GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Collaborative Embedded Systems

CrESt

CrESt Projektabschluss

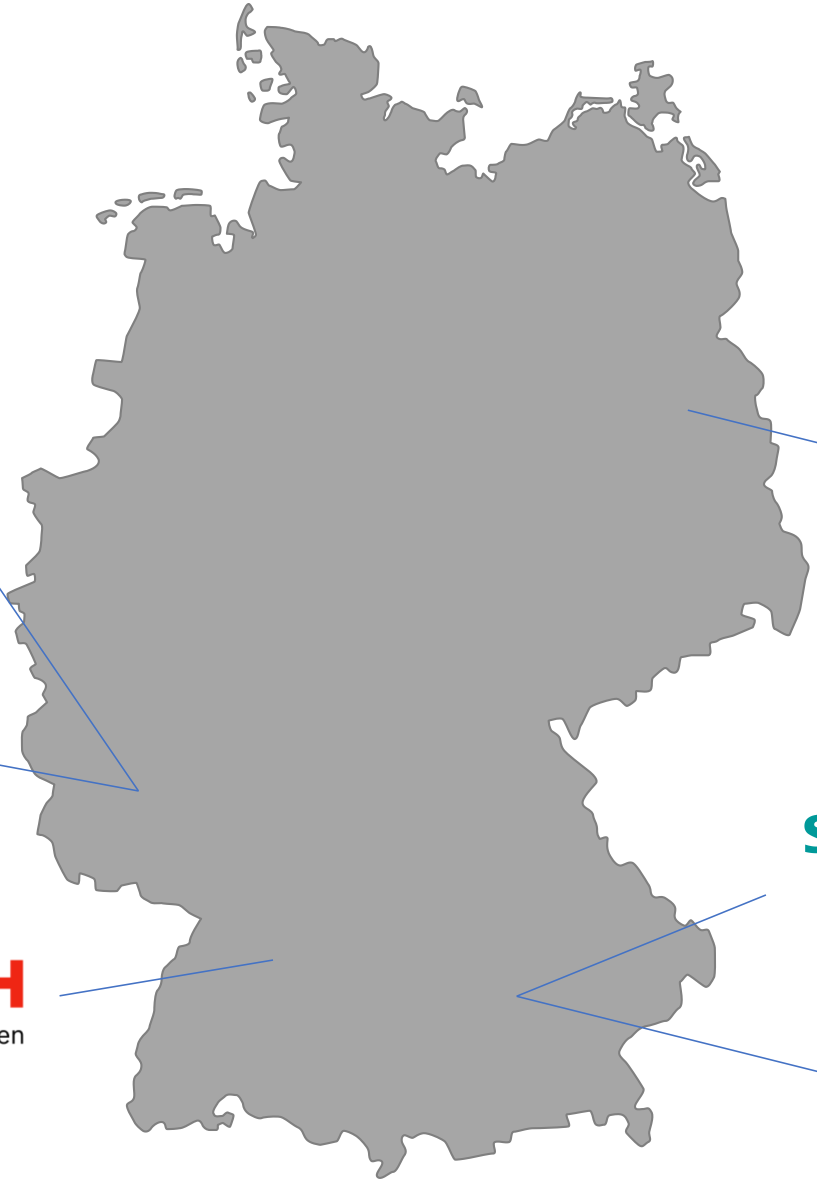
Dynamic Safety Certification for Collaborative Embedded Systems at Runtime

Felix Möhrle

TU Kaiserslautern, 16.10.2020

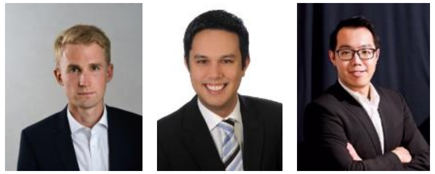
Collaborative Embedded Systems CrESt

Partners



TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Fraunhofer IESE



BOSCH Technik fürs Leben

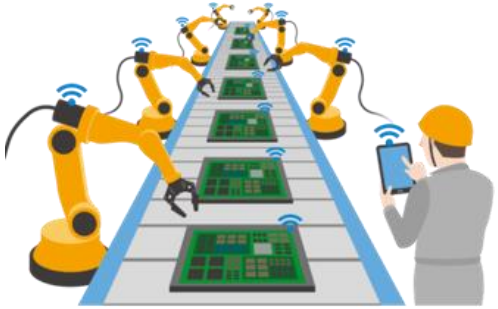
expleo

SIEMENS Ingenuity for life

Siemens DAM

TUM

Overview

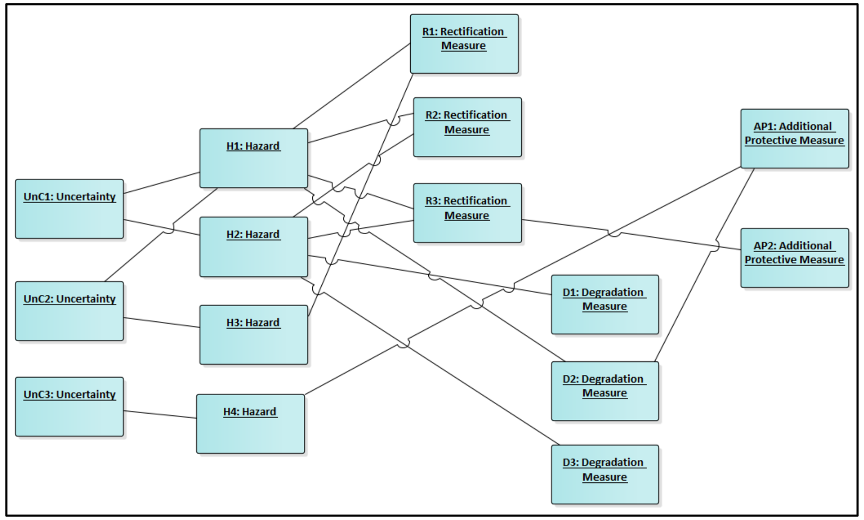


Focus of our work:

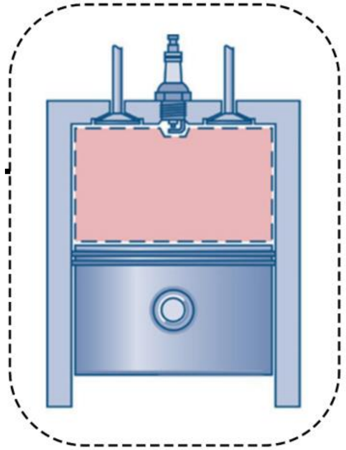
- Dynamic safety certification of collaborative embedded systems (CESs)

Contents:

- Dynamic safety certification
- Safety certification concept
    - Document-based
    - Contract-based
- Safety-related supporting techniques
    - Context modeling
    - Runtime uncertainty handling
    - Integrating model-based risk assessment



Motivation



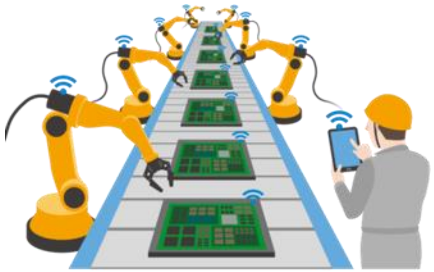
System
boundary

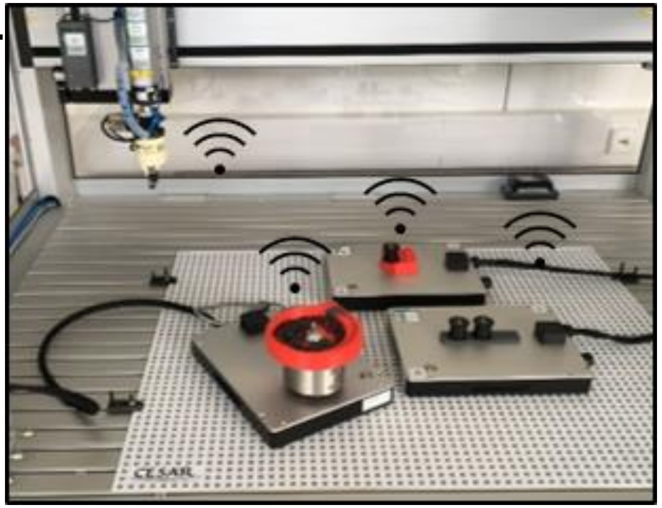
Traditional systems

- are fully specified during design time
- work in a closed context with little uncertainty
- can be assessed with established and standardized procedures

Collaborative embedded Systems (CESs)

- Dynamic collaborations at runtime
    - Collaborative System Groups (CSGs)
- Usually flexible deployment
- High uncertainty regarding context
- New techniques for safety assessment required

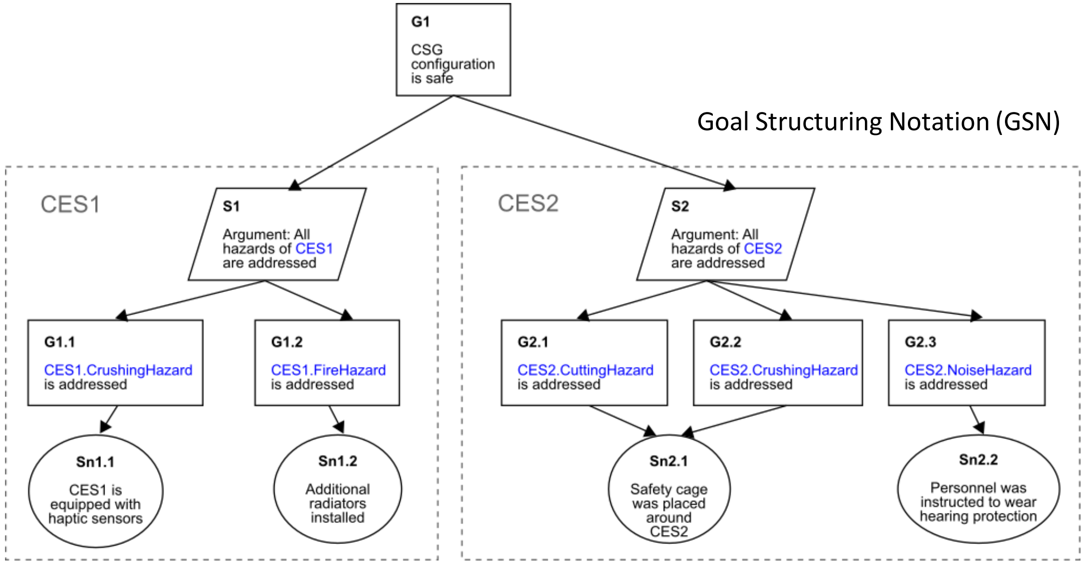


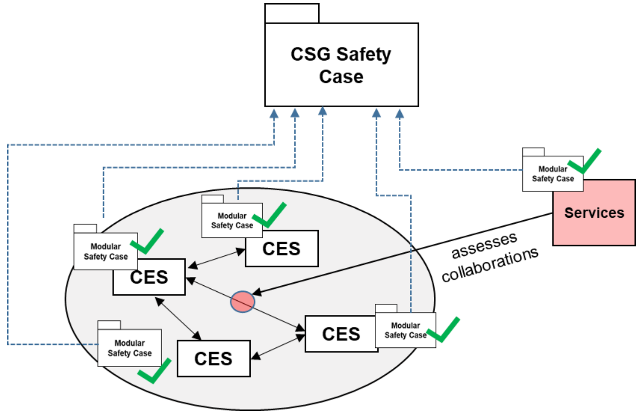


The goal of our work was the development of new safety certification concepts suitable for CESs.

Dynamic safety certification

- Our proposed process for dynamic safety certification is aimed at
  - Accelerating the operational safety approval (i.e. certification) after CSG reconfigurations
- Semi-automated approach
  - With human involvement (**human-in-the-loop**)
  - Goal: Support the safety engineer
  - Document-based
  - Industrial use case: Adaptable factory
- Fully automated approach
  - Without human involvement (**peer-to-peer**)
  - Contract-based
  - Industrial use case: Platooning
- Fundamental concept: modular safety cases





Document-based certification

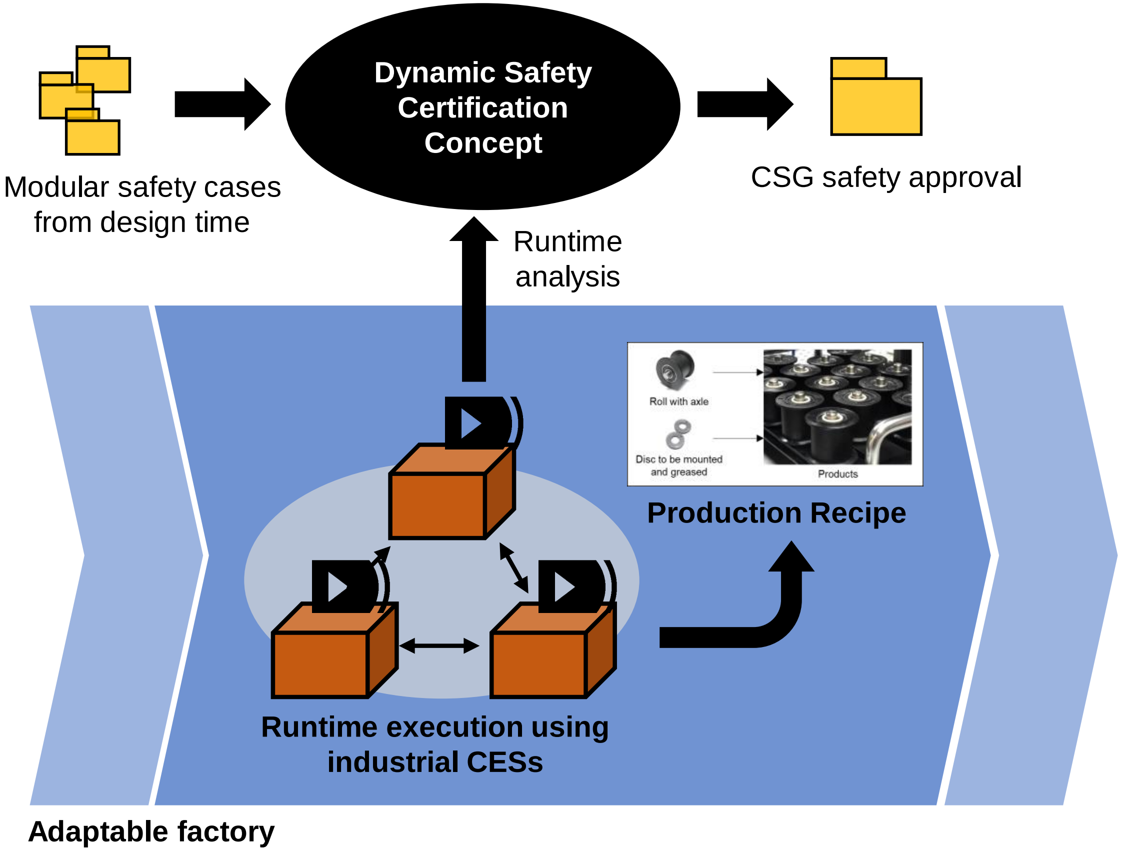
Goal:

- Partially automate the (manual) certification process to support the safety engineer
- Enable software support

Adaptable factory:

- Factory consists of mechatronic objects (MOs)
- MOs are arranged as needed for individual products (plug & produce)
- Health and safety engineer is responsible for the safety certification (legal requirement)

For more information, we refer to our video presentation in the CrESt marketplace (SQ2: Runtime Safety Certification for Adaptable Factories)



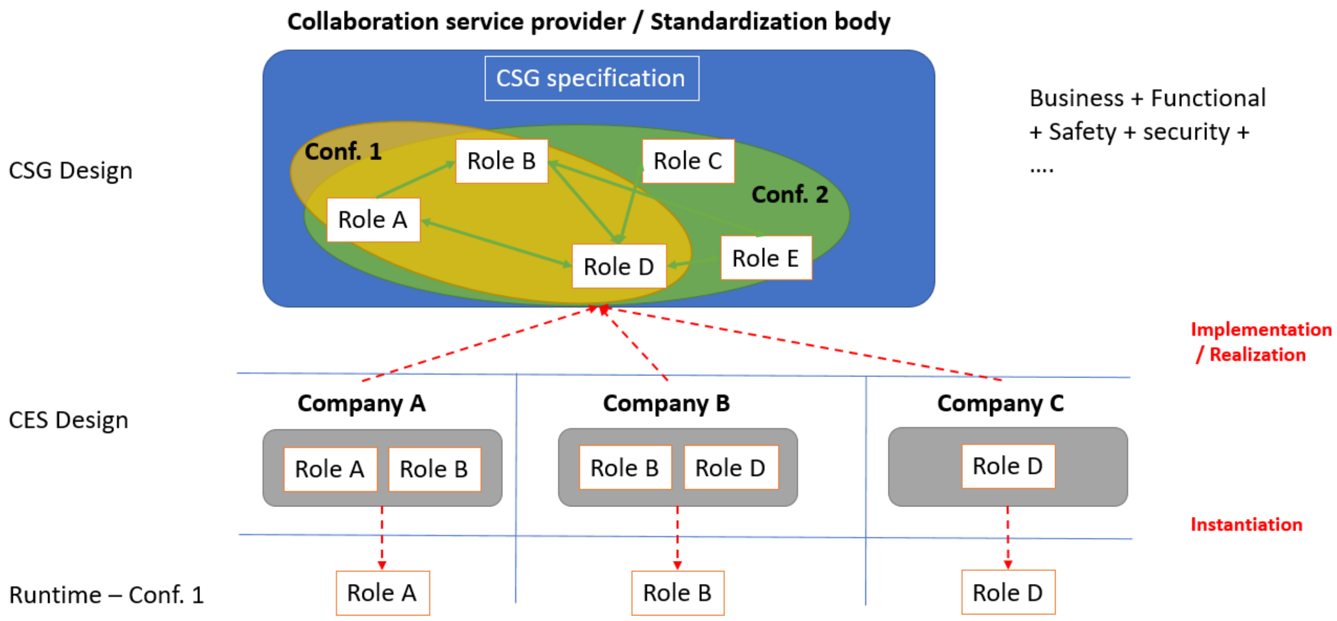
Contract-based certification

Goals:

- Enable **peer-to-peer** safety certification without the necessity of human involvement

Concept:

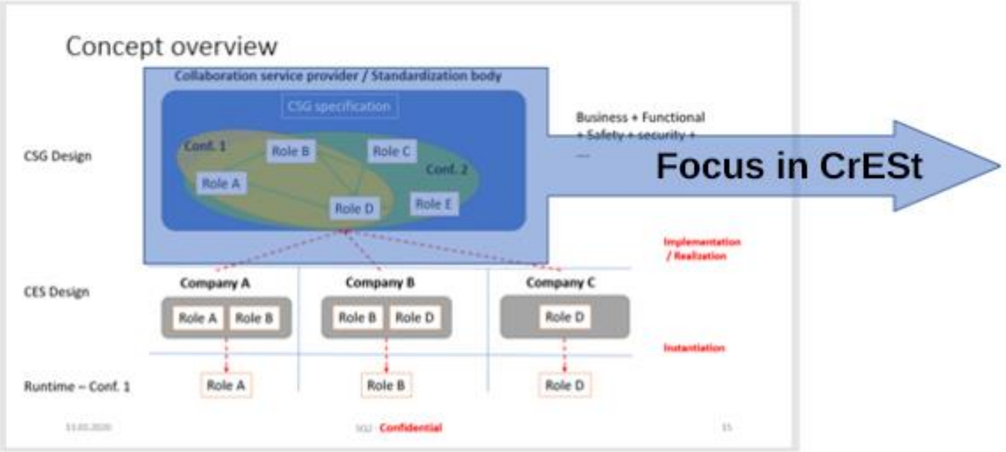
- CESs are equipped with modular safety cases at design time
- At runtime, CESs negotiate contracts for provided and required services
- The result is a safety case for the integrated CSG

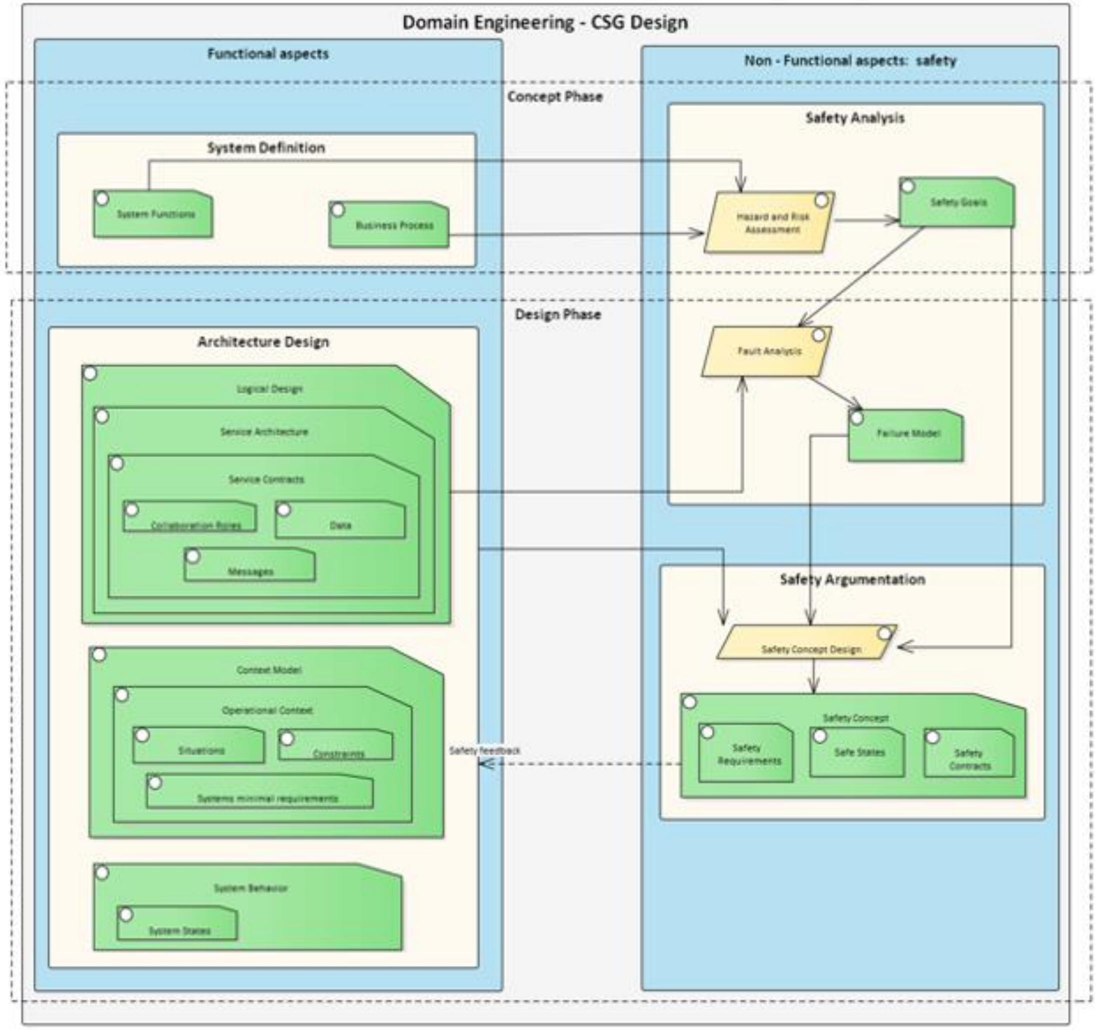


Contract-based certification

CSG specification:

- Architecture aspects
  - Roles, communication means, functions, services, behavior, structure, functional contracts,…
- Safety aspects
  - Hazards, failure models, safety requirements, degradation modes, warning and safety concept, safety contracts, ….

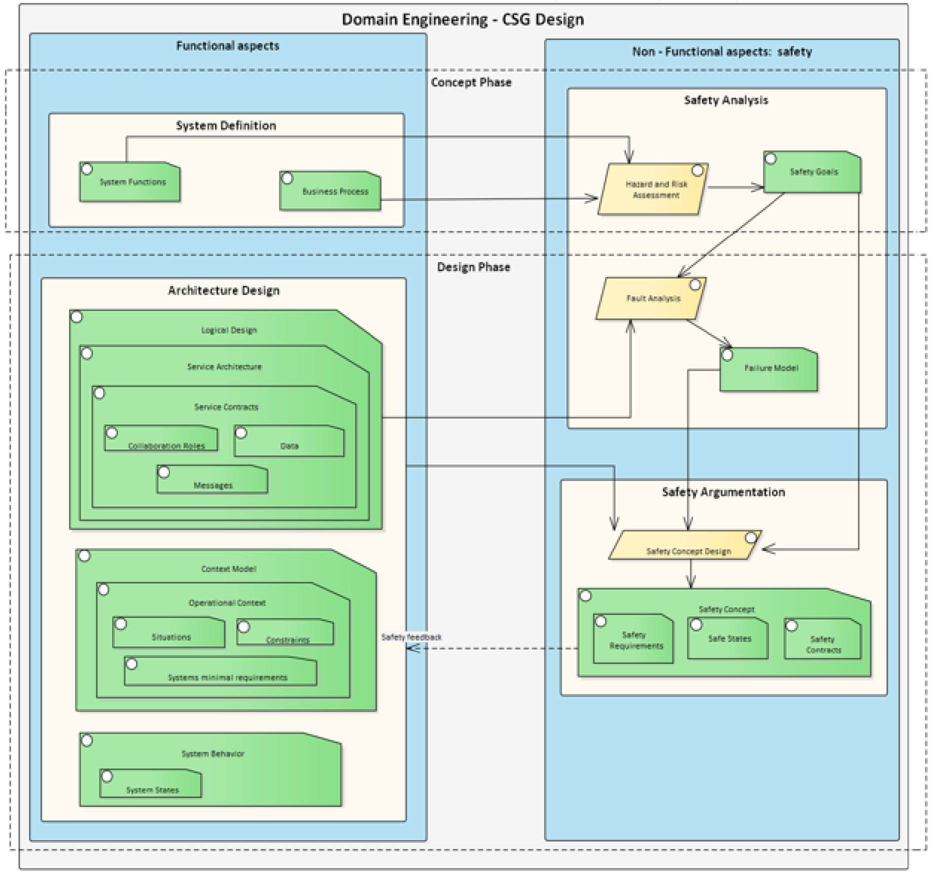




Contract-based certification

Main results:

- Integration of the **Service Oriented Architecture** (SOA) with the **SPES XT** modeling concepts for the specification of functionality through services.
  - Adaptation and implementation of SOA ML (Modeling Language) within the **safeTbox modeling tool**.
- Integration of Component Fault Trees (CFT) with SOA, for the creation of fault models.
  - Development of a **realization view concept for CTFs**. This serves to deal with the modeling complexity when analyzing systems with a large number of hazards.
  - Conception of an information **visualization approach for CFTs**.
- **Domain engineering** concept for the definition of **safety contracts** for degrading systems.



Contract-based certification

Item def.

Use cases

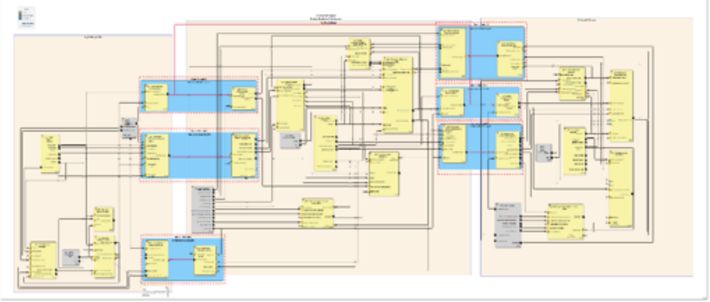
Design concept

Service architecture

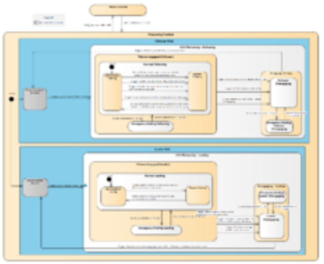
Comm. and Messages

Function decomposition

Functional network {functions, services, ConSerts}

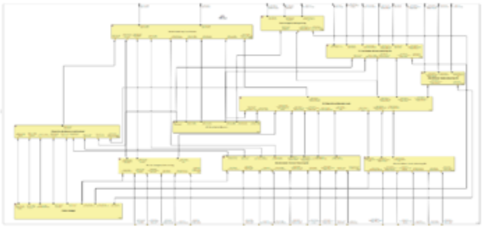


State machine



HARA

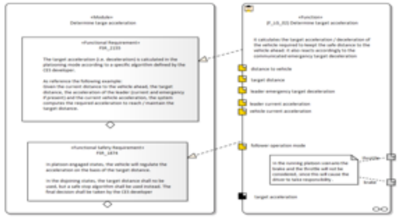
FTA



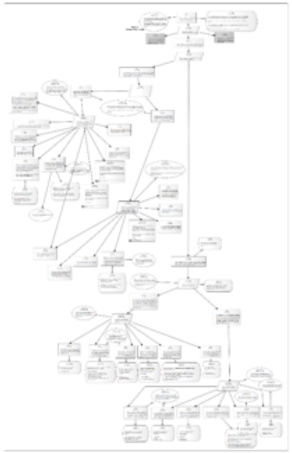
Contracts

Contracts Visual representation

Function – Requirements map.



Safety concept

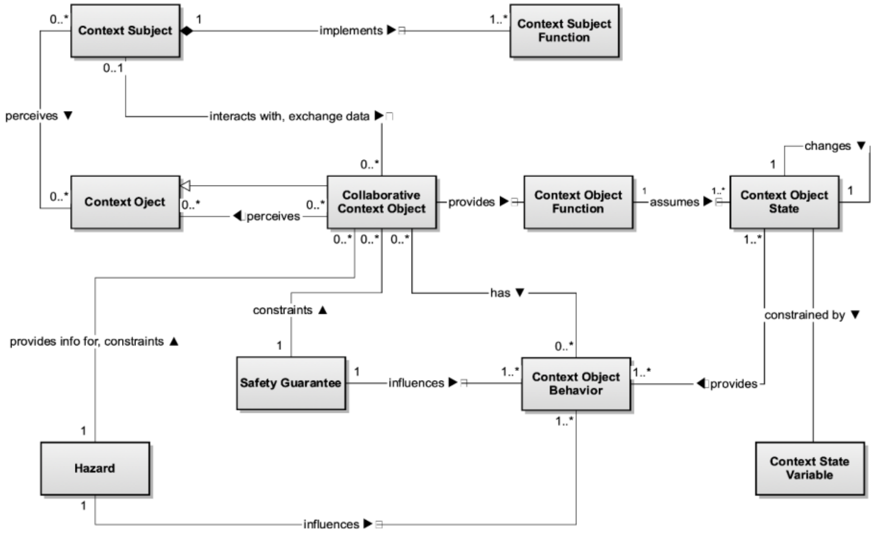


Context modeling

- Every system (CES) operates in its individual *context:*
  - the perceivable surrounding that consists of all the objects from the environment relevant for that system

- CESs form CSGs with other systems from their context
  - The context cannot be fully anticipated during design time.
  - The need for context awareness emerges.

- Context awareness is generally accomplished through the creation of context models
  - In practice, there are differences in the context modeling concepts among different manufacturers and suppliers → "semantic heterogeneity"
  - The use of ontologies unfolds the potential to serve as a conceptual and technological representation of such models



Context ontology

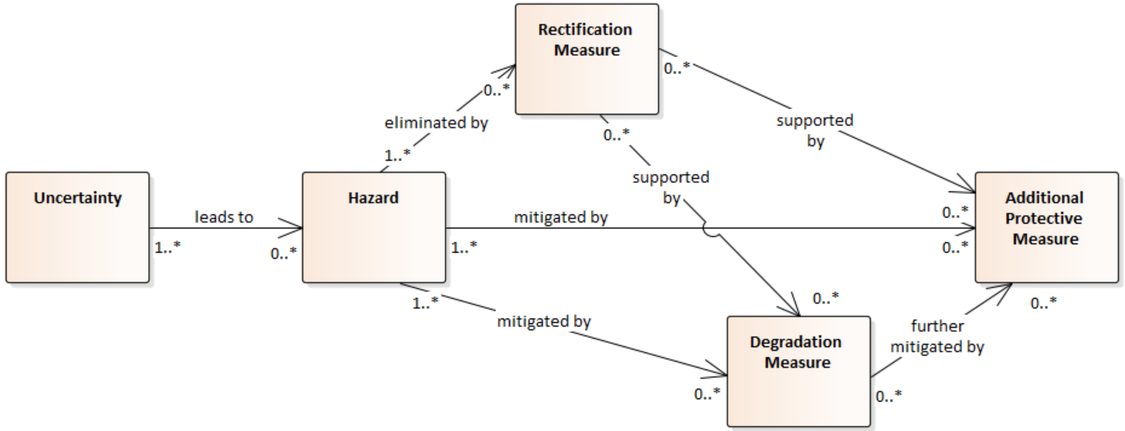
Our context ontology integrates elements of two types of context:

(1) classes and relationships of the interacting CESs, known as the **operational context**, and
(2) sources of information with respect to the CESs, seen as the **context of knowledge**.

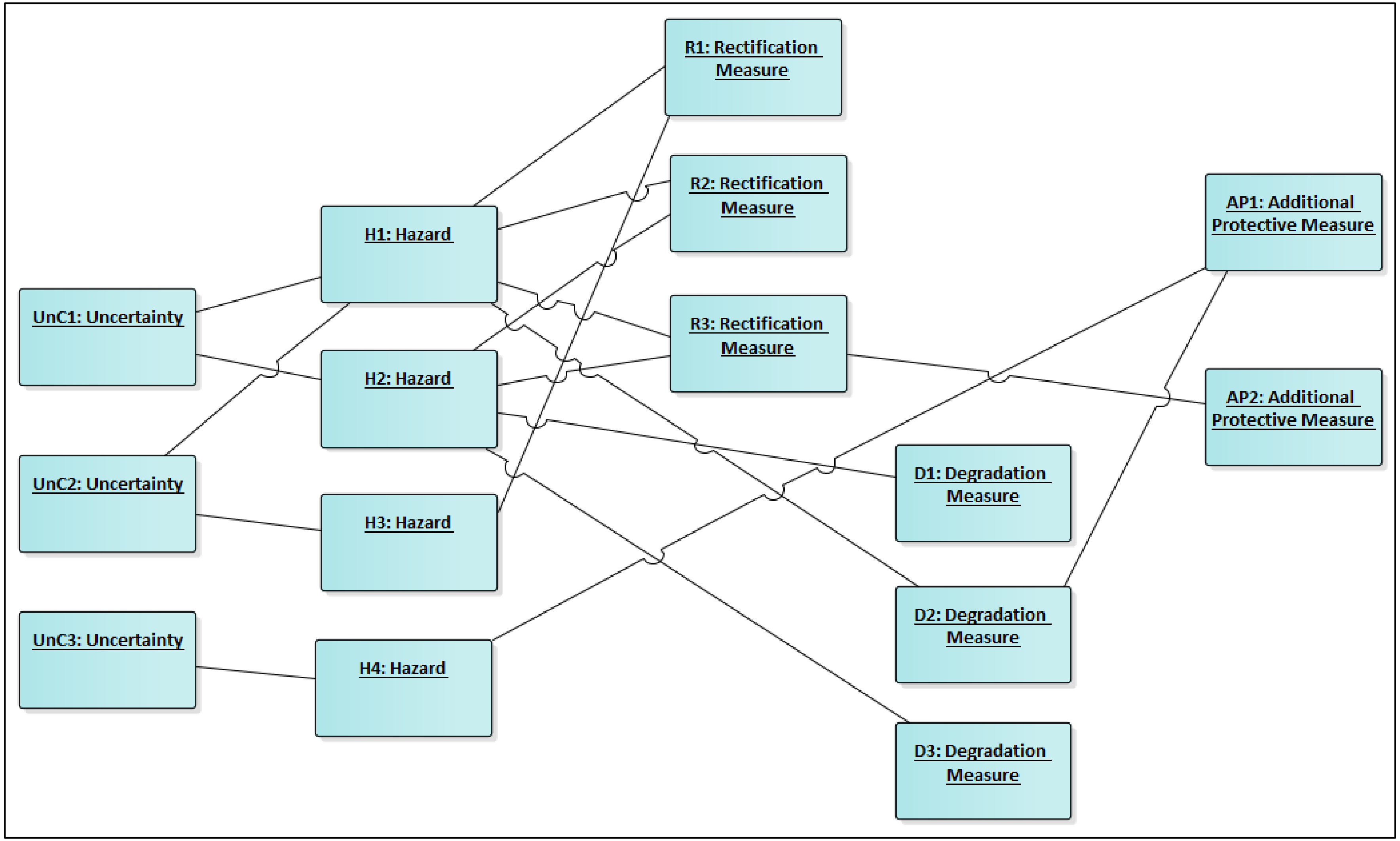
Runtime uncertainty handling

- **Uncertainty**: Required information is only partially available or inconsistent from different sources.
- Runtime uncertainties are of high relevance for safety.

- **U-Map**: Reference map for safe handling of runtime uncertainties
  - Acts as a knowledge base (considering MAPE-K feedback loops)
  - Maps potential uncertainties → possible hazards → mitigation measures
  - Mitigation measures
    - Rectification measure
      - Attempt to eliminate uncertainty during integration
      - Complete elimination might not be possible
    - Degradation measure
      - Change in the functionality or configuration of the system
      - Runtime reconfiguration / adaptation
    - Additional protective measure
      - Reduce severity of possible accidents in safety critical states
      - Can be external measures



Runtime uncertainty handling



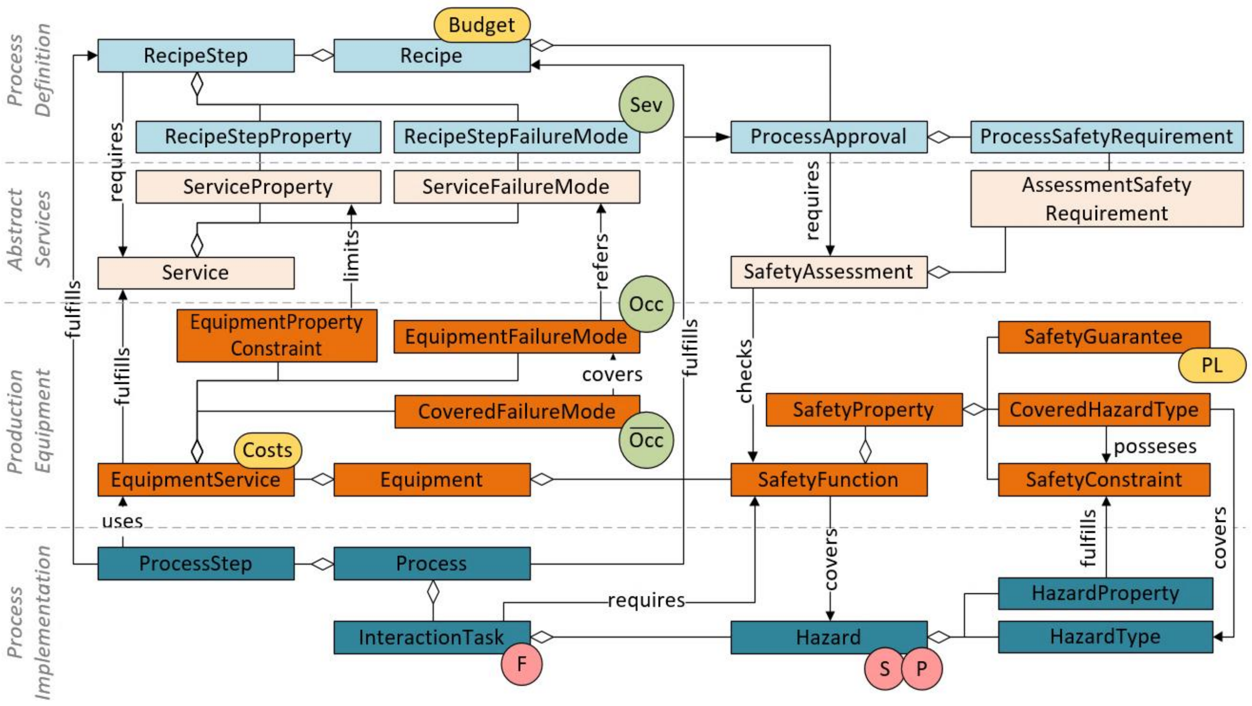
Runtime uncertainty handling

No	Uncertainty	Detection	Hazards	Rectification	Degradation modes	Additional protective measures
U_nC_1_e	Mechatronic object service descriptions incomplete	Manually during safety analysis	Unforeseen movements (machine)	● Check individually all service descriptions and add them accordingly	● Reduced Motion ● Immediate STOP funtion	
U_nC_2_a	Hazard zone information is missing in the self-descriptive characteristics of an MO	incomplete information communicated to the orchestration unit	Ineffective safety analysis	● Individually analyze the missing specifications ● Training to the HSE w.r.t the new context and funcionality of the system ● Visual inspection of available inherent safe design measures	-	-
U_nC_6_b	Current surges lead to intermittent magnetic flux in the electric motors of nearby MOs	Visual identification through appropriate labeling of corresponding components	Unforeseen movements (machine)			
			Sensor failures (machine)			
U_nC_6_c	Welding machine present in close vicinity of a light sensor guided MO	Visual identification of high voltage machines by appropriate labeling	Sensor failures (machine)			
			Unforeseen movements (machine)			
U_nC_7_a	Unintended entering of human workforce into the hazard zone	Detected by sensitive protective equipments (SPEs)	Electrocution (human)		● Power shut down ● Reduced speed and motion of movable components when human presence detected by SPEs	● Installation of protective guards ● Installation of light barriers with addition SPEs where human presence cannot be avoided ● Info material regarding Hazard zones ● Marking “go” / “no go” areas
			Burn (human)			
			Trapping (human)			
			Stabbing or puncture (human)			
			Crushing or impact (machine, human, product)			
			Being thrown (product, human)			

Integrated model-based risk assessment

Metamodel-based, automatic generation of process FMEA ensures production quality

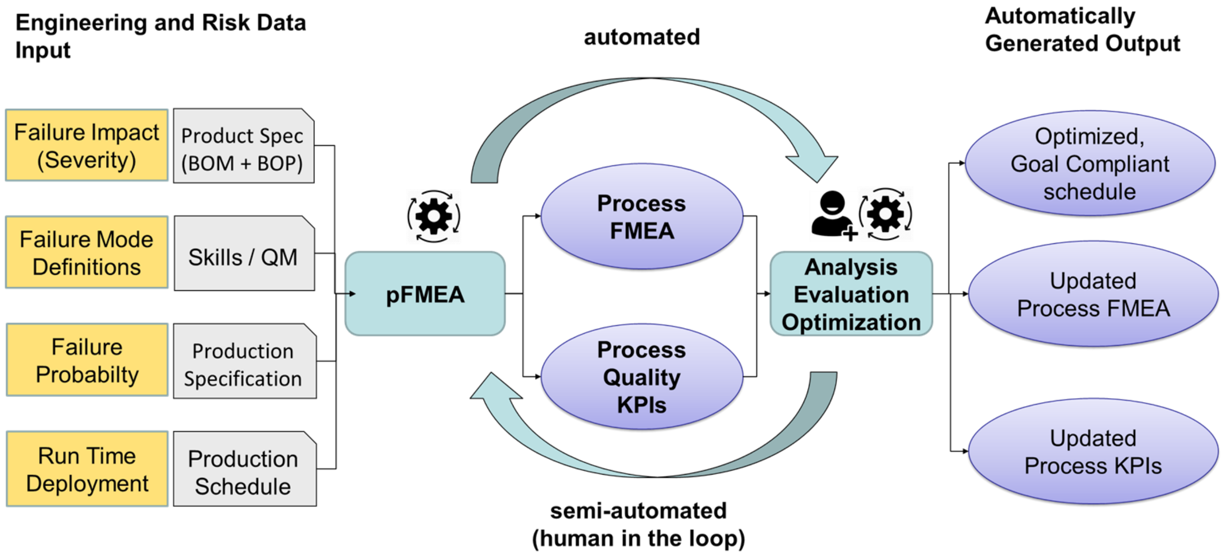
- All Information for automated risk assessment captured in one place, machine-processable
- Model-based and modular approach supports development processes
- Decouple independent stakeholders
- Reuse existing solutions and knowledge from risk analysis for production services, product definition (BOM/BOP)
- Automated (re-) generation of artifacts



- Method supported by tooling: prototypical tooling based on MPS developed within CrESt supports semi-automatic analysis, evaluation and optimization

Integrated model-based risk assessment

Metamodel-based, automatic generation of process FMEA ensures production quality



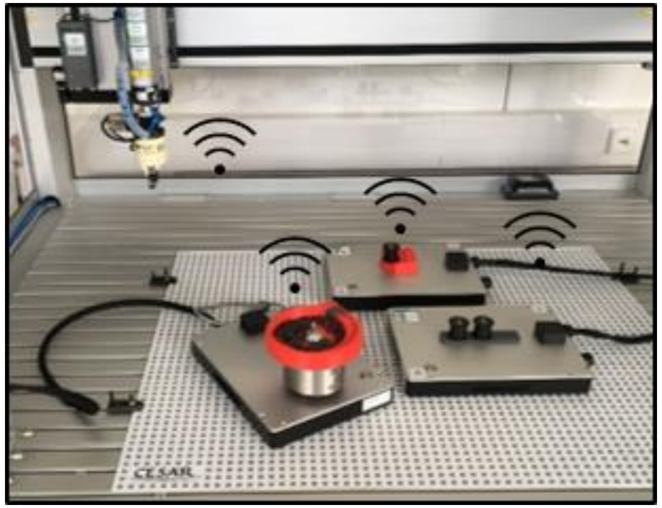
- All Information for automated risk assessment captured in one place, machine-processable
- Model-based and modular approach supports development processes
- Decouple independent stakeholders
- Reuse existing solutions and knowledge from risk analysis for production services, product definition (BOM/BOP)
- Automated (re-) generation of artifacts
- Method supported by tooling: prototypical tooling based on MPS developed within CrESt supports semi-automatic analysis, evaluation and optimization

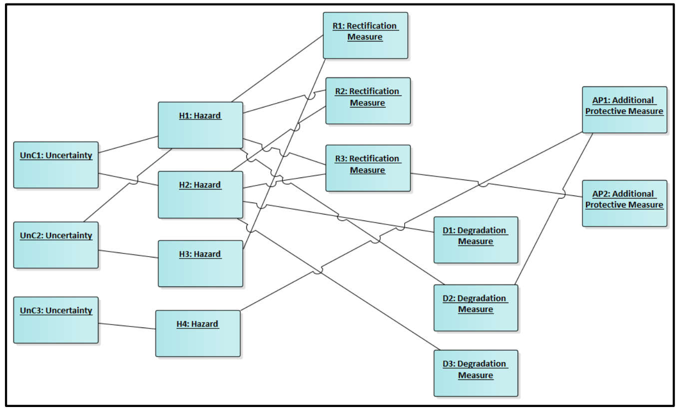
Conclusion

- **Focus:** Dynamic safety certification of collaborative embedded systems (CESs)

- **Modular safety cases** are combined to build a safety case for the integrated CSG
    - Document-based (adaptable factory)
    - Contract-based (platooning)

- **Supporting techniques:**
    - Context modeling (context awareness)
    - Runtime uncertainty handling
    - Integrating model-based risk assessment





DLR Projektträger

Collaborative Embedded Systems

CrESt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Fraunhofer IESE

BOSCH Technik fürs Leben

Vielen Dank!

(expleo)

SIEMENS Ingenuity for life

Siemens DAM

TUM