INSTITUT VEDECOM
DU VÉHICULE DÉCARBONÉ ET COMMUNICANT ET DE SA MOBILITÉ

RELATIONSHIP BETWEEN SECURITY AND SAFETY

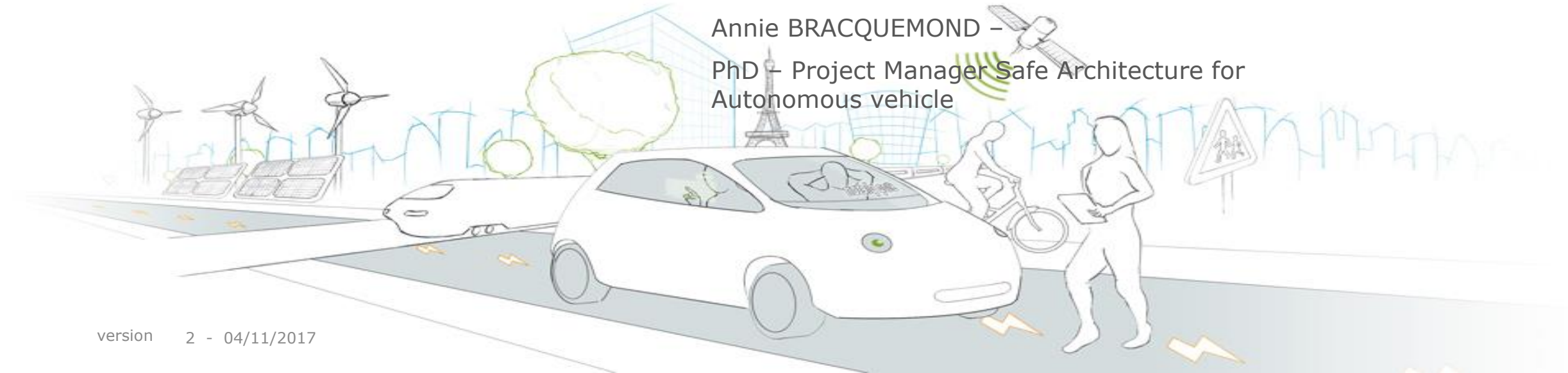
SIP-ADUS 2017

Strategic Innovation Promotion Program - Automated Driving for Universal Services

14th of November 2017 - TOKYO - Japon

Annie BRACQUEMOND –

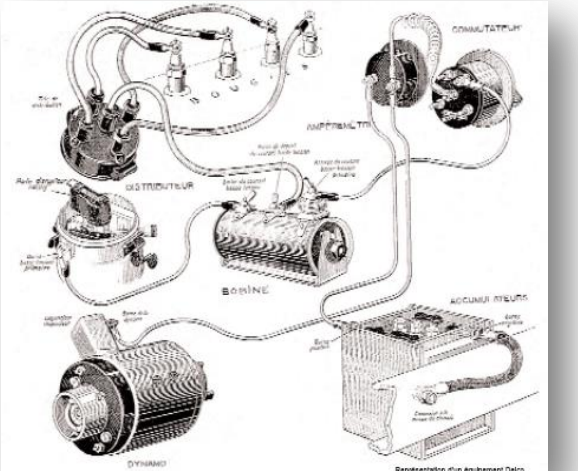
PhD – Project Manager Safe Architecture for Autonomous vehicle

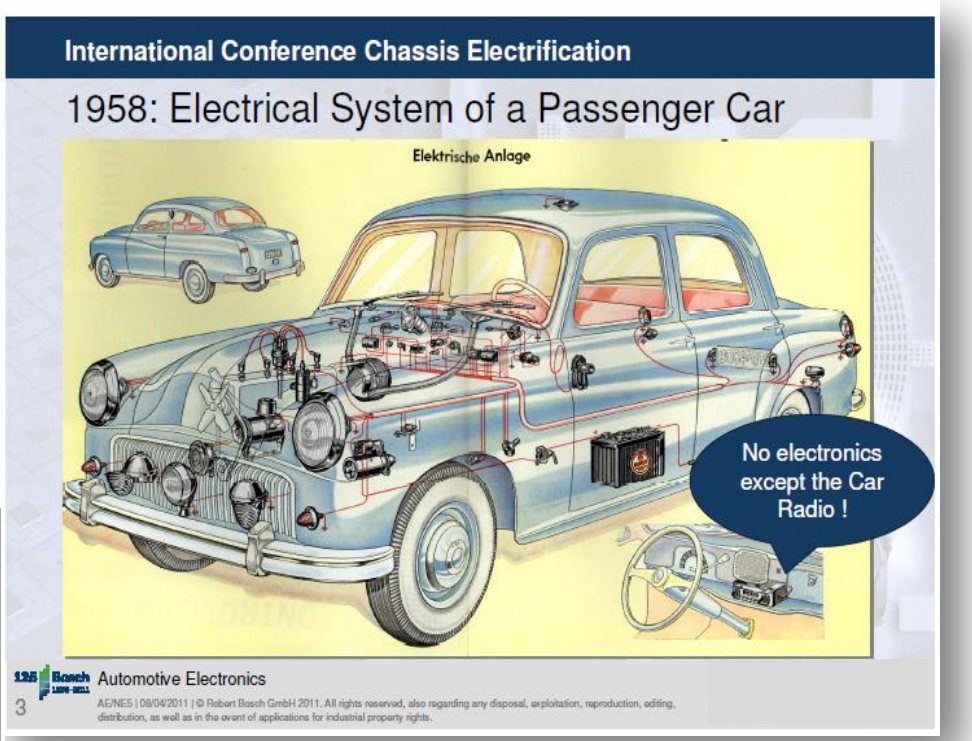


version 2 - 04/11/2017

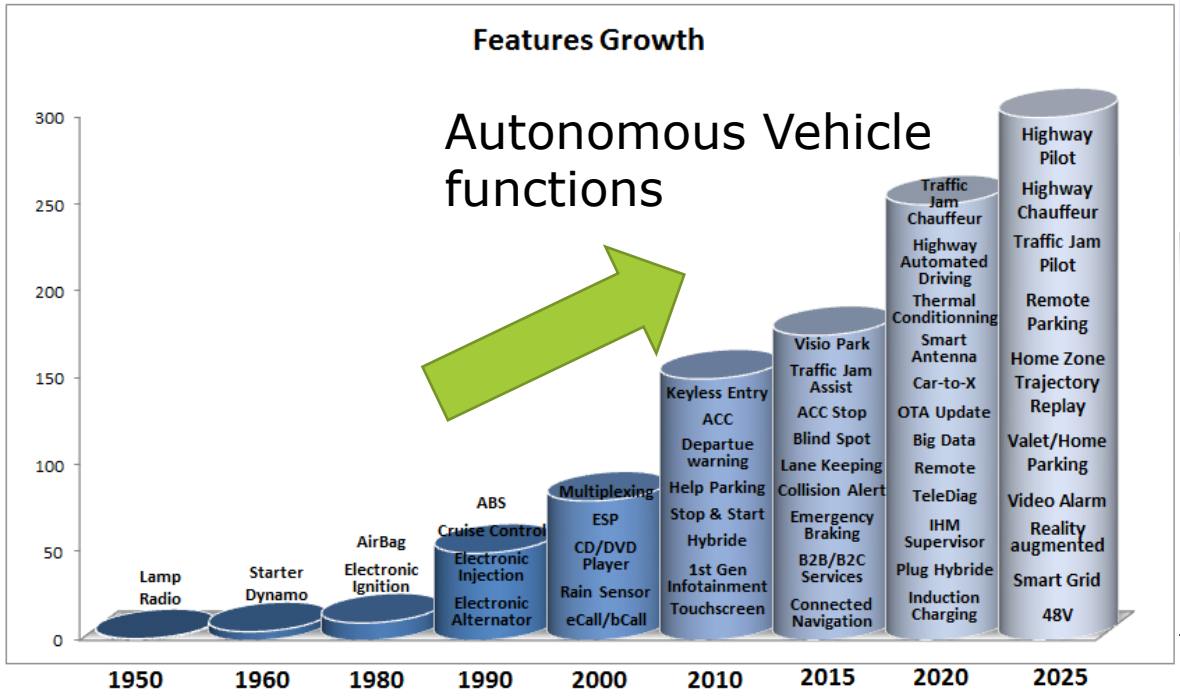
MORE AND MORE COMPLEX FUNCTIONS TO AUTONOMOUS VEHICLE

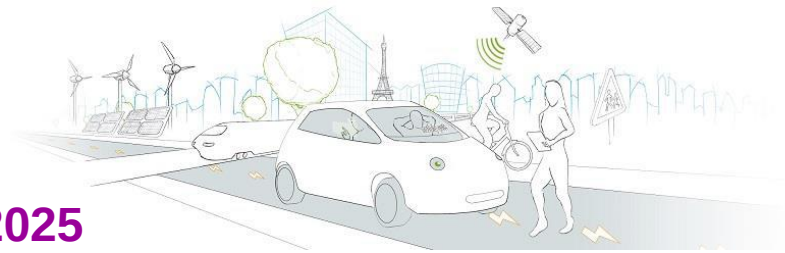
1930





1958





2025

INSTITUT VEDECOM

AUTOMOTIVE ATTACKS

Security researcher warns cars can be hacked to remotely take control

Jonathan Brossard said of his work for vehicle manufacturers Europe, it's possible to sit at desk, hack and remotely seize control of a car on the other side of the globe

Network World | Jun 1, 2014 12:03 PM PT

TECH 2/23/2015 @ 6:15AM | 28 609 views

14-Year-Old Hacks Connected Cars With Pocket Money

+ Comment Now + Follow Comments

Jeep experience

https://www.youtube.com/watch?v=MK0SrxBC1xs

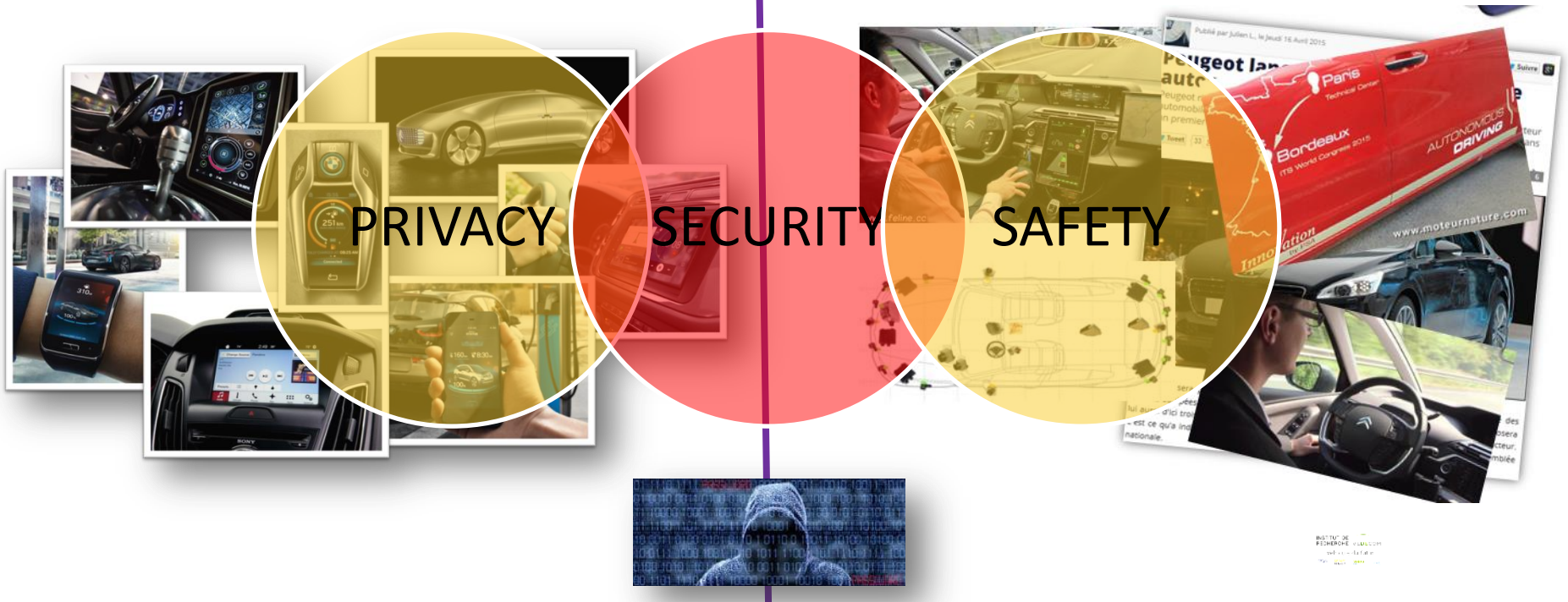
2010	2011	2013	2015	2016	2017
Experimental Auto Security Analysis	Comprehensive Analyses of Auto Attack Surfaces	Physical Hacking	Remote Attacks	Nissan Leaf Hack	
			BMW ConnectedDrive Hack	Mitsubishi Outlander Hack	
			GM OnStar Hack	BMW Web Applications Hack	
			Chrysler Jeep Hack	Chrysler Jeep Hack 2	
			Tesla Model S Hack	Attacks Against Sensors of Autonomous Vehicles	
			Audi TT Hack	Tesla Model S Remote Hack	
				Tesla Smartphone App Hack	

Q4 2016

CONNECTED & AUTONOMOUS VEHICLE

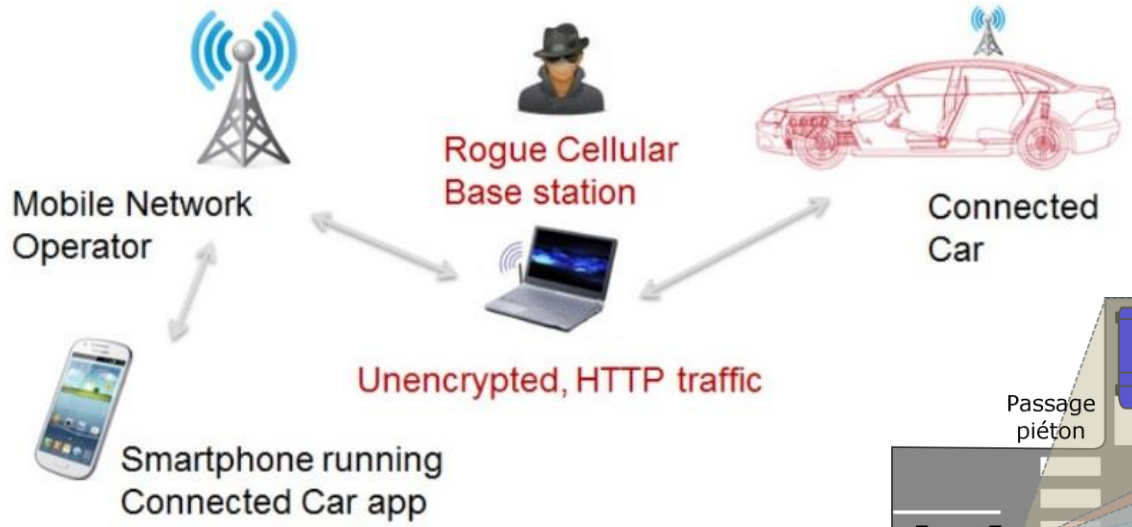
Connected Vehicle

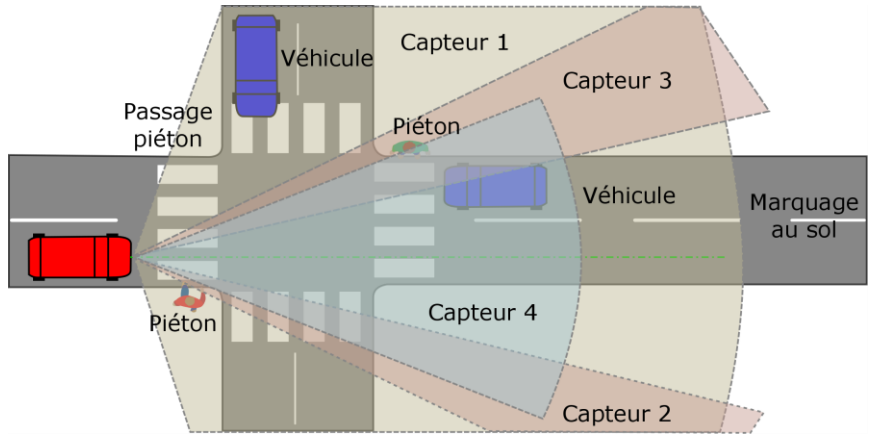
Autonomous Vehicle

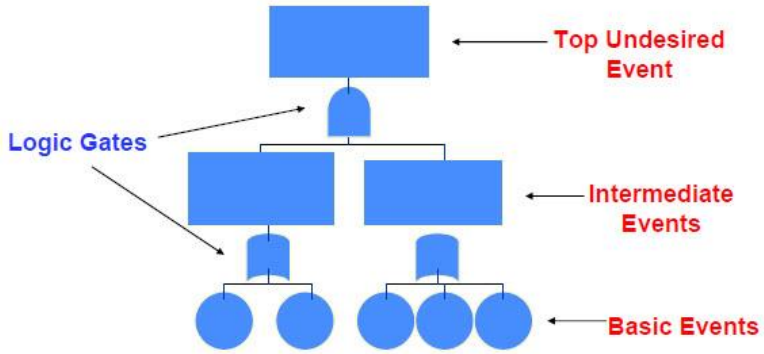


Opening data is a dangerous operation
Data protection is essential
Firewall is fundamental

RELATIONSHIP BETWEEN SECURITY AND SAFETY



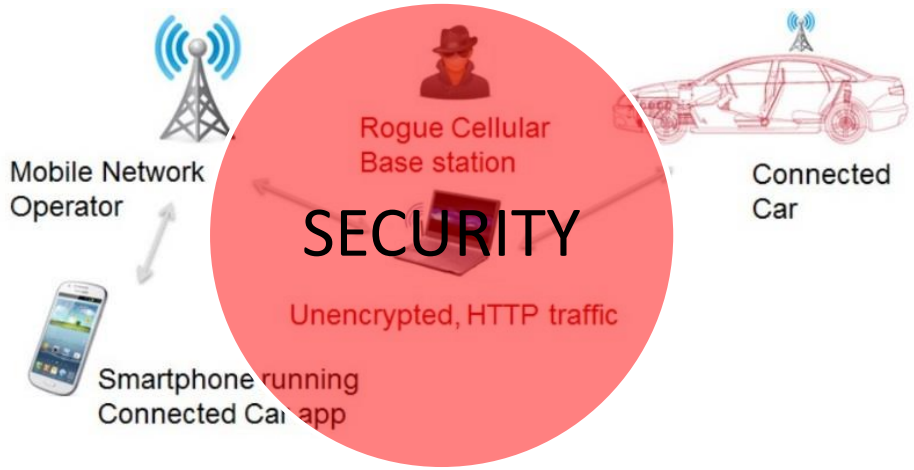




SECURITY ARCHITECTURE

Principles of Security

- ❑ Adapt countermeasures to attacker capabilities
- ❑ Take into account security requirements e.g. accessibility
- ❑ Protect all functions handling input exterior to the connected system
- ❑ Identification of data flows which are easy to generate or control (copy or create)
- ❑ Prevent the system from accepting non valid data



Methods :

- ❑ *Authentication* Methods (password, keys…)
- ❑ *Data origin* authenticity e.g. information origin identification
- ❑ *Encryption*/Decryption mechanisms
- ❑ *Plausibility check*
- ❑ Verification of *confidentiality* and authenticity of communications

Attacks :

- ➢ Exploit known vulnerabilities on HW/SW
- ➢ Test with basic attacks (e.g. fuzzing, open ports, …)
- ➢ Use attack applications (e.g. metasploit)
- ➢ Exploit failures in HW (ECUs)

SAFETY ARCHITECTURE

Safety Principles :

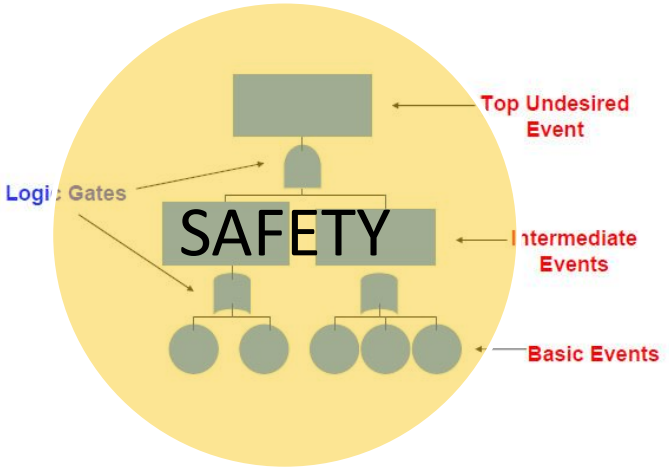
- ❑ Identification of data or parameters which contribute to the safety
- ❑ Identify low statistical level of reliability/safety for each parameter
- ❑ Identify errors HW/SW
- ❑ Ensure CPUs and buses are not overloaded

Architecture Principles

- ➢ HW/SW Partitioning
- ➢ Redundancy HW and SW
- ➢ Parallel..
- ➢ Networks to compare, separate,…
- ➢ Split complex functions
- ➢ …

Methods

- ❑ Hazard Analysis / Fault Trees
- ❑ Reliability rate, Proven by use
- ❑ Separation and redondance of flow for safety parameters
- ❑ Compute safety values twice with two different computation techniques in parallel.
- ❑ Watchdogs to analyze error data sequences (data flow)
- ❑ Ensure that timing specifications are met



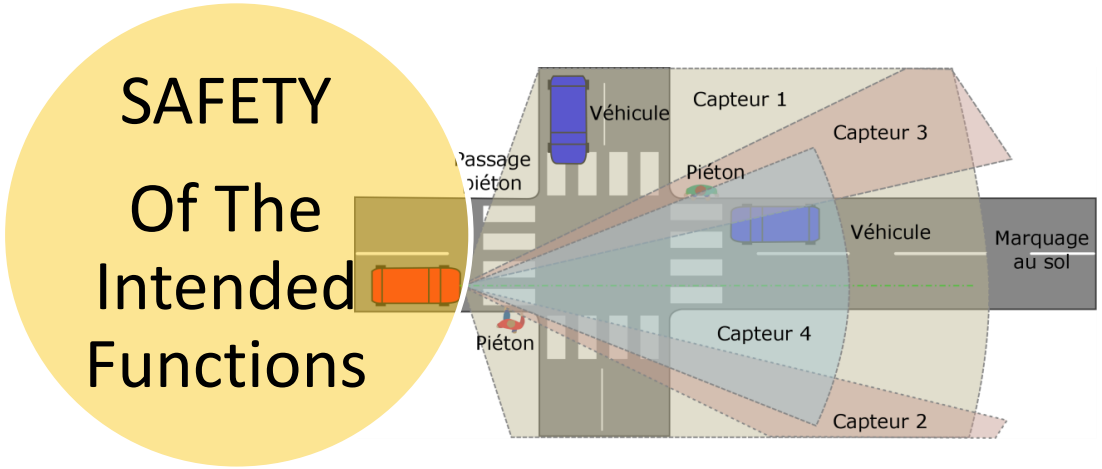
SOTIF ARCHITECTURE

Safety Of The Intended Functions :

- ❑ Confidence of perception algorithms
- ❑ Comparaison between strongly correlated functions to detect incoherence
- ❑ Environmental conditions of AV : which disturbe perception (rains, fog,..)
- ❑ Decision defining the best trip amongst the safe ones
- ❑ Knowledge of sensor performance and the related limits
- ❑ Historicals
- ❑ Prediction safe trajectory
- ❑ Lost Sensor messages detection (radar/GPS/…)
- ❑ Analysis of desired behavior, performance, timing,

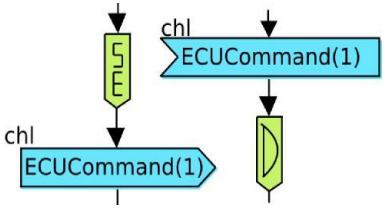
Methods

- ❑ Reliability algorithm SW or Sensors HW
- ❑ Parameter redondances comparison
- ❑ Abnormal latency detection
- ❑ Safety Mode refuge, safety states,..
- ❑ Compute safety values twice with two different computation techniques in parallel.
- ❑ States Graph to search if Error states cannot be reached

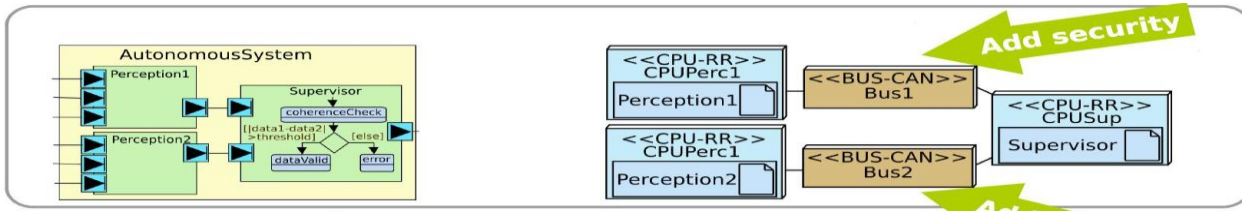


MECHANISM EXAMPLES

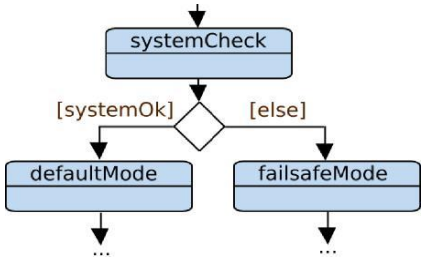
DATA ENCRYPTION / AUTHENTICATION of safety data contributes to associate a hight level of confidence to this command but increase latency (measurement between safety critical events)



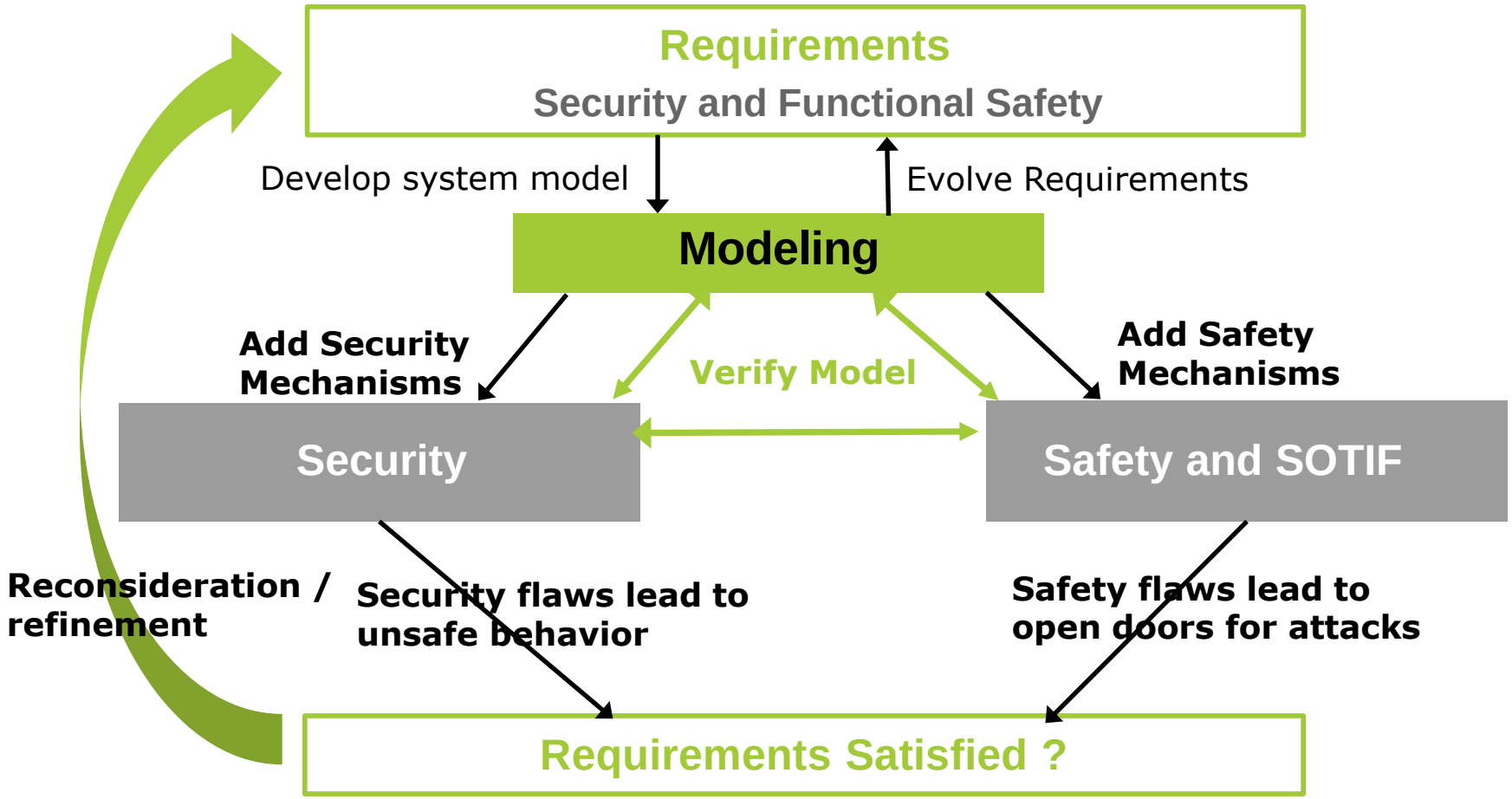
REDUNDANCY
contributes to Coherence Check for SOTIF to identify the best perception CPU or the best perception algorithm, and identify an incoherent replay attack. But there are more doors to attack.



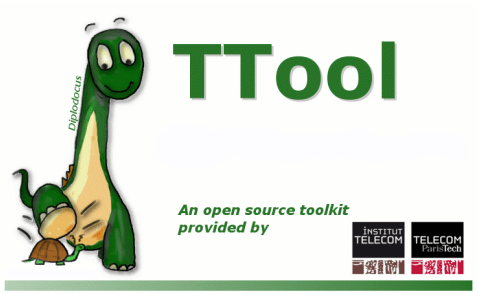
FAILSAFE MODE are associated with SOTIF refuge mode :
Safety decision to commute between SW modules, if a module failed by attacks or SW errors.

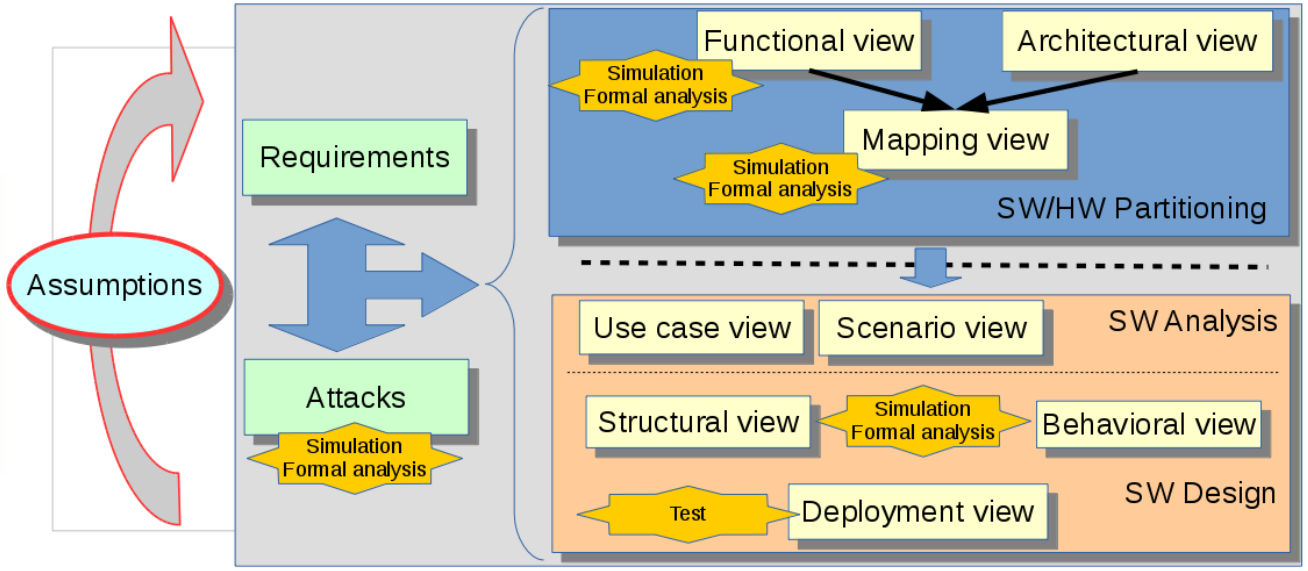


SAFE AND SECURE DESIGN METHODOLOGY



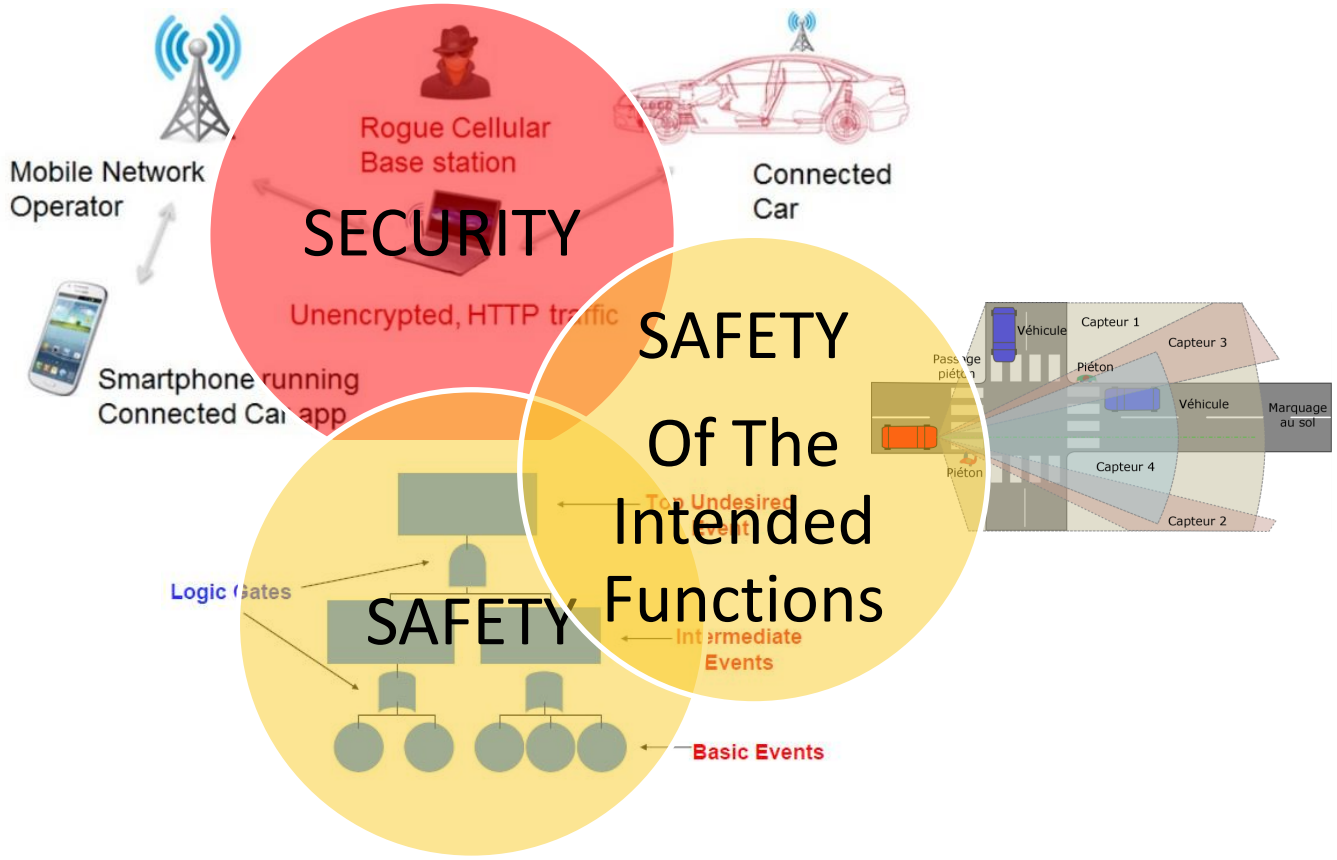
TOOLS





- Describe system requirements
- Model system behavior and architecture
- Automatically verify safety, performance, and Security
- Add safety mechanisms (redundancy, failsafe mode)
- Automatically generate security mechanisms
- Refine model over iterations

CONCLUSION : PROTECTION AGAINST ATTACKS WITH SECURITY AND SAFETY ARCHITECTURE



Thank’s for your attention

Questions…