TELECOM ParisTech
Une école de l'IMT

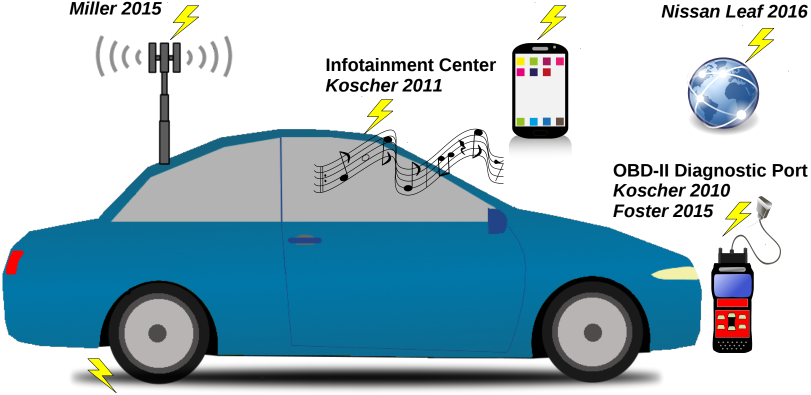
INSTITUT VEDECOM
DU VÉHICULE DÉCARBONÉ ET COMMUNICANT ET DE SA MOBILITÉ

Design and Verification of Secure Autonomous Vehicles

Letitia W. Li, Ludovic Apvrille, Annie Bracquemond
letitia.li@telecom-paristech.fr

ITS

Attacks on Connected Vehicles



3G/4G Cellular Network
Miller 2015

Infotainment Center
Koscher 2011

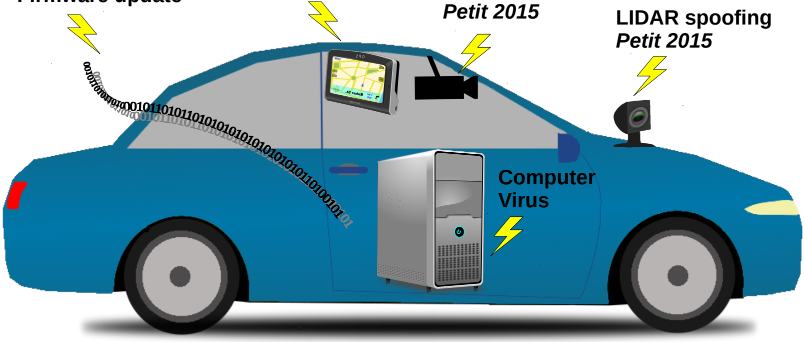
Malicious Mobile Applications
Woo 2015

Exploitation of Web APIs
Nissan Leaf 2016

OBD-II Diagnostic Port
Koscher 2010
Foster 2015

Tire Pressure Sensor
Rouf 2010

Attacks on Autonomous Vehicles



Over-the-air
Firmware update

GPS Spoofing
Humphreys 2008

Camera Blinding
Petit 2015

LIDAR spoofing
Petit 2015

Computer
Virus

EVITA Project

- FP7 project ended in 2012
- E-safety Vehicle Intrusion Protected Applications
- Design of architecture for secure automotive on-board networks
- EVITA does not address side-channel attacks i.e. hardware is assumed to be tamper-resistant
- Several EVITA-compatible ECUs on the market (STM, Bosch, etc.)

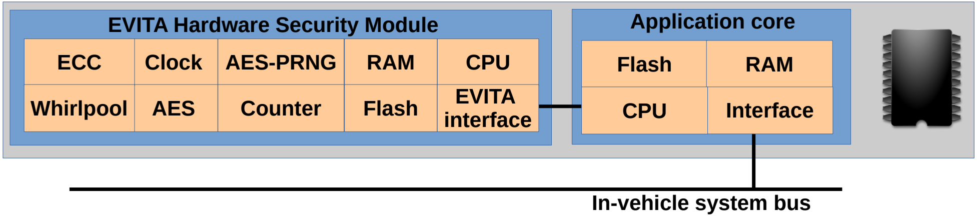
Security Requirements

- Authenticity of vehicle software and data
- Authenticity of vehicle communication
- Confidentiality of vehicle communication
- Integrity of vehicule communication
- ...

EVITA Results

- Security Protocols
  - Protocols are CAN compatible
  - Formally verified with SysML-Sec
- APIs
  - Integration in Autosar
- Specification of Hardware Security Modules

Hardware Security Modules



EVITA Hardware Security Module

ECC | Clock | AES-PRNG | RAM | CPU

Whirlpool | AES | Counter | Flash | EVITA interface

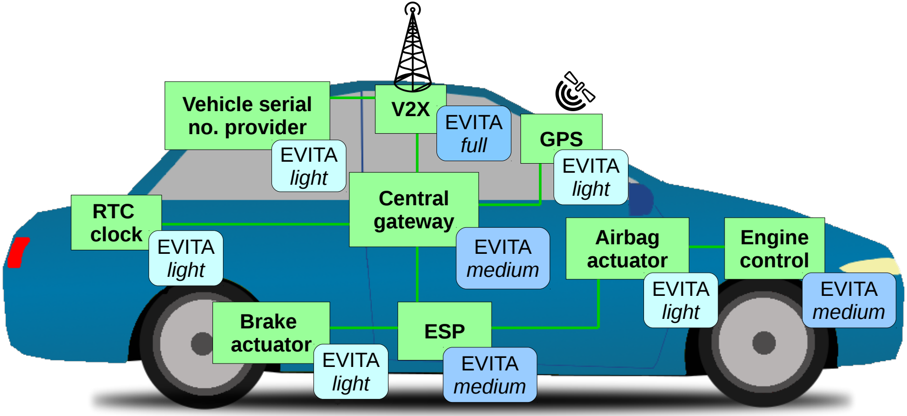
Application core

Flash | RAM

CPU | Interface

In-vehicle system bus

EVITA Architecture



How to Design a Secure Automotive System?

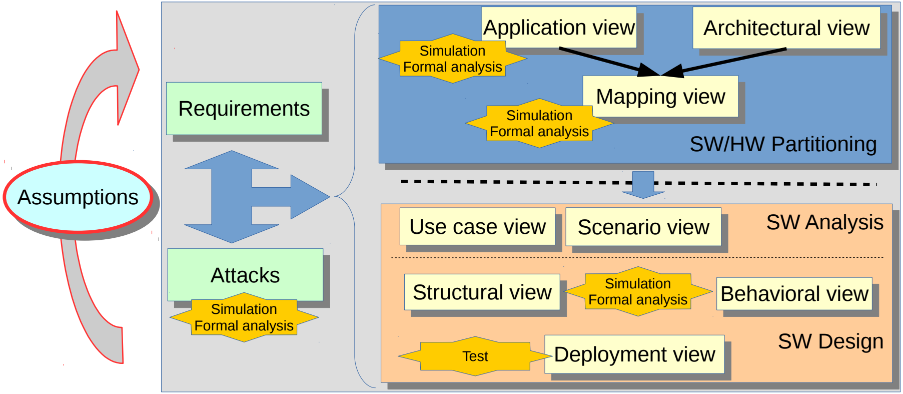
"Those who fail to plan, plan to fail."

Benjamin Franklin

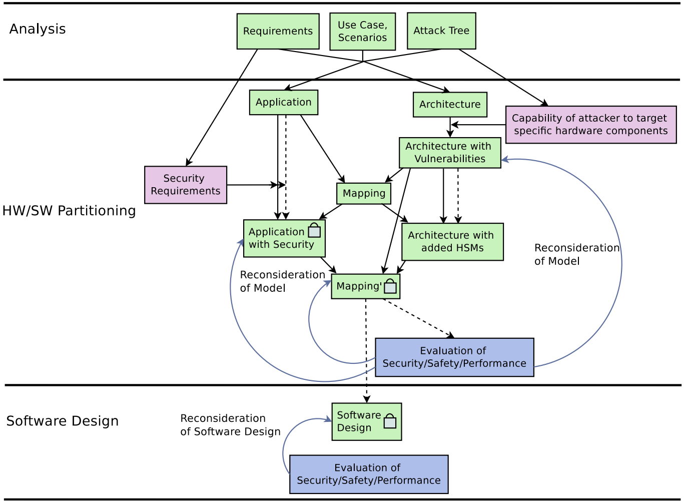
- Use of a model-driven approach (**SysML-Sec**)
- Support of safety, performance and **security** (formal) verification

SysML-Sec Methodology

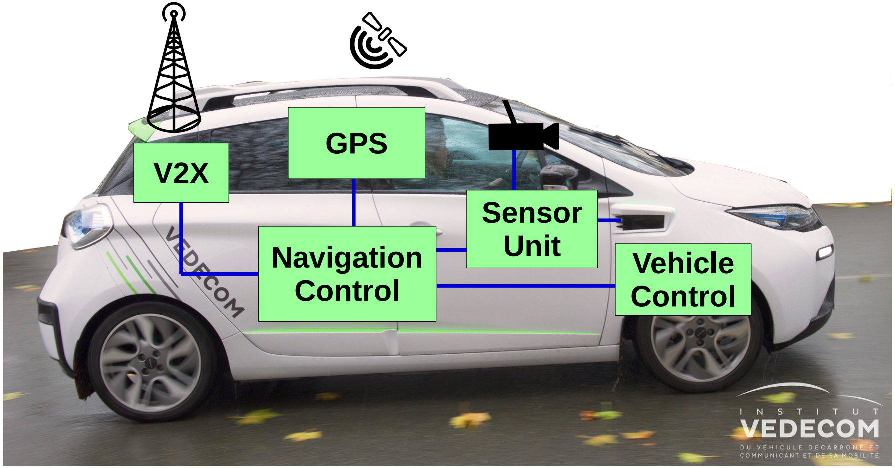
TTool
An open source toolkit provided by



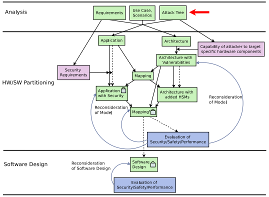
Methodology in detail

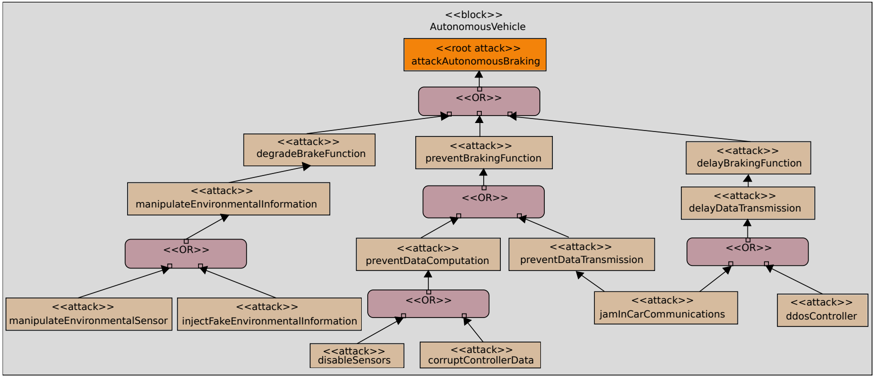

Analysis
Requirements
Use Case, Scenarios
Attack Tree
HW/SW Partitioning
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
Mapping
Application with Security
Architecture with added HSMs
Reconsideration of Model
Reconsideration of Model
Mapping'
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance

Autonomous Vehicle under Design

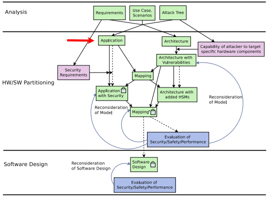


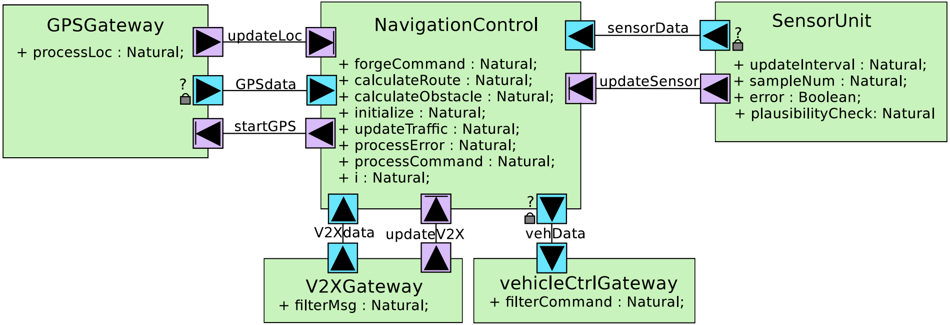
Attack Tree


Analysis
Requirements
Use Case, Scenarios
Attack Tree
HW/SW Partitioning
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
Mapping
Application with Security
Architecture with added HSMs
Reconsideration of Model
Mapping'
Reconsideration of Model
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance


<<block>>
AutonomousVehicle
<<root attack>>
attackAutonomousBraking
<<OR>>
<<attack>>
degradeBrakeFunction
<<attack>>
preventBrakingFunction
<<attack>>
delayBrakingFunction
<<attack>>
manipulateEnvironmentalInformation
<<OR>>
<<attack>>
delayDataTransmission
<<OR>>
<<attack>>
preventDataComputation
<<attack>>
preventDataTransmission
<<OR>>
<<attack>>
manipulateEnvironmentalSensor
<<attack>>
injectFakeEnvironmentalInformation
<<OR>>
<<attack>>
jamInCarCommunications
<<attack>>
ddosController
<<attack>>
disableSensors
<<attack>>
corruptControllerData

Application View


Analysis
Requirements
Use Case, Scenarios
Attack Tree
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
Mapping
HW/SW Partitioning
Application with Security
Architecture with added HSMs
Reconsideration of Model
Mapping'
Reconsideration of Model
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance



GPSGateway
+ processLoc : Natural;

updateLoc

GPSdata

startGPS

NavigationControl
+ forgeCommand : Natural;
+ calculateRoute : Natural;
+ calculateObstacle : Natural;
+ initialize : Natural;
+ updateTraffic : Natural;
+ processError : Natural;
+ processCommand : Natural;
+ i : Natural;

sensorData

updateSensor

SensorUnit
+ updateInterval : Natural;
+ sampleNum : Natural;
+ error : Boolean;
+ plausibilityCheck: Natural

V2Xdata

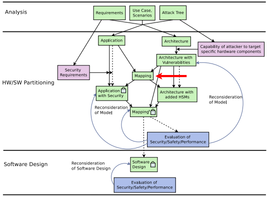
updateV2X

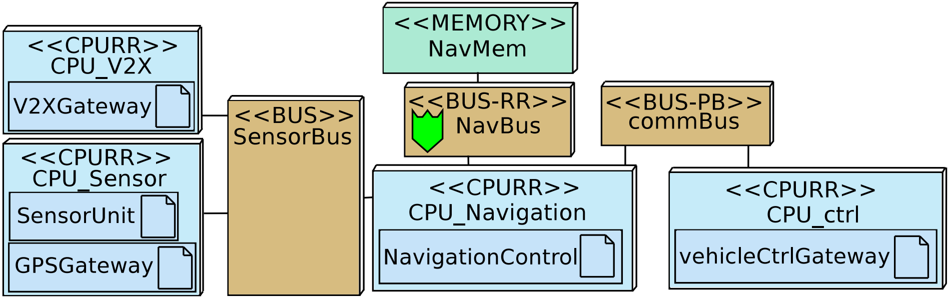
vehData

V2XGateway
+ filterMsg : Natural;

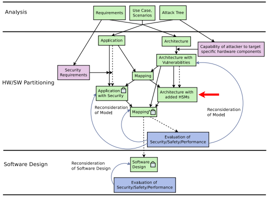
vehicleCtrlGateway
+ filterCommand : Natural;

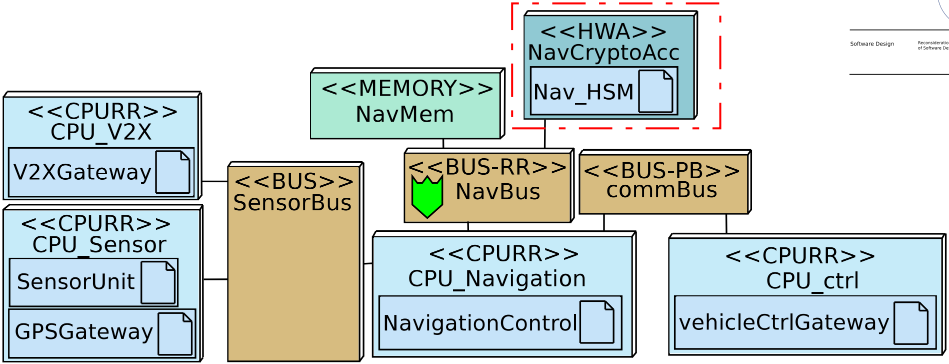
Architecture/Mapping View


Analysis
Requirements
Use Case, Scenarios
Attack Tree
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
HW/SW Partitioning
Mapping
Application with Security
Architecture with added HSMs
Reconsideration of Model
Mapping'
Reconsideration of Model
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance

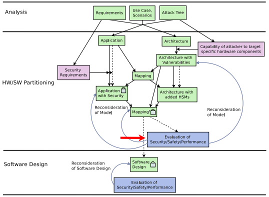


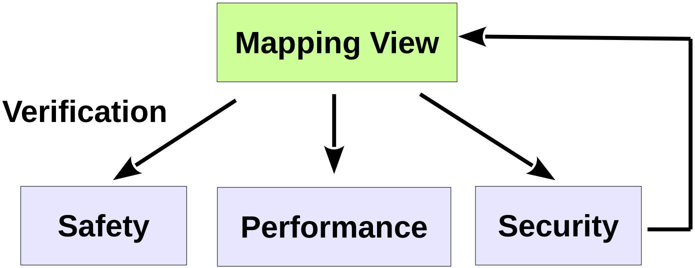
Hardware Security Modules


Analysis
Requirements
Use Case, Scenarios
Attack Tree
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
Mapping
HW/SW Partitioning
Application with Security
Architecture with added HSMs
Reconsideration of Model
Mapping'
Reconsideration of Model
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance

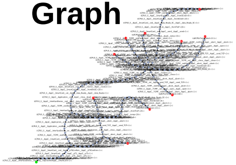


Model Verification

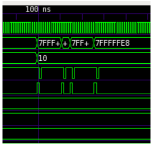

Analysis
Requirements
Use Case, Scenarios
Attack Tree
HW/SW Partitioning
Application
Architecture
Capability of attacker to target specific hardware components
Architecture with Vulnerabilities
Security Requirements
Mapping
Application with Security
Architecture with added HSMs
Reconsideration of Model
Mapping'
Reconsideration of Model
Evaluation of Security/Safety/Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security/Safety/Performance



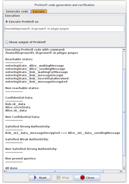
Reachability Graph



Simulation



ProVerif



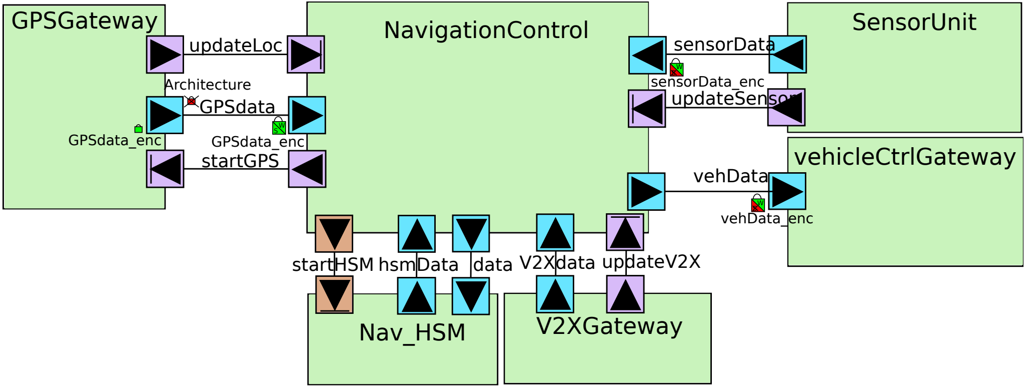
● Execute ProVerif as

/home/file/proverif1.91/proverif -in pitype pvspec

□ Show output of ProVerif

```
Executing ProVerif code with command:
/home/file/proverif1.91/proverif -in pitype pvspec

Reachable states:
----------------
enteringState__Alice__makingMessage
enteringState__Alice__sendingMessage
enteringState__Bob__waitingForMessage
enteringState__Bob__messageDecrypt
enteringState__Bob__SecretDataReceived
enteringState__Bob__messageDecrypted

Non reachable states:
----------------

Confidential Data:
----------------
Bob.sk__data
Alice.secretData
Alice.sk__data

Non Confidential Data:
----------------

Satisfied Strong Authenticity:
----------------
Bob__m2__data__messageDecrypted ==> Alice__m1__data__sendingMessage

Satisfied Weak Authenticity:
----------------

Non Satisfied Strong Authenticity:
----------------

Non proved queries:
----------------

All done
```

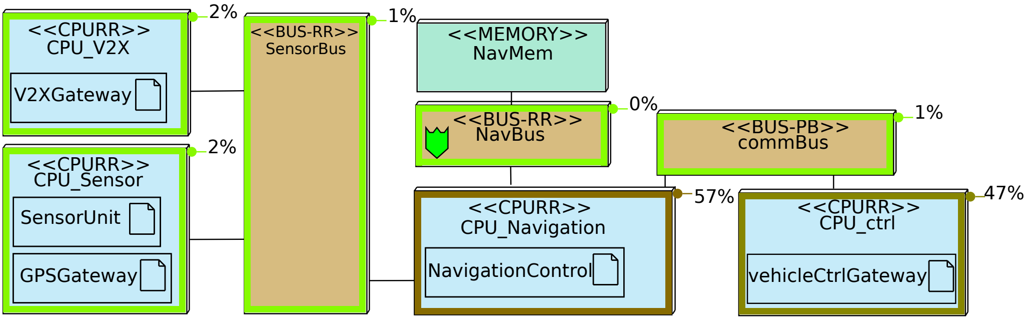
Security Verification Results



Impact of Security on Performance and Safety

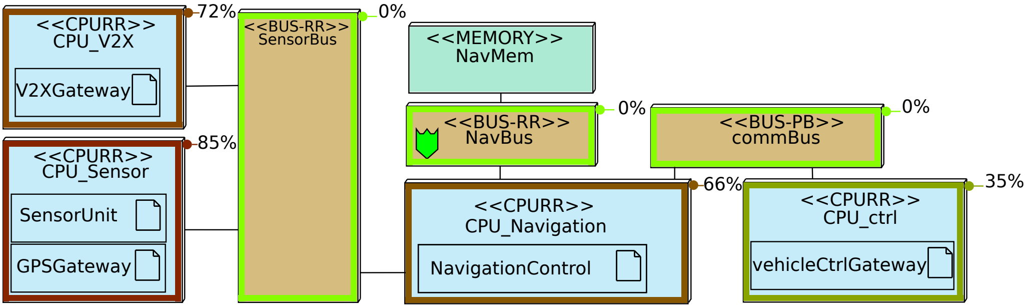
- Encryption/Decryption occupy execution cycles
- Communications increase due to key exchange, increased message size

Model Simulation



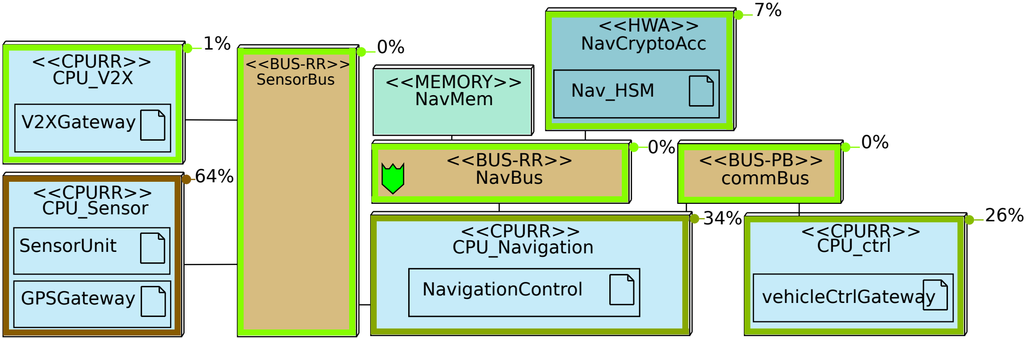
14000 cycles

Secured Model



17000 cycles

Secured with HSM



16000 cycles

Test of Security Countermeasures

Conclusion and Future Work

Contributions

- New security considerations for autonomous vehicles
- Increased connectivity introduces vulnerabilities
- Model-Driven approach towards modeling and verification of (automotive) embedded systems

Future Development

- Iterations betwen requirements, attacks and partitioning solutions
- Modeling the relationship between safety and security
- Better relations between partitioning and subsequent modeling stages

Thank You!

References

TTool: ttool.telecom-paristech.fr

SysML-Sec: http://sysml-sec.telecom-paristech.fr/

Personal website: http://perso.telecom-paristech.fr/∼apvrille