Safety Certification of Software-Intensive Systems with Reusable Components

Artemis: SafeCer

http://www.safecer.eu/

IEC 61508

Generic Industry standard, applicable to electrical / electronic / programmable electronic **safety-related** systems.

Safety Integrity Levels
SIL 1, SIL 2, SIL 3, SIL 4

ISO 26262

Automotive Industry standard, adaptation of IEC 61508 for electrical / electronic systems within **road vehicles**

Safety Integrity Levels
ASIL A, ASIL B, ASIL C, ASIL D

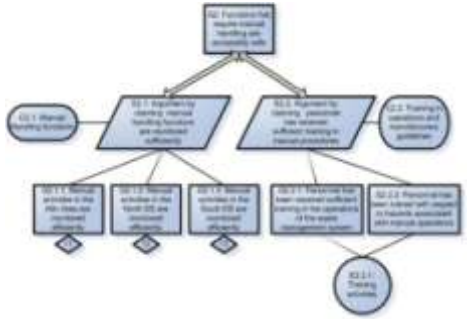
OMG SYSTEMS MODELING LANGUAGE SysML

Overview

- Background Information
- SafeCer Technology & Tools
- Demonstration & Evaluation
- HEV Use Case (AVL+VIF)

Challenges

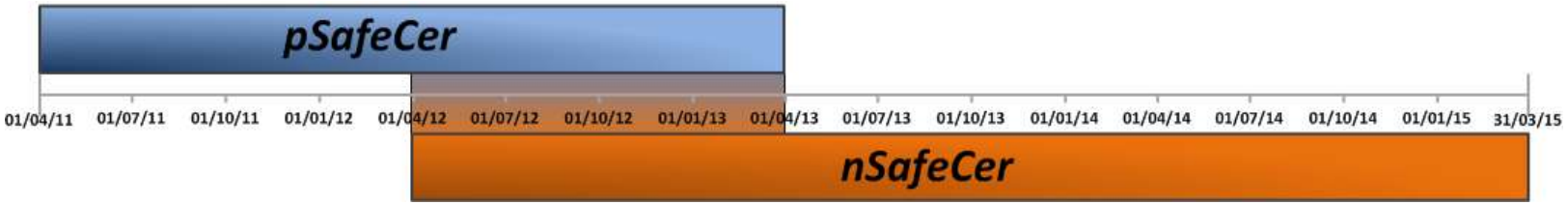
- Qualification, certification and verification of (sub-)systems accounts for up to **75% of the development cost**
- Component based design (CBD) has proven successful for system development but **dependability aspects** (e.g. safety) have not yet received full attention
- Techniques for **safety argumentation** exist but lack a unifying modelling and tool framework
- The issues above are present and similar in **many industrial domains**



(p+n) SafeCer ?

- SafeCer addresses the mentioned challenges
  - **SafeCer = pSafeCer + nSafeCer**
  - **4YR project – 2YR pilot started April 2011**

- pSafeCer
  - **Started April 1, 2011 (duration 2 years)**
  - **Focus on solution concepts**
  - **23 partners**



- nSafeCer
  - **Started April 1, 2012 (duration 3 years)**
  - **1 year overlap with pSafeCer**
  - **Focus on demonstration**
  - **29 partners**

SafeCer by Country

- **Austria**
  - AIT, VIF, AVL, TTTech, Thales Rail Signalling
- **France**
  - AdaCore, CEA-List, Delphi, Magillem Design Services, Thales Communications
- **Italy**
  - Akhela, Fondazione Bruno Kessler, Intecs, ResilTech, Vitrociset
- **Latvia**
  - Algorego, Latvian Railways, Riga Technical University
- **Spain**
  - GMV Aerospace & Defence, OSATU, Technical University of Madrid, Thales Alenia Space Espania, Traintic, ULMA, University of Montragon
- **Sweden:**
  - CrossControl, Mälardalen University, Quiviq, SP, Volvo CE, Volvo Global Trucks Technology

SafeCer

SafeCer by Competence

- **Avionics & Aerospace**
  - GMV Aerospace & Defence, Intecs, Thales Alenia Space Espania, Thales Communications, TTTech, Vitrociset
- **Automotive & CE**
  - AVL, Delphi, ResilTech, Virtual Vehicle Competence Center, Volvo CE, Volvo Global Trucks Technology
- **Railway**
  - Latvian Railways, Thales Rail Signalling, Traintic
- **Technology Providers**
  - AdaCore, Akhela, Algorego, CrossControl, Magillem Design Services, OSATU, Quiviq, ULMA Embedded Solutions
- **Research Institutes**
  - AIT, CEA-LIST, Fondazione Bruno Kessler, Mälardalen University, Riga Technical University, SP, Technical University of Madrid, University of Mondragon

Project Objectives

- **Overall objectives**
  - To **reduce the cost** of qualification, certification and verification
  - To **provide a framework** for compositional development and certification of safety relevant embedded systems

- **Main idea**
  - Process and technology that enable **composable qualification** and **certification**
  - **Qualification/certification** of systems/subsystems based on **reuse of** already established **arguments** for and properties of their parts.

- **Main industrial domains targeted:**
  - Automotive & Construction equipment
  - Avionics
  - Rail
  - Cross-domain






The SafeCer Approach

- **SafeCer component (meta) model**
  - Based on component meta models from different domains
  - Covering certification properties & contracts from domain specific standards
  - Foundation for a certification framework

- **Safety Cases complying to safety standards** (e.g. ISO 26262) → Top-down process
- **Derive the overall confirmation measures for verification and validation** → Bottom-up process
  - Evidence gathered by analysis and testing

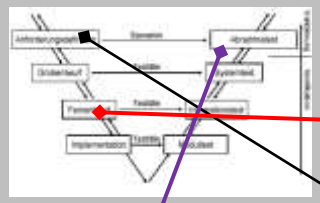
- **Development of a Certification Tool Framework**
- **Development of a Certification Artefact Repository**
- **Concrete instantiations and demonstrations**

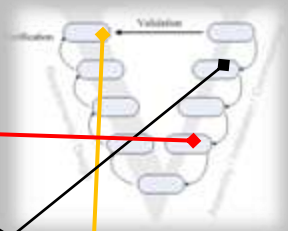
Background: Certification Process

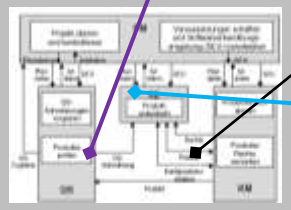
virtual vehicle
Vehicle EE & Software

Safety standard

Company







Documentation

Independent Safety Assessor

Improved Certification Process

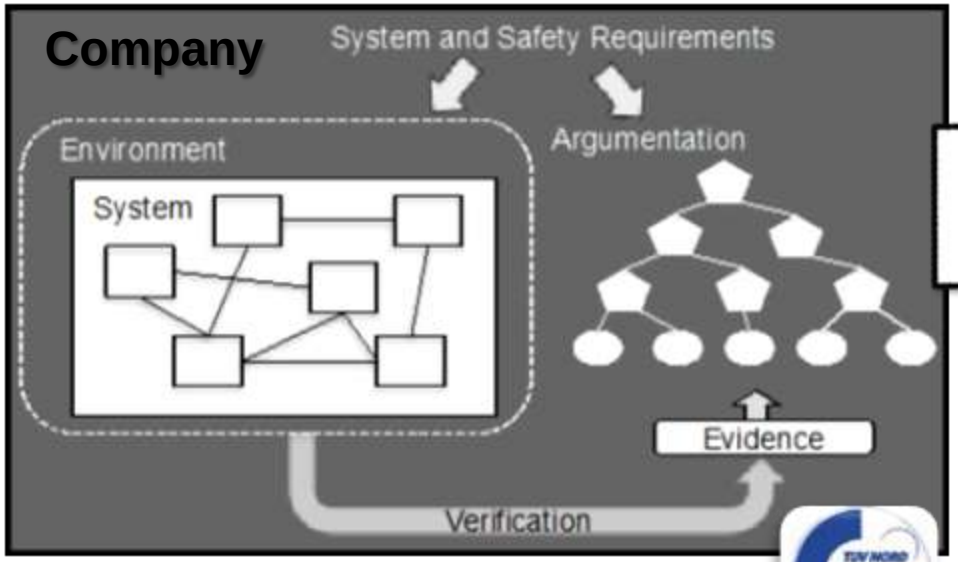
virtual vehicle
Vehicle EE & Software

Safety Standard

SafeCer

Independent safety assessor

Company



Safety Argumentation provides Guidance through Documents

TECHNOLOGY

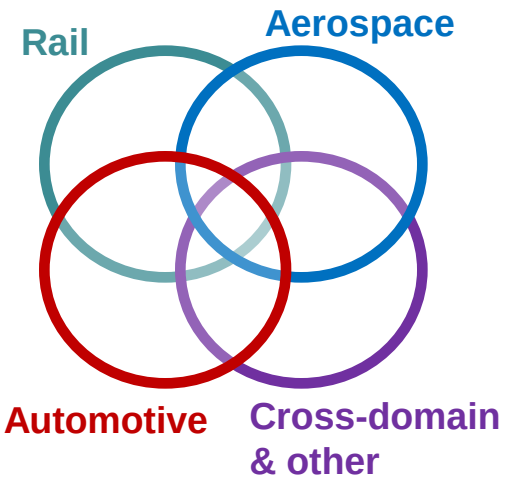
- **Co-certification** = Development + Verification + Argumentation
- **Process** integrating development and argumentation
- **Component model** extended with safety contracts
- **Argumentation** – Composable safety argumentation and gathering of evidence
- **Verification and validation** integrating testing and formal verification

TOOLS

- **Certification Artefacts Repository (CAR)**
  - A certification-oriented configuration management system
  - Store certification evidence and end-to-end traceability
- **Certification Tool Framework (CTF)**
  - Assumption: tight tools integration is not economically feasible
  - Lightweight tool integration metadata exchange
- **The CAR and CTF are configured with a process model**

Demonstration & Evaluation

- **Instantiation of tools and technology**
- **Rail demonstrators**
  - Automatic braking system
  - Safety-system for railway crossings
  - On-board train control and monitoring
- **Aerospace demonstrators**
  - On board control system
  - Air-traffic control system
- **Automotive & Construction Equipment demonstrators**
  - Hybrid powertrain controller
  - Autosar basic software modules
  - Construction equipment product-line
- **Cross-domain & other domains demonstrators**
  - Ethernet switch used in 3 different domains
  - On-line diagnosis component
  - Healthcare demonstrator



Thank you for your attention!

www.safecer.eu

safecer-coordinator@safecer.eu