ECSEL
Joint Undertaking

European
Commission

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 - Industrial and Automation Control Systems (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 - Industrial and Automation Control Systems (Schneider Electric)

CS1 Description

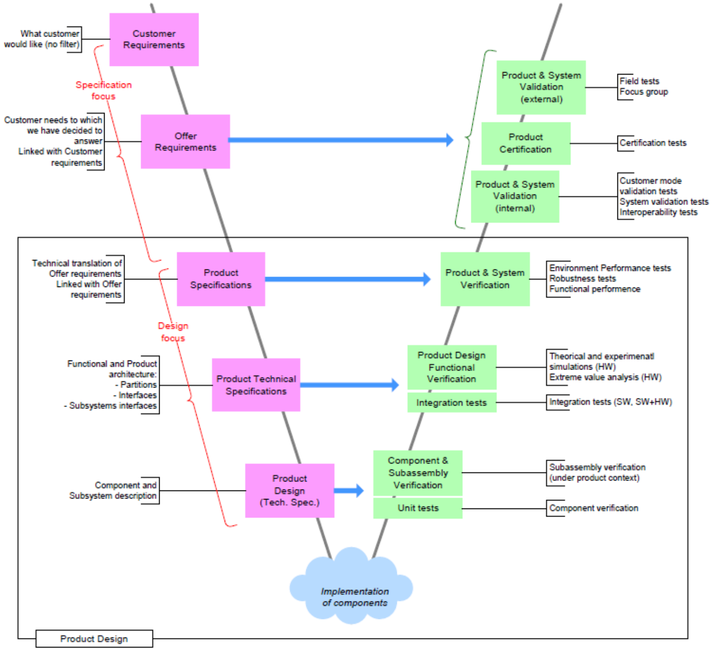
Saitel® RTU platform:

- 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 - Industrial and Automation Control Systems (Schneider Electric)

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.

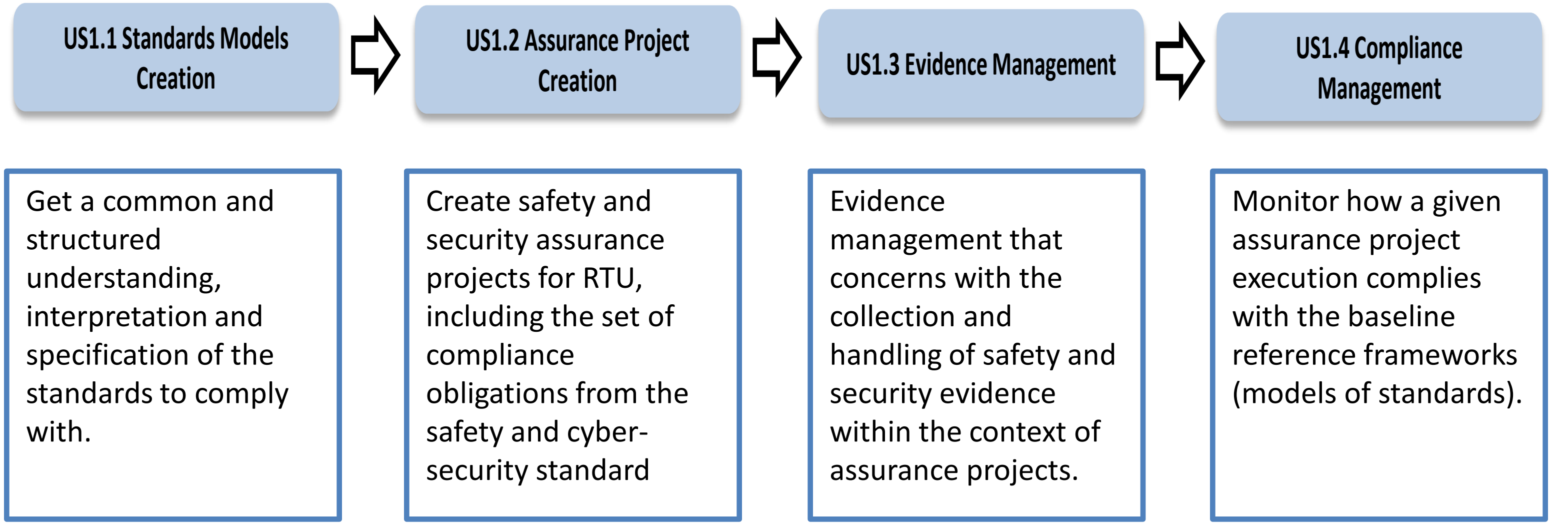

What customer would like (no filter)
Customer Requirements
Specification focus
Customer needs to which we have decided to answer
Linked with Customer requirements
Offer Requirements
Product & System Validation (external)
Field tests
Focus group
Product Certification
Certification tests
Product & System Validation (internal)
Customer mode validation tests
System validation tests
Interoperability tests
Technical translation of Offer requirements
Linked with Offer requirements
Product Specifications
Product & System Verification
Environment Performance tests
Robustness tests
Functional performence
Design focus
Functional and Product architecture:
- Partitions
- Interfaces
- Subsystems interfaces
Product Technical Specifications
Product Design Functional Verification
Theorical and experimenatl simulations (HW)
Extreme value analysis (HW)
Integration tests
Integration tests (SW, SW+HW)
Component and Subsystem description
Product Design (Tech. Spec.)
Component & Subassembly Verification
Subassembly verification (under product context)
Unit tests
Component verification
Implementation of components
Product Design

⇒ *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 - Industrial and Automation Control Systems (Schneider Electric)

CS1 Usage Scenarios

US1. Compliance management



US1.1 Standards Models Creation

Get a common and structured understanding, interpretation and specification of the standards to comply with.

US1.2 Assurance Project Creation

Create safety and security assurance projects for RTU, including the set of compliance obligations from the safety and cyber-security standard

US1.3 Evidence Management

Evidence management that concerns with the collection and handling of safety and security evidence within the context of assurance projects.

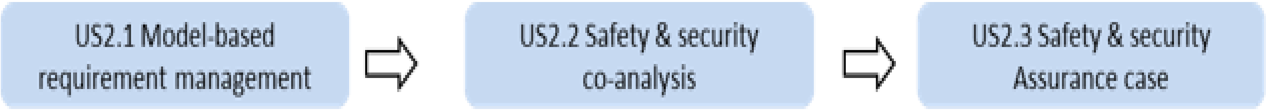
US1.4 Compliance Management

Monitor how a given assurance project execution complies with the baseline reference frameworks (models of standards).

CS1 - Industrial and Automation Control Systems (Schneider Electric)

CS1 Usage Scenarios

US2. Safety and security co-assessment


US2.1 Model-based requirement management
US2.2 Safety & security co-analysis
US2.3 Safety & security Assurance case

Develop a novel and practical approach for an all-in-one requirement management for system co-analysis and co-engineering.

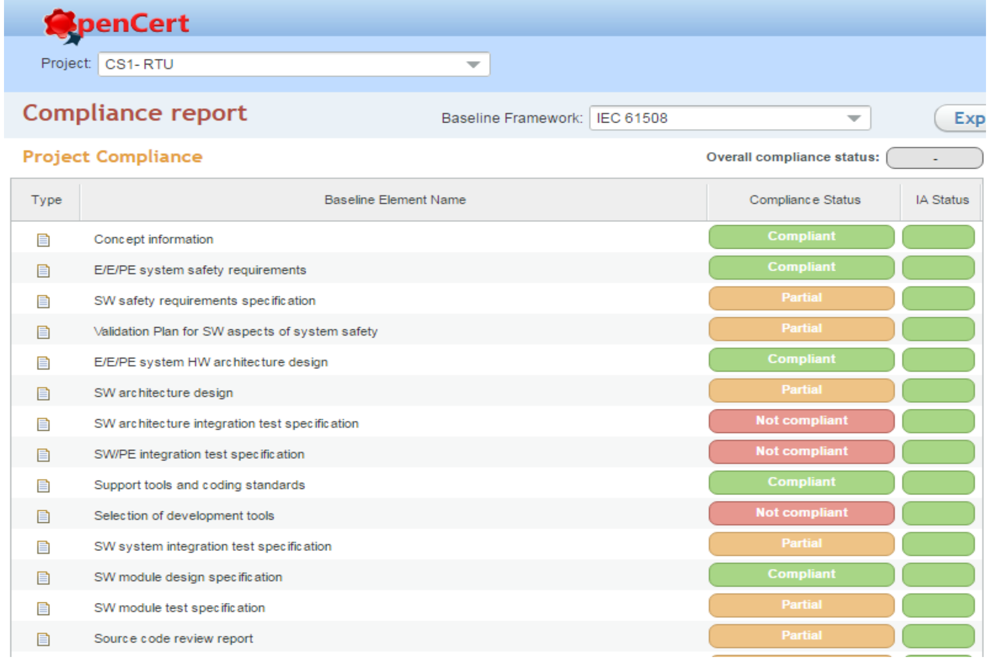
Apply Failure Mode, Vulnerability, and Effects Analysis (FMVEA) and Microsoft threat modelling for the identification of safety and security requirements and concerns

Structure and document all safety and security assurance related information to argue about safety and security.

CS1 - Industrial and Automation Control Systems (Schneider Electric)

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)



Project: CS1- RTU

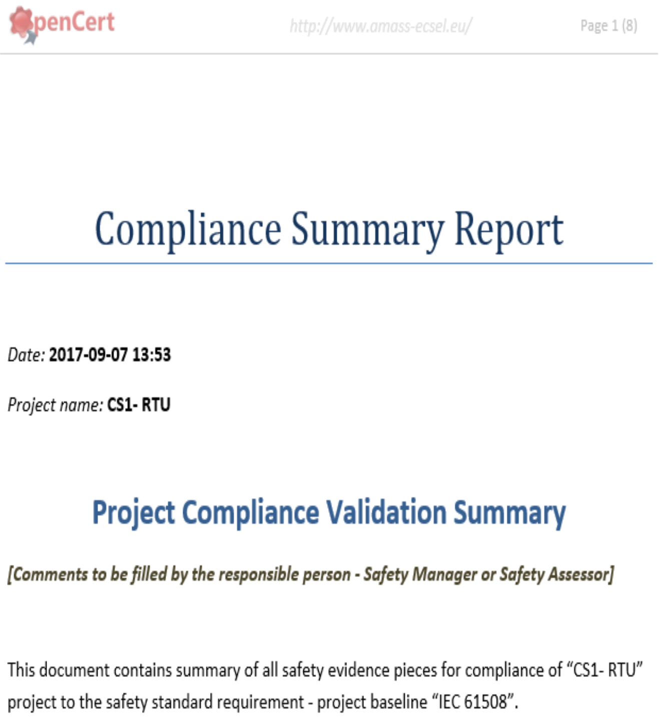
Compliance report

Baseline Framework: IEC 61508

Project Compliance

Overall compliance status: -

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	🟩



http://www.amass-ecsel.eu/ Page 1 (8)

Compliance Summary Report

Date: **2017-09-07 13:53**

Project name: **CS1- RTU**

Project Compliance Validation Summary

[Comments to be filled by the responsible person - Safety Manager or Safety Assessor]

This document contains summary of all safety evidence pieces for compliance of “CS1- RTU” project to the safety standard requirement - project baseline “IEC 61508”.

Thank you for your attention!

?