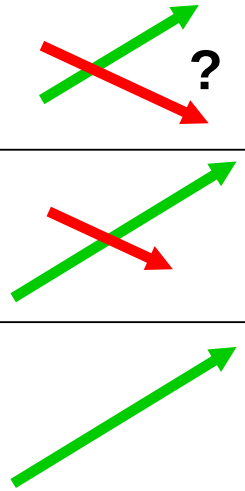
Data Security with Hardware Security Module



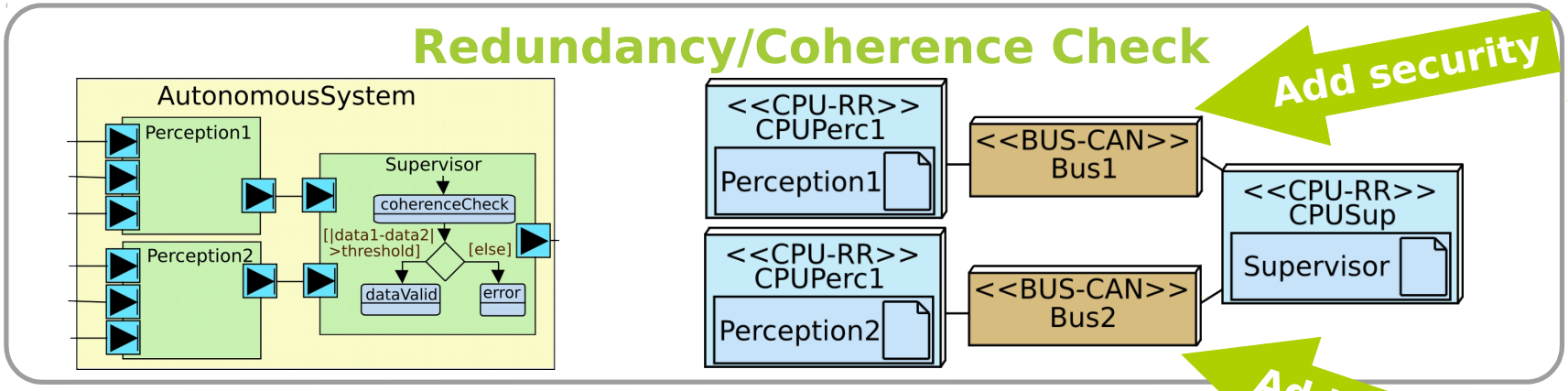
Safety

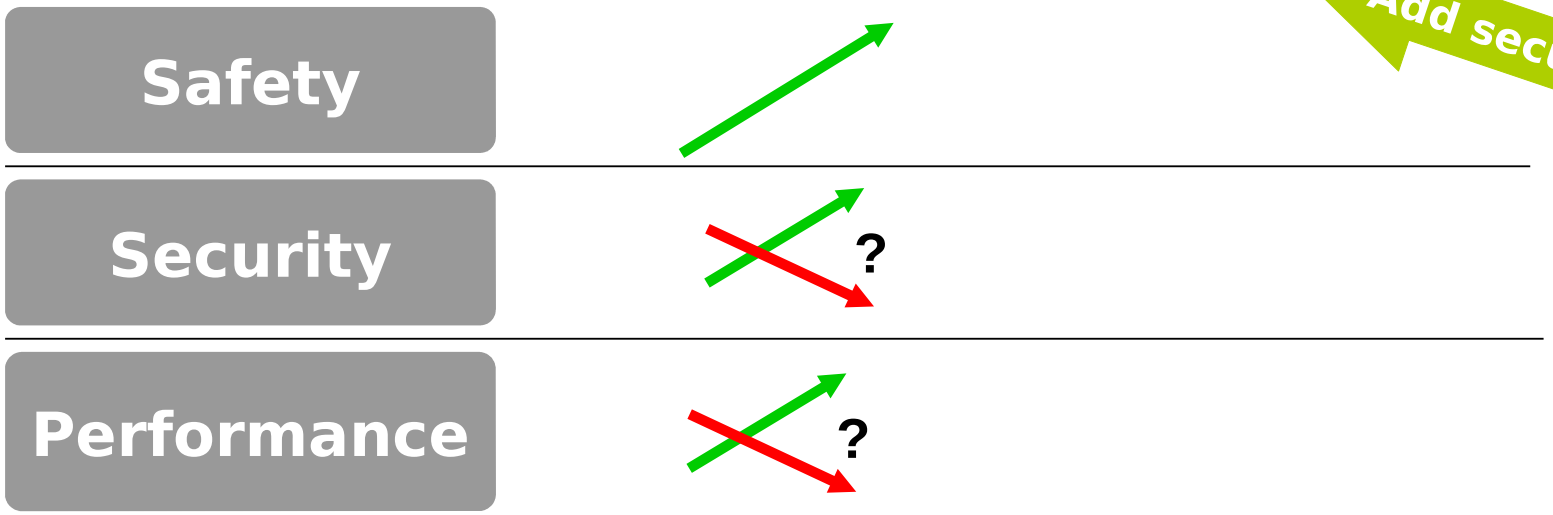
Security

Performance

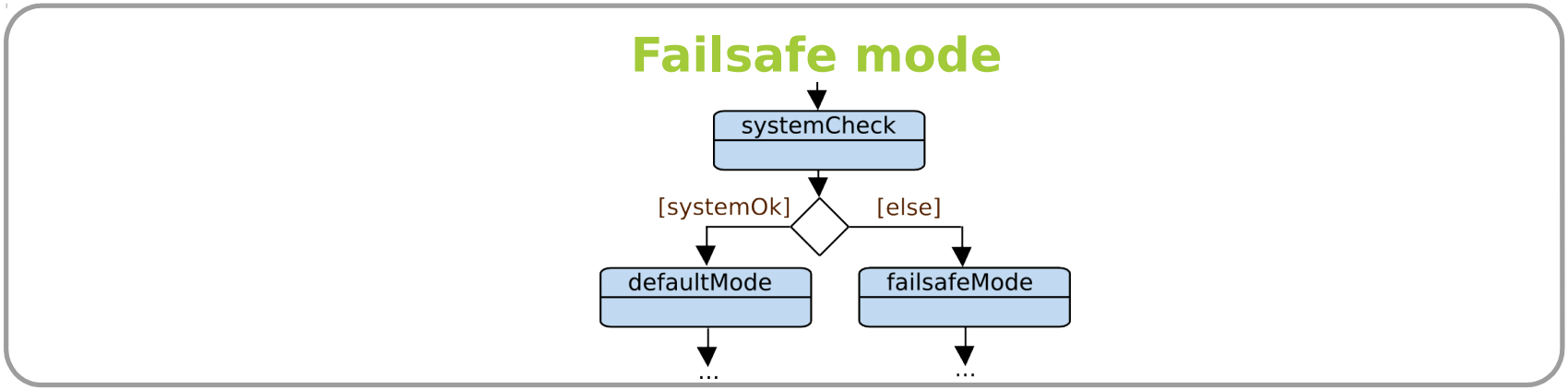


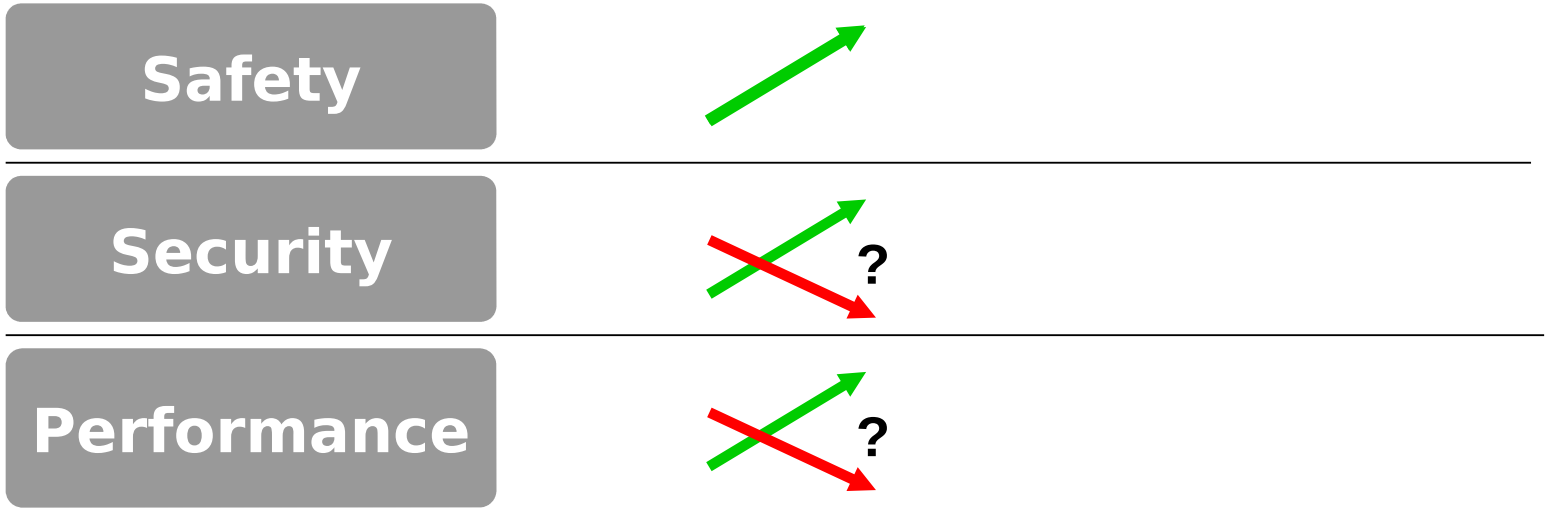
Safety and Security Mechanisms (Cont.)



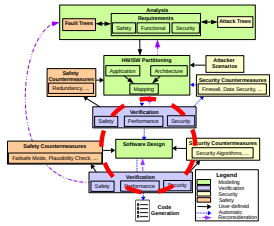


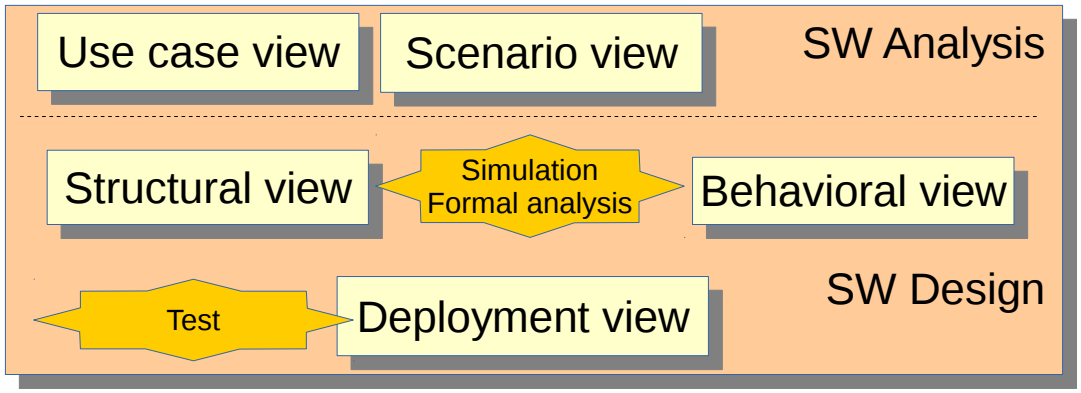
Safety and Security Mechanisms





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

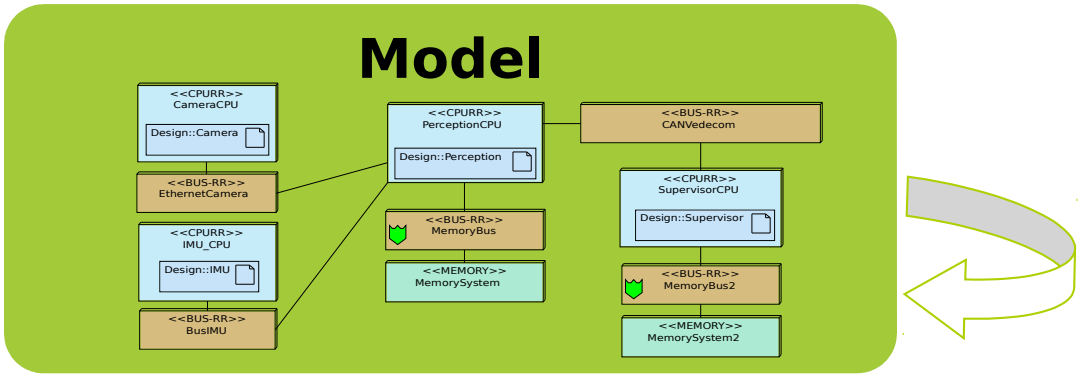
H2020 AQUAS

- 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



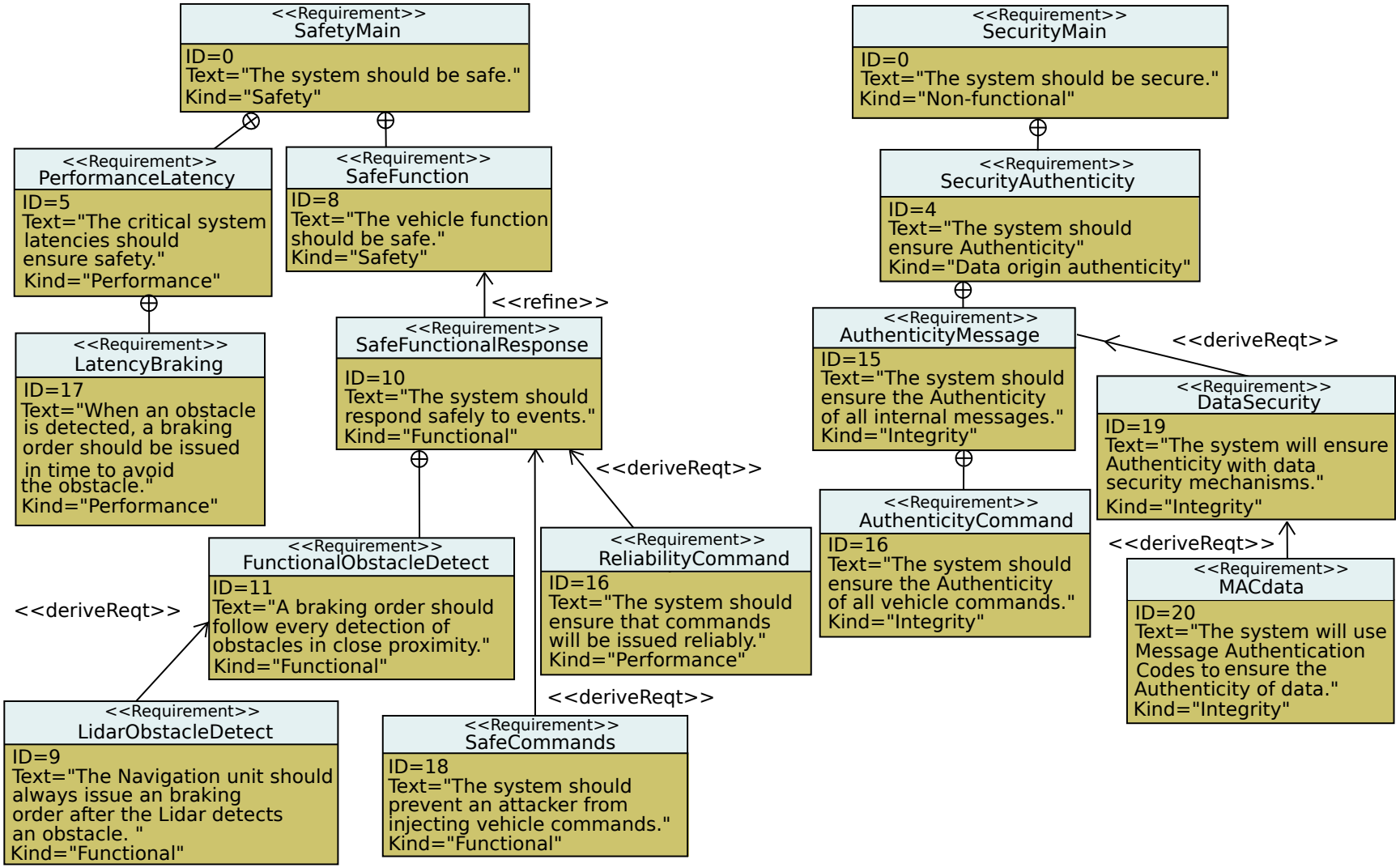
Verification

Tests

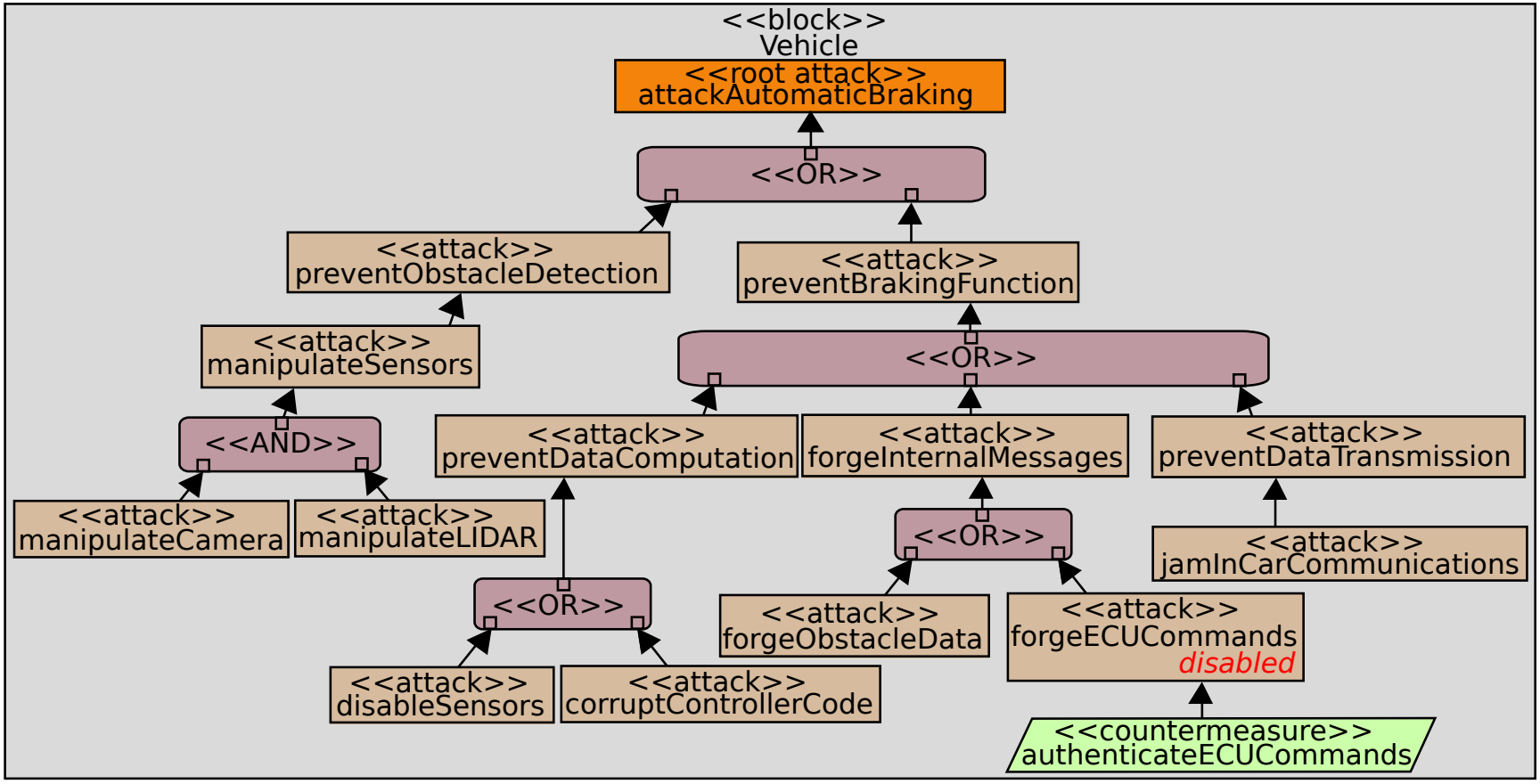
Constraints

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

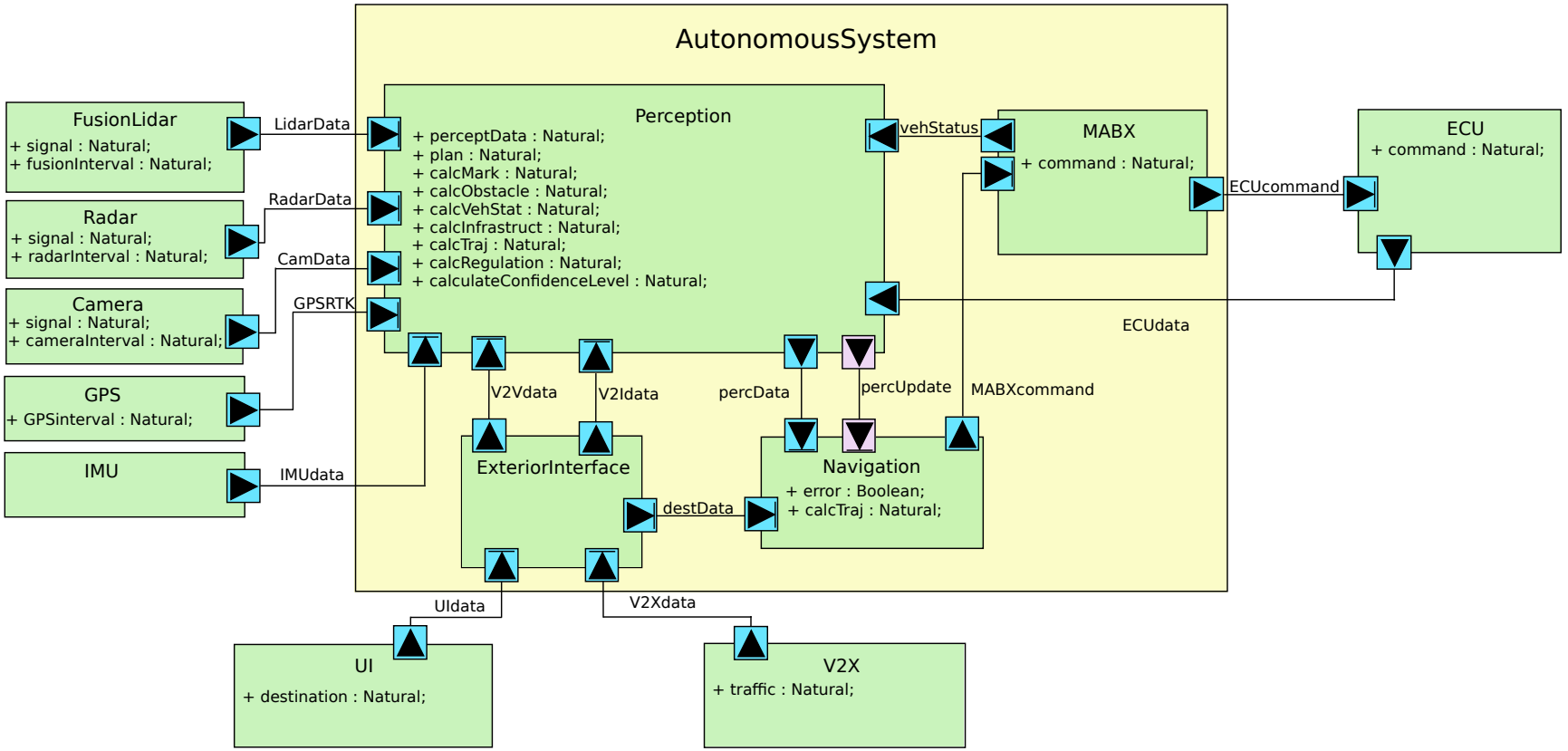
Requirements



Attacks

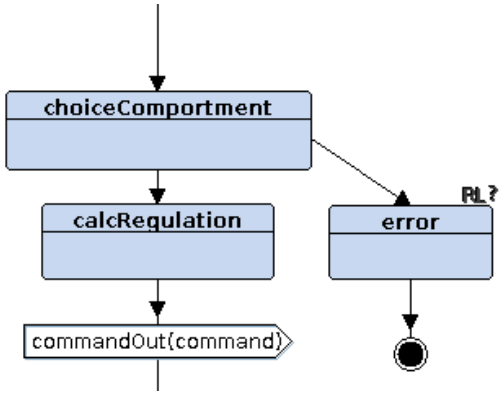

<<block>>
Vehicle
<<root attack>>
attackAutomaticBraking
<<OR>>
<<attack>>
preventObstacleDetection
<<attack>>
preventBrakingFunction
<<attack>>
manipulateSensors
<<OR>>
<<AND>>
<<attack>>
preventDataComputation
<<attack>>
forgeInternalMessages
<<attack>>
preventDataTransmission
<<attack>>
manipulateCamera
<<attack>>
manipulateLIDAR
<<OR>>
<<OR>>
<<attack>>
jamInCarCommunications
<<attack>>
forgeObstacleData
<<attack>>
forgeECUCommands
disabled
<<attack>>
disableSensors
<<attack>>
corruptControllerCode
<<countermeasure>>
authenticateECUCommands

Functional View



Safety Verification (Before Mapping)

Reachability/Liveness

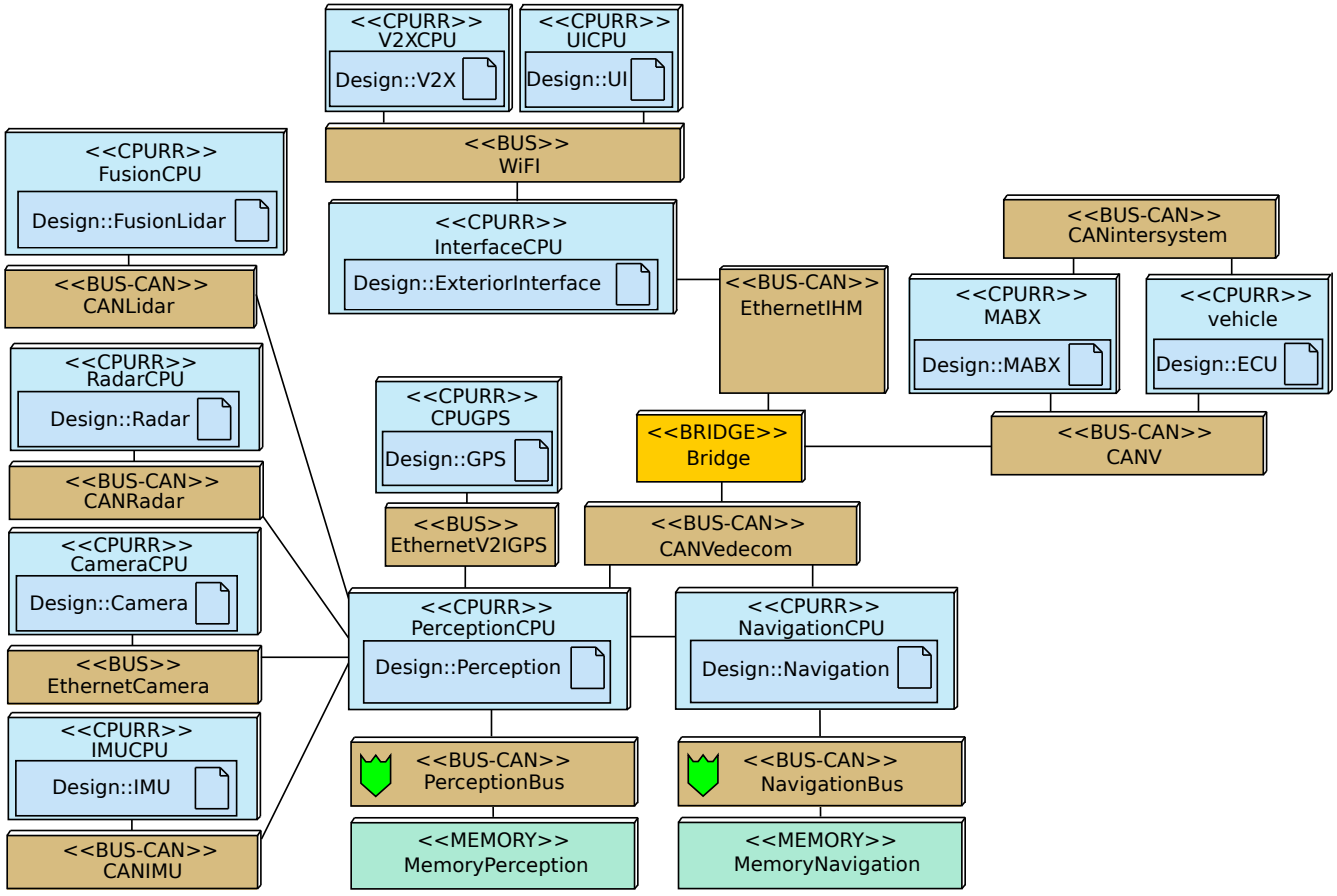


Queries

Safety Pragma

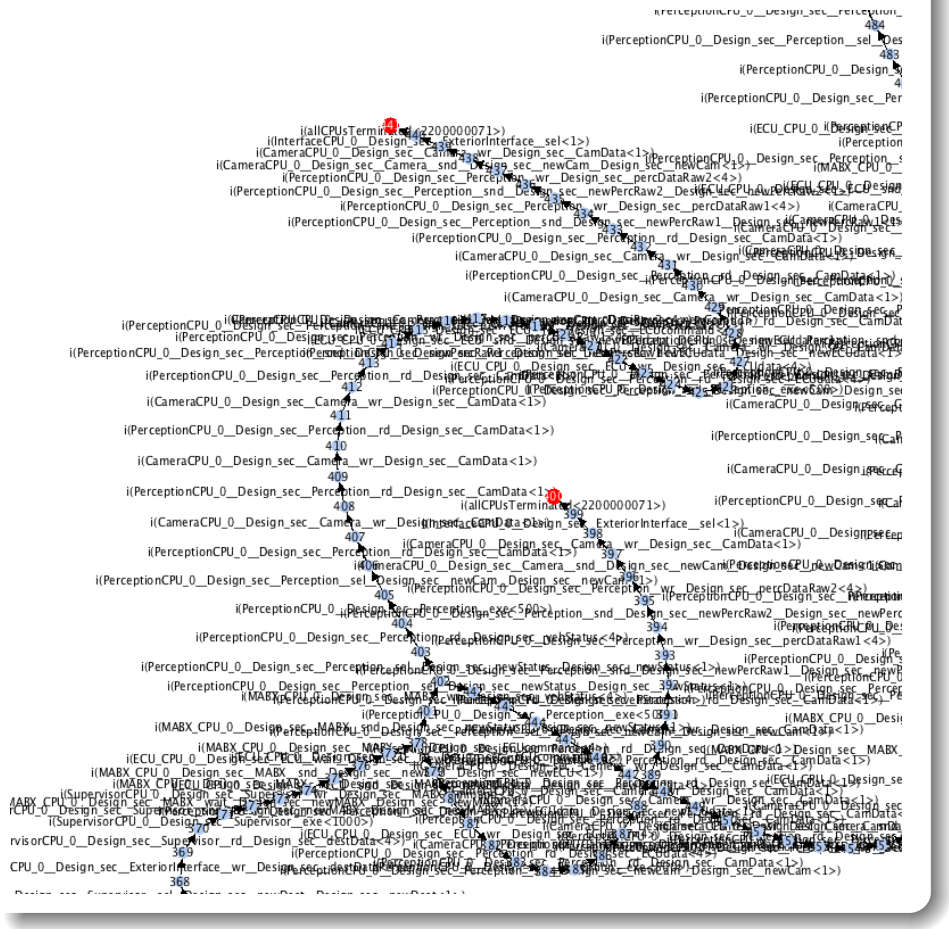
A[] Supervisor.running
Perception.distance<threshold -->
Supervisor.brakingOrder

Architecture and Mapping Views

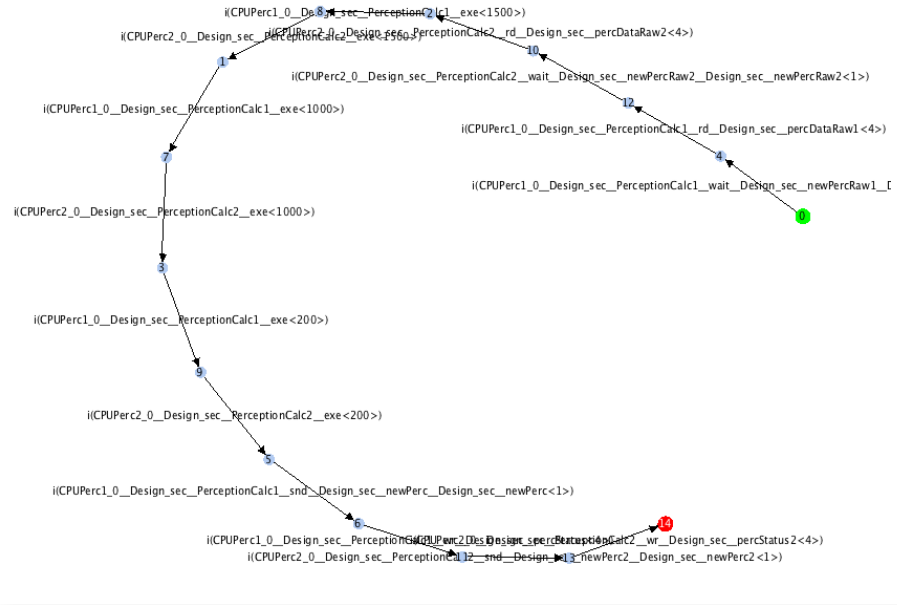


Safety Verification (After Mapping)

Reachability Graph

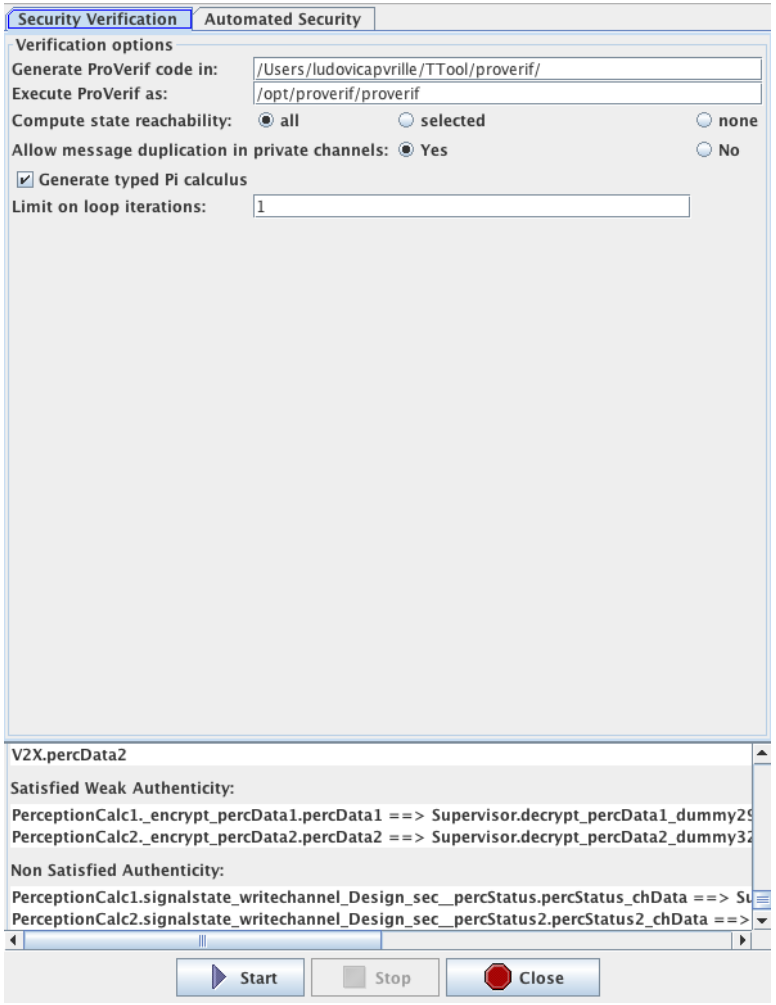


Minimized RG

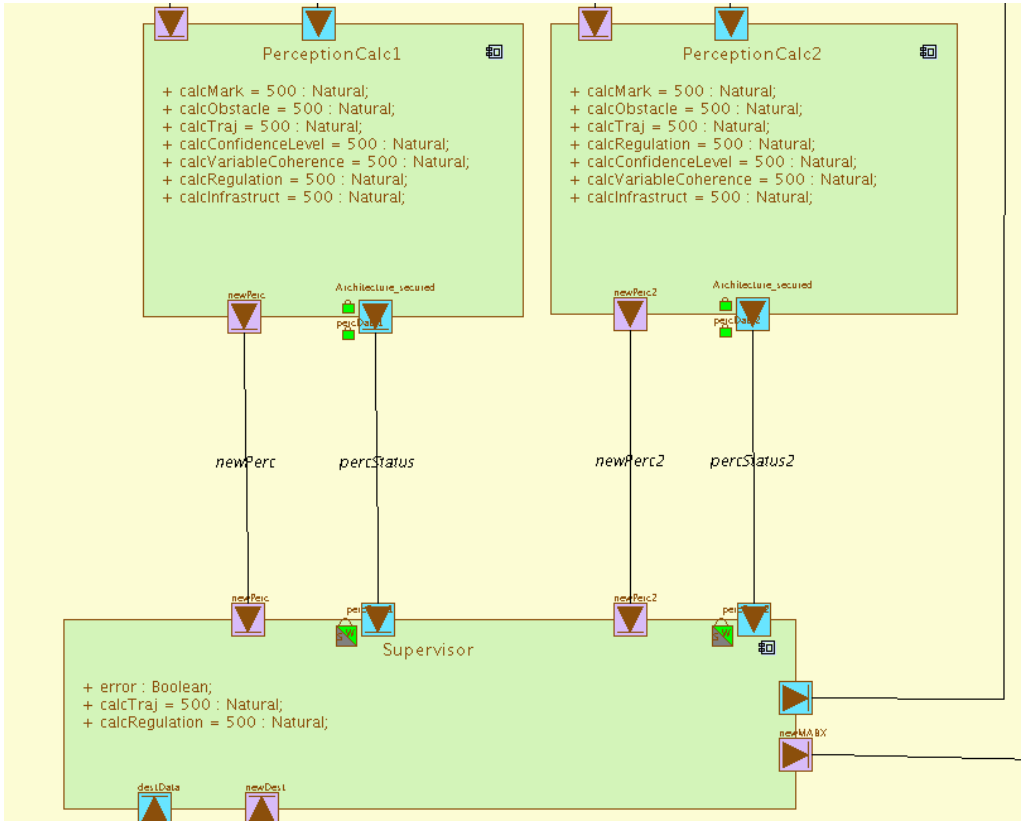


Security Verification

Dialog window

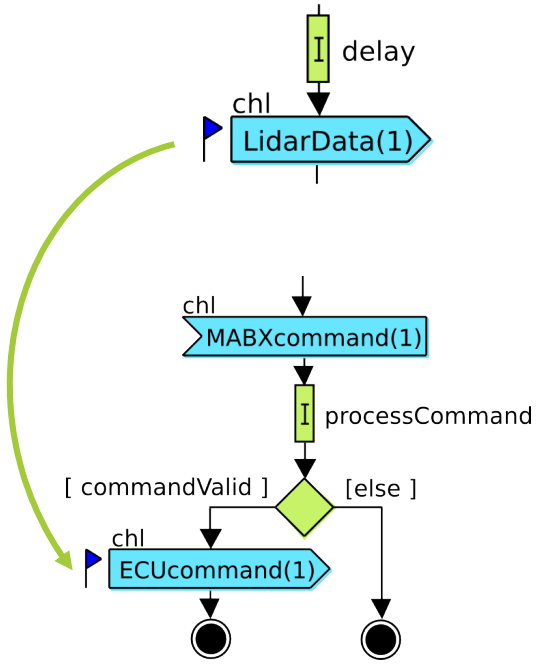


Backtracing

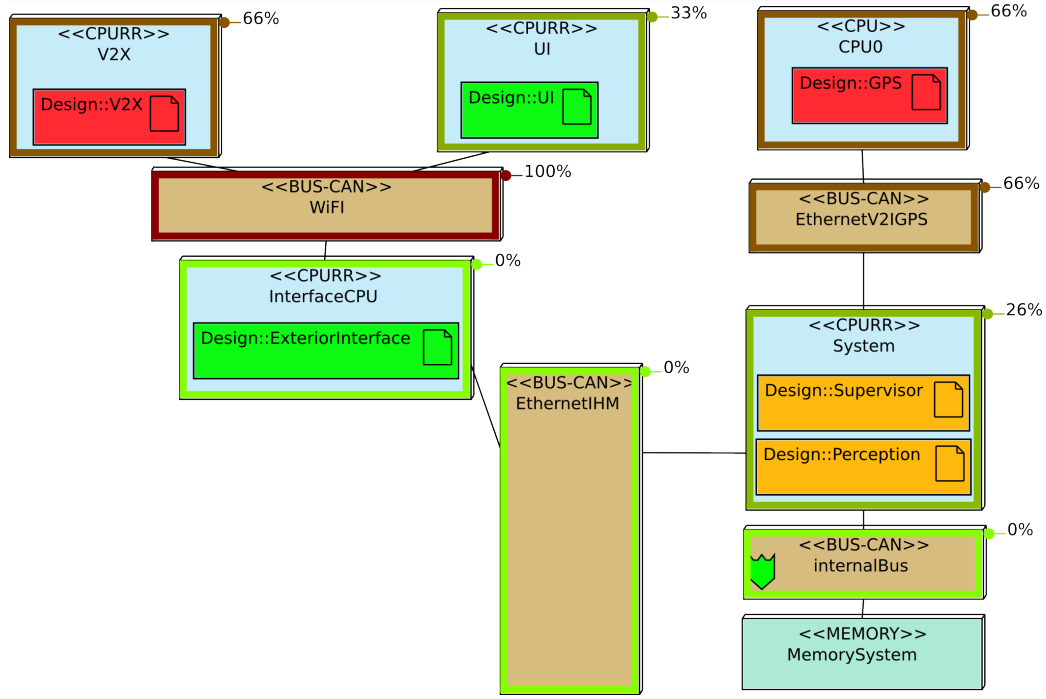


Performance Verification

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 assessment and backtracing
- Assistance in handling conflicts between security/safety/performance
  - Design space exploration

For more information ...

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