AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

CS1 – Industrial and Automation Control Systems

EAB Workshop 1
11-12 September, 2017

Benito Caracuel
Case Study CS1 Leader
Schneider Electric

CS1 Description

- Focused on the Smart Grid domain
- Industrial Control Systems (ICS) and **Remote Terminal Units (RTU)** for the electrical substation management
- Critical Infrastructure -> Safety and Security as main concerns for manufacturers and utilities
- 60% of incidents involving process control systems occur during the specification, design and implementation phases
- IEC 61508 (safety) and IEC 62443 / IEC 62351 (security)

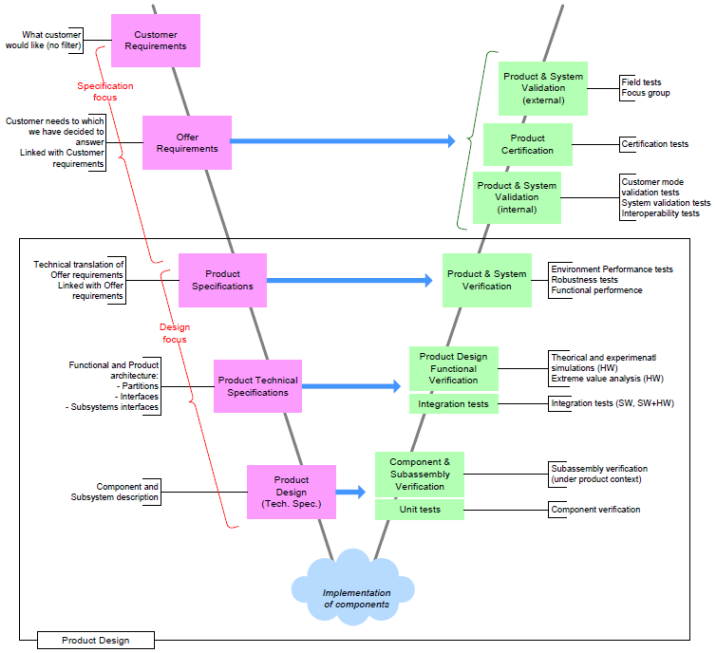
CS1 Description

Saitel® RTU platform:

- Real time control device
- Acquisition and communication functions
- Multiple signals and communication ports
- Cybersecurity
- OS Linux
- Baseline® software platform
- Tools: Easergy Builder (configuration) and webApp (monitoring)

CS1 Business Interest

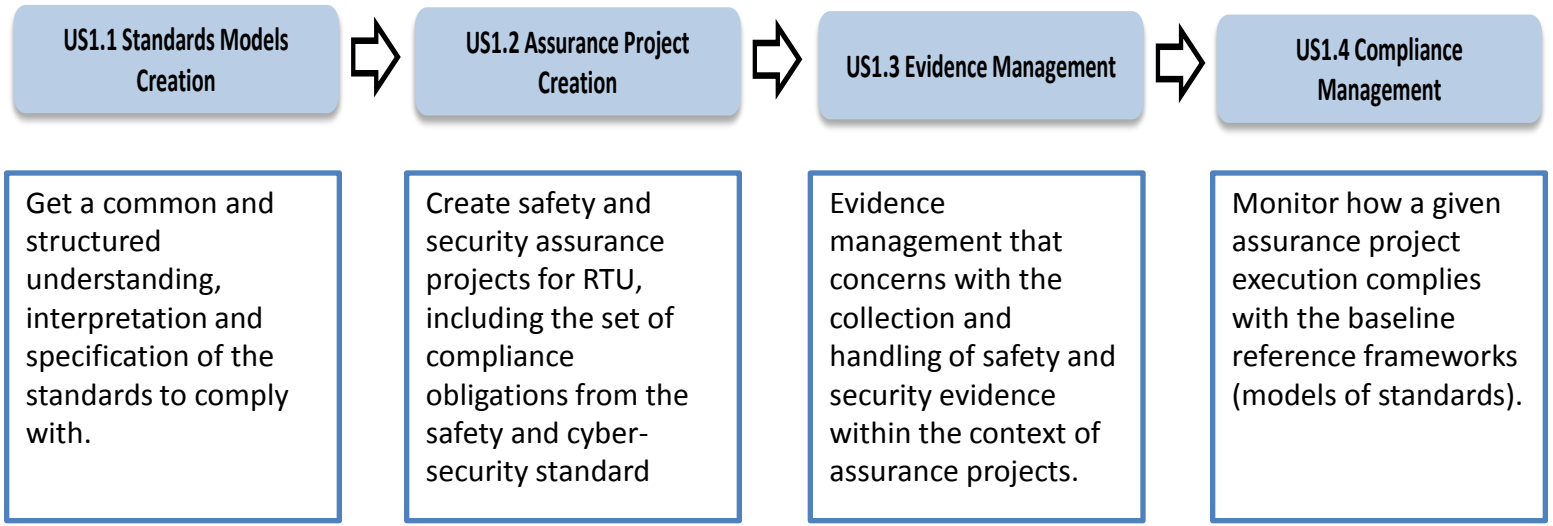
- NOW -> RTU Verification and Validation plan.
- AMASS Improvements: safety and security integration in the RTU design process, safety and security assessment, SIL estimation.
- Business needs -> reduce effort and cost in assurance and certification processes.



⇒ *Thanks to AMASS tools, the RTU designer will introduce the safety and security aspects in the early phases of the RTU process. This will reduce the effort and cost related to the safety and security analysis, compliance and certification processes.*

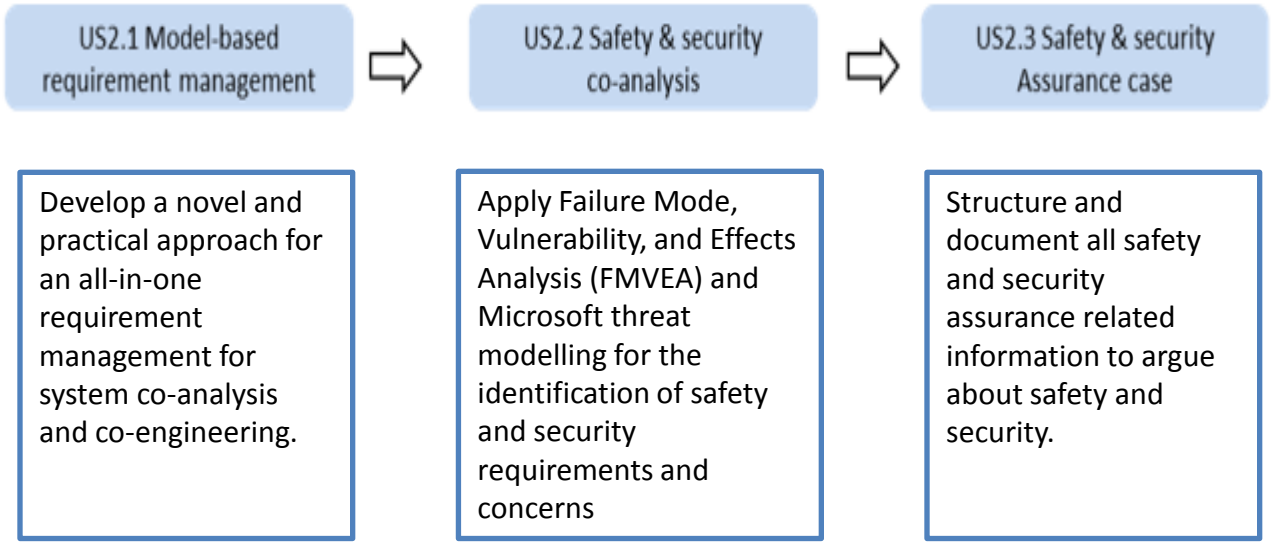
CS1 Usage Scenarios

US1. Compliance management



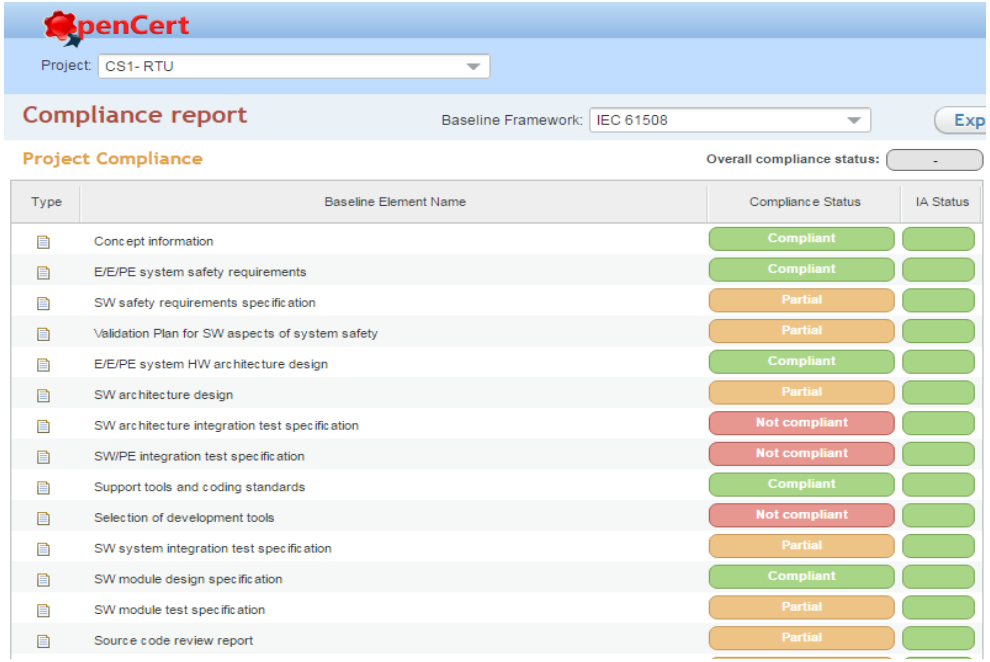
CS1 Usage Scenarios

US2. Safety and security co-assessment



CS1 First Prototype (US1)

- Standards modelling (IEC 61508-3 & IEC 62443-4-2)
- RTU Assurance projects (Safety & Security)
- RTU Evidence models (Safety & Security)
- RTU Compliance report (IEC 61508)



Type	Baseline Element Name	Compliance Status	IA Status
	Concept information	Compliant	
	E/E/PE system safety requirements	Compliant	
	SW safety requirements specification	Partial	
	Validation Plan for SW aspects of system safety	Partial	
	E/E/PE system HW architecture design	Compliant	
	SW architecture design	Partial	
	SW architecture integration test specification	Not compliant	
	SW/PE integration test specification	Not compliant	
	Support tools and coding standards	Compliant	
	Selection of development tools	Not compliant	
	SW system integration test specification	Partial	
	SW module design specification	Compliant	
	SW module test specification	Partial	
	Source code review report	Partial	

Thank you for your attention!

ECSEL Joint Undertaking

European Commission

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

Case Study 3
Cooperative ACC / Platooning

BERNER & MATTNER
AN ASSYSTEM COMPANY

First EAB Workshop
Trento, September 11, 2017

Helmut MARTIN
T6.4 Leader
Contributor to WP2, WP4, WP6

virtual vehicle

Overview

- Involved Partners
- Description and Business Interest of CS3
- Case Study 3 Usage Scenarios
- First Prototype - Actual Working Status

Case Study 3: Involved Partners

BERNER & MATTNER
AN ASSYSTEM COMPANY

Case Study CS3

BERNER & MATTNER
AN ASSYSTEM COMPANY

tecnalia Inspiring Business

virtual vehicle

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

ANSYS
medini™ analyze

ALL4TEC

MÄLARDALEN UNIVERSITY
SWEDEN

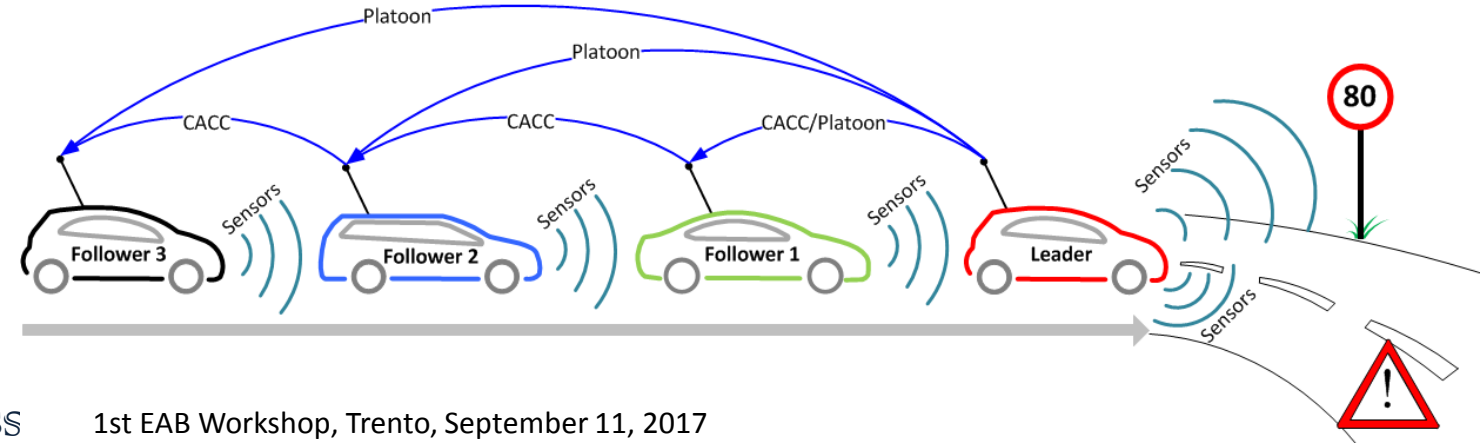
Overview

- Involved Partners
- Description and Business Interest of CS3
- Case Study 3 Usage Scenarios
- First Prototype - Actual Working Status

Case Study CS3: Cooperative ACC / Platooning

Description

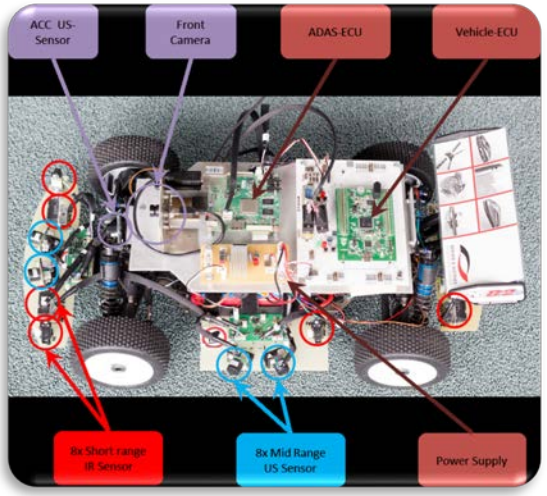
- Up to four cars participate in a motorway platoon
  ⇨ represented by four autonomous model cars (1:8 scale)
- Different vendors with different capabilities meet on the highway randomly and join a platoon
- Intermediate solution ACC (sensors) and CACC (WiFi)
- Failures in any of the cars as well as in communication breaks may occur at any time
- Safety Goal «No rear crash» must be assured at any time



Case Study CS3: Cooperative ACC / Platooning

Description

- Use Case supports research and development of autonomous driving
- Distinguish between “freeway” and “laboratory” use cases
  - Realistic driving conditions
  - 2 simultaneous and interacting platoons (e.g. split or join platoon)
  - Laboratory environment only simulate one-lane-freeway
  - CACC/Platoon-function is designed for full-speed-range (FSR-CACC)



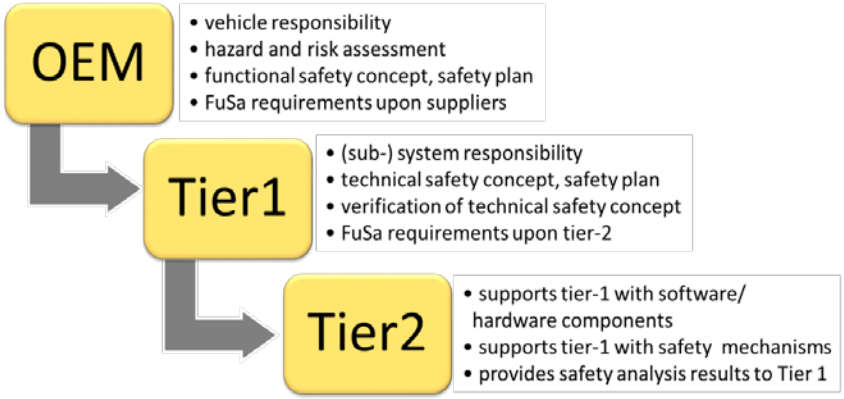
- Model vehicles with different equipment to simulate platoons from different OEM‘s

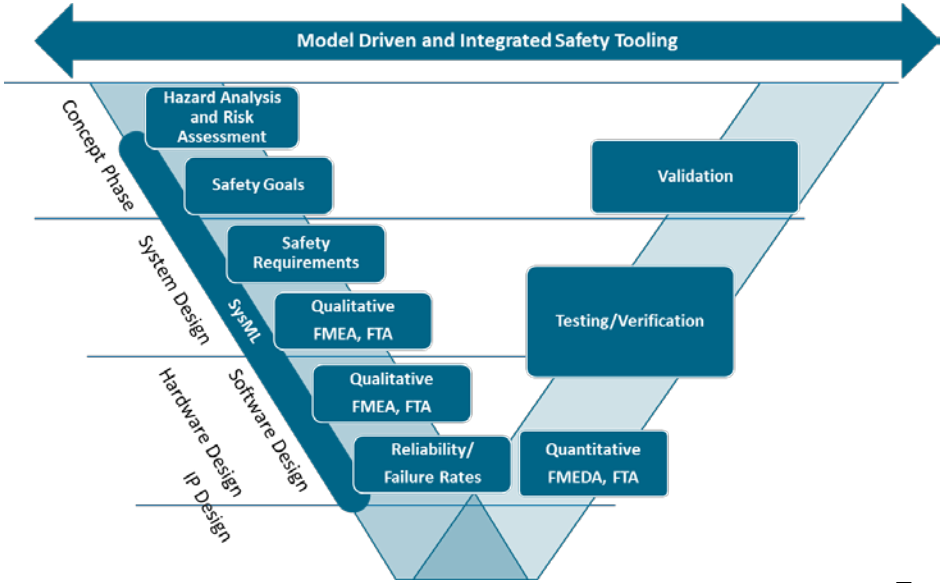
Case Study CS3: Cooperative ACC / Platooning

Business Interest

- Model-based and contract-based development
- Derivation of safety analysis from system architecture
- Safety solution for systems-of-systems

  ⇨ No single manufacturer – supply-chain!
- Relating system models to safety case artefacts



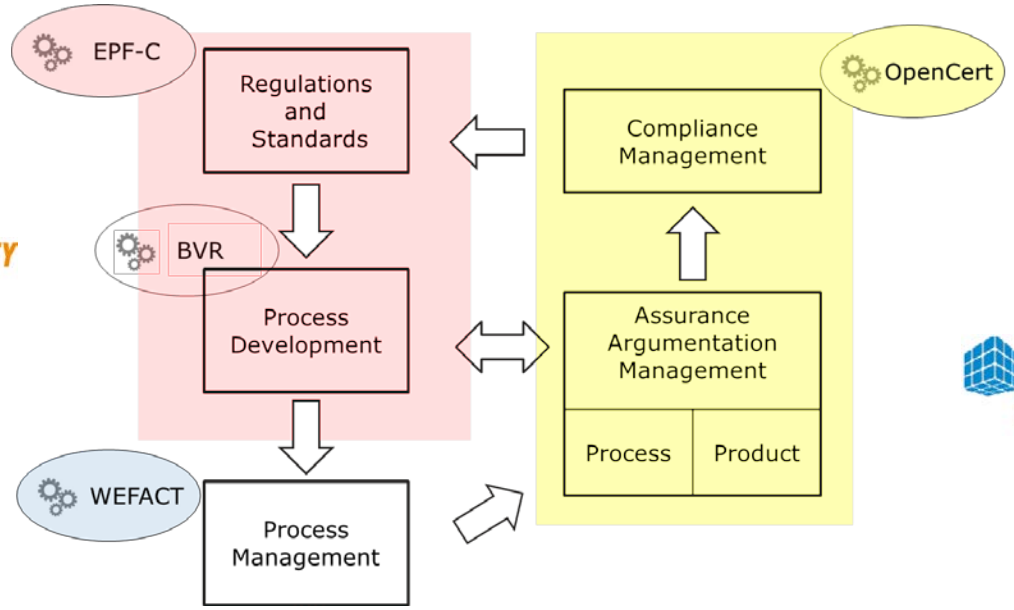


Overview

- Involved Partners
- Description and Business Interest of CS3
- Case Study 3 Usage Scenarios
- First Prototype - Actual Working Status

Safety and security co-engineering

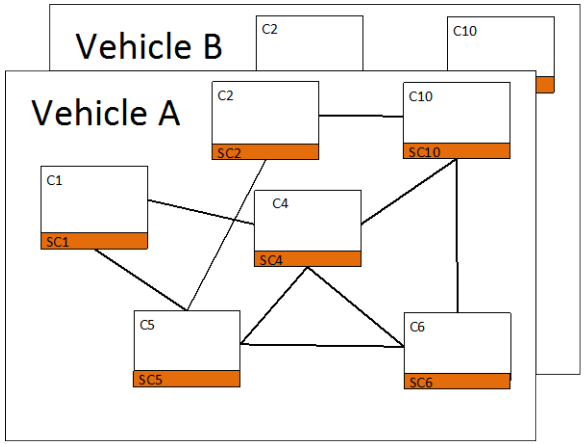
- Process modelling (ISO 26262, SAE J3061) [EPF-C]
- Process and variability management [WEFACT, BVR]
- Co-engineering analysis [MediniAnalyze, FMVEA]
- Assurance case for safety and security [OpenCert]



MÄLARDALEN UNIVERSITY SWEDEN

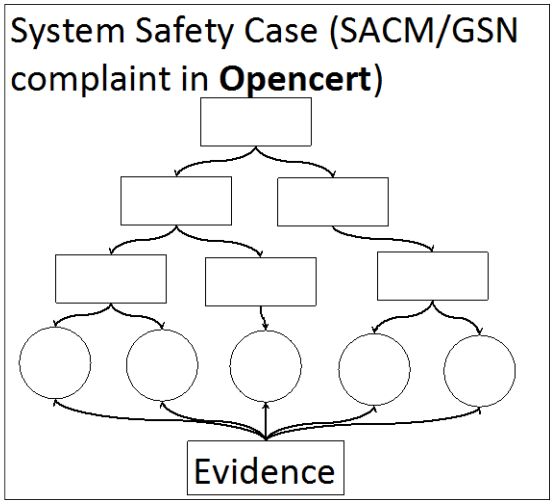
Assuring degradation cascades of car platoons via contracts

- Safety assurance approach for cooperative SoS exhibiting degradation cascades
- Boundary of the system broadened from a single vehicle to multiple vehicles for a single function
- System modelling [CHESS] and contract refinement [OCRA]
- Argumentation generation from the contracts [OpenCert]



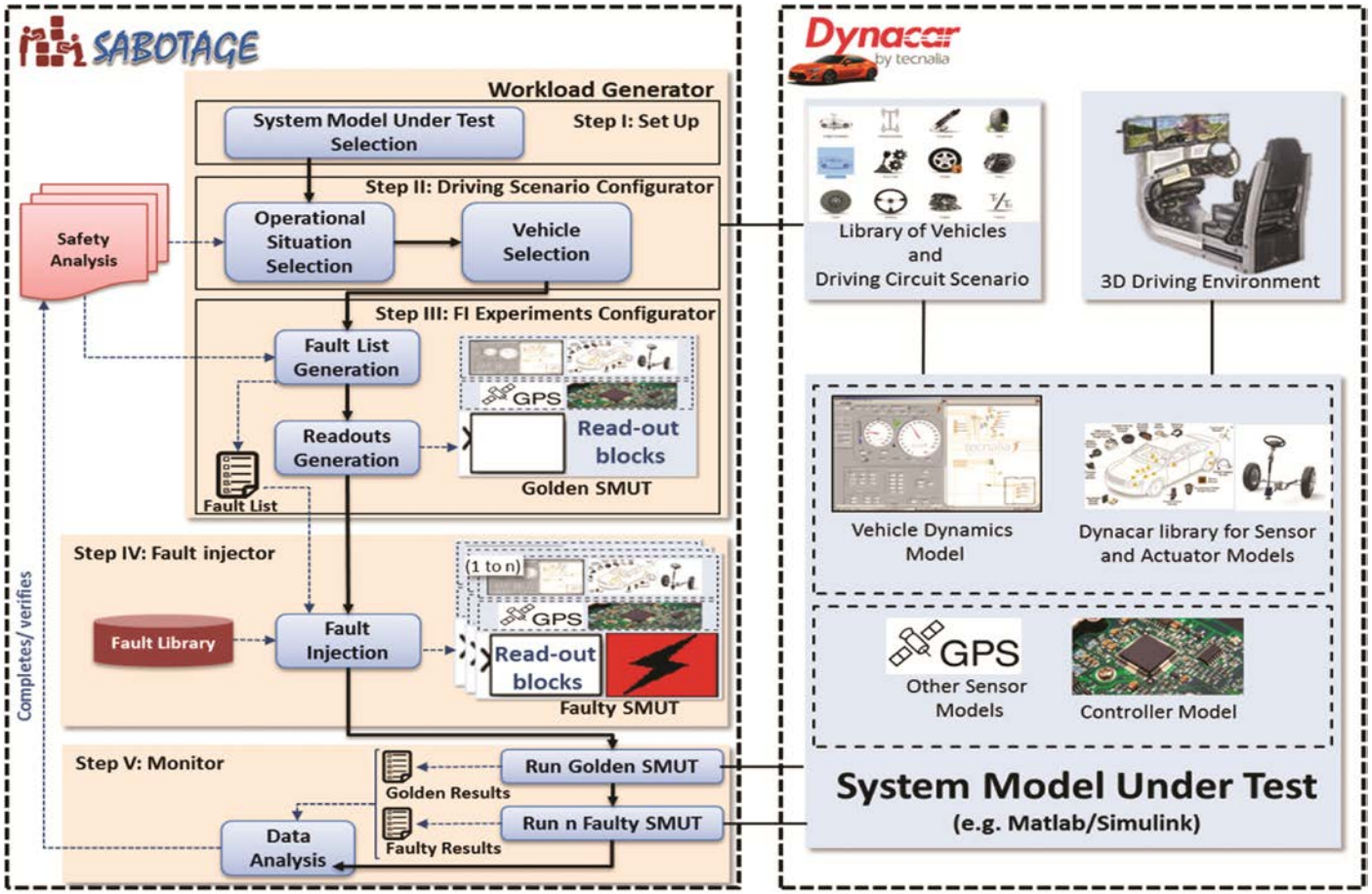
CHESS system model with assumption guarantee contracts

Contract validity and refinement checks in **OCRA**



Simulation-based Fault Injection

- Early safety assessment
- Generate the failure logic



Overview

- Involved Partners
- Description and Business Interest of CS3
- Case Study 3 Usage Scenarios
- First Prototype - Actual Working Status

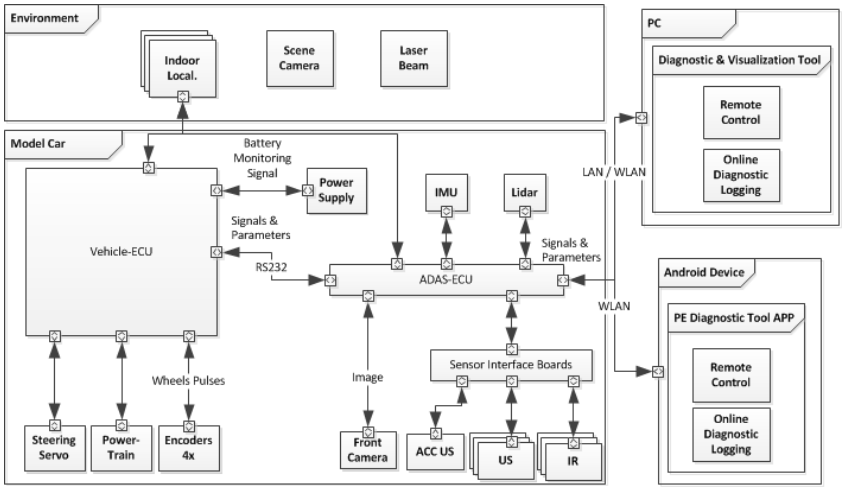
Case Study CS3: Actual working status

First Prototype Case Study

- Vehicle-ECU - Implementation of actuator controlling and ego-detection
- ADAS-ECU - Implementation of ADAS- and ADV-related functions
- Implemented ADAS- and ADV-related functions:
  - Lane recognition V0.1
  - Lane keeping V0.2
  - CACC/Platooning V0.2
  - Object detection V0.3
  - ACC V1.0

- Lane-Recognition and -Keeping V1.0 (Early 2018)
- CACC/Platooning V1.0 (Mid 2018)
- Object-Detection V1.0 (tbd)
- Environment Mapping (tbd)
- Park Slot Detection (tbd)

- Use Cases and System architecture models with interfaces between model cars and environment available

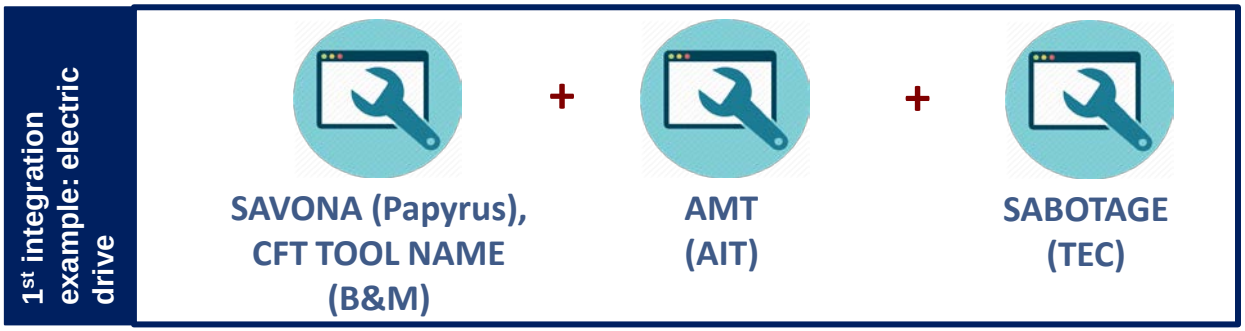


Case Study CS3: Actual working status

First Prototype Usage Scenarios

- Process Variability Modelling and Management for Safety and Security [by EPF-C and BVR]
- Experience on SysML models facility and contract specification and refinement tool [by Savona/Papyrus+CHESS]
- Argumentation generation from contracts [by OpenCert]

  ⇨ Currently done manually, automation under construction
- Collaboration on contract-based specification (B&M) + assertion monitors (AIT) + fault injection (TEC)



Thank you for your attention!

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

CS5 – Railway Domain - Platform Screen Doors Controller

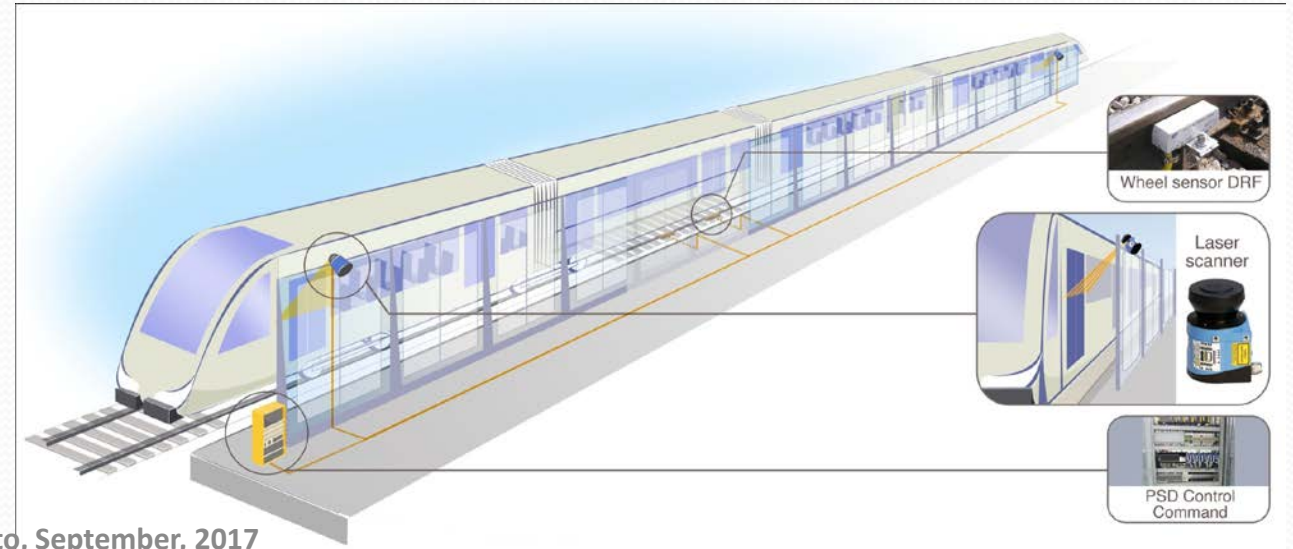
EAB Workshop 1
11-12 September, 2017

Thierry Lecomte, David Deharbe
Case Study CS5 Leader
ClearSy Systems Engineering

PSD Controller (Railways)

Case Study Specification

- COPPILOT São Paulo system installed in 2009 (SIL3 certified)
- Almost unique requirement: *"open safely the PSD in less than 200 ms"*
- System to be redesigned for each new metro line
- Safety case : a thesis demonstrating why the target is safe
- Security: not yet a formal requirement but
  - our systems are partly operated remotely
  - new architecture for communication-based devices



PSD Controller (Railways)

Business Interest

- **G1**: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort

Usage Scenario 1 – generation of Frama-C asserted C code from B models

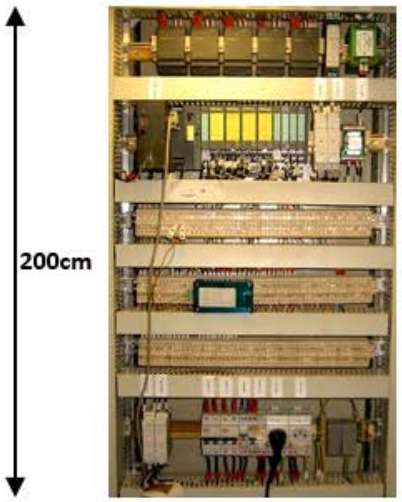
- Improving the code review process to lower verification costs and risks
  - Better level of confidence in the software
  - Code peer review for safety critical functions is of paramount importance, as no certified code generator is used in the toolchain.

Usage Scenario 2 – support for system-level model, including safety and security aspects

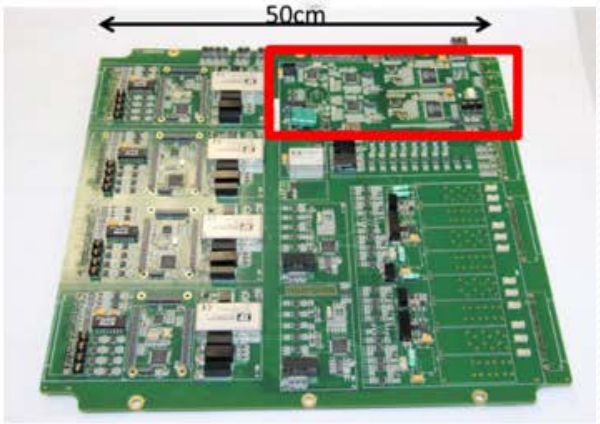
- Integrating seamlessly security study into existing safety case.
  - Security is not yet part of the safety case
  - Given the global tendency to have all systems connected, new risks due to this forthcoming connectivity have to be taken into account and introduced/combined to existing risks analysis.

PSD Controller (Railways)

- Key constraints:
  - Ability to fully address in-house existing systems (functional specification, architecture)
  - Ability to take into account product line features (reuse and adapt)
  - Ability to take into account technology improvements (PLC -> LCHIP): modelling tools need to adapt to products and not the contrary



Sao Paulo L2 & L3 (2009)

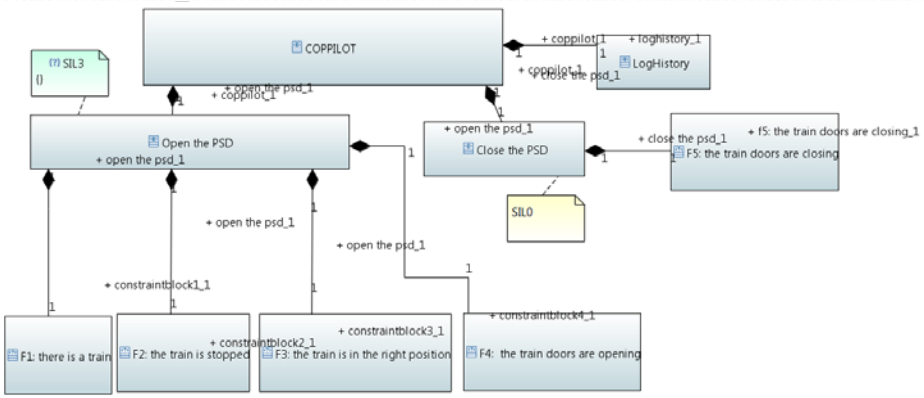


Coppilot.M board PLC SIL4

PSD Controller (Railways)

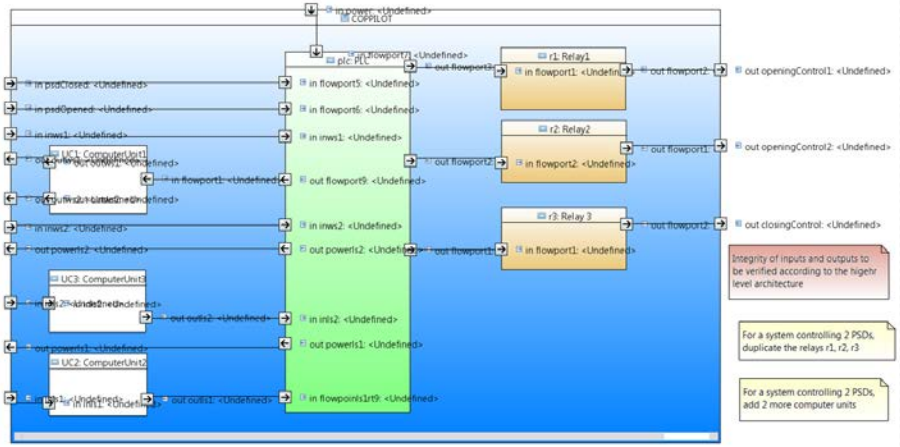
AMASS Tools Evaluation

- System functional modelling (Papyrus



System Functions

- Architecture modelling (Papyrus)

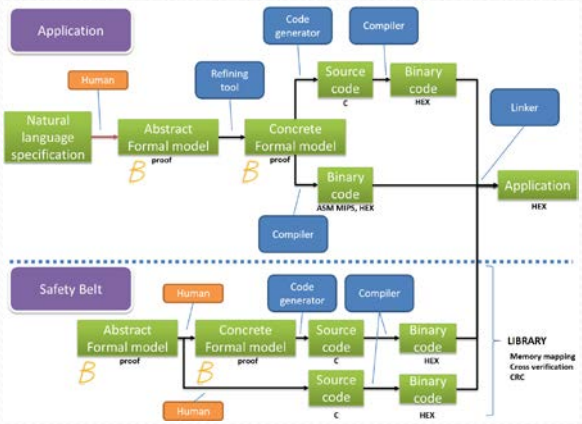


Internal COPPILOT Cubbicle Architecture

PSD Controller (Railways)

AMASS Tools Evaluation

- Integration of most elements from inputs documents
- Functional and architecture modelling completed with partners (discussions, Q/A)
- Code generation assessment
  - Software partly formally developed with the B method (formal models for specification and program, code generation from program model)



- Improvement of the level of confidence of the C code generated
  - Production of assertions in the C code, from the B formal models
  - Automatic proof with Frama-C

frama C Software Analyzers

PSD Controller (Railways)

AMASS Tools Evaluation

- Initiated this year:
  - Security analysis (PAPYRUS$_4$SECURITY)
  - Assessment on another COPPILOT system
    - Hardware not based on PLC but on in-house low cost high integrity execution platform
    - Different architecture / environment
      - Security issues are more pregnant (communication-based sub-system)
  - C Code generation assessment with Frama-C


BUREAU VERITAS Certification

Certificate

CLEARSY System Engineering
320, Avenue Archimède
Les Pléiades, Bât. A
13857 AIX EN PROVENCE Cedex 3

CENELEC EN 50126: 2000, EN 50128: 2011, EN 50129: 2003

COPPILOT.M Stockholm application « série A »

implementing the SIL3 safety function
"Automatic Sliding Doors (ASD) Opening Authorization"

following the description, configuration & limitations defined in appendix 1

Certificate N°: 6393741

Date of issue: 03rd March, 2017

COPPILOT.M Stockholm application « série A »

implementing the SIL3 safety function
"Automatic Sliding Doors (ASD) Opening Authorization"