Collaborative Embedded Systems CrESt
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung
fortiss

Checkable Safety Cases

A Safety Case Maintenance Approach

Automated safety case maintenance supports the assessment of the impact of frequent re-configurations of collaborative embedded systems/collaborative system groups on system safety

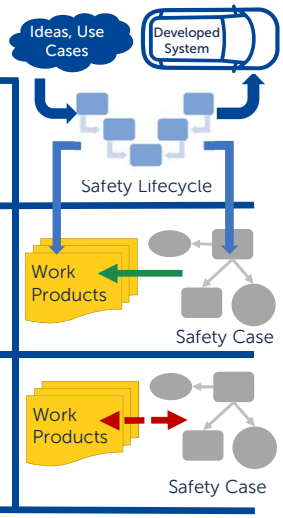
Safety Assurance in Automotive

The execution of the ISO 26262 safety lifecycle outputs a set of safety work products (e.g., hazards list, requirements lists, architecture)

Safety cases are safety work products that provide an argument that safety requirements are satisfied, based on evidence compiled from other safety work products

Safety cases shall be maintained consistent w.r.t safety work products. Given a modification of the item …

- ❑ The impact is evaluated
- ❑ The safety case is updated



State of the practice

Safety case maintenance is a manually executed, and thus expensive process

State of the art

GAP: Approaches are too conservative (potentially impacted safety case elements are identified)

GAP: No guidelines for how to update the safety case considering the modifications

Impacted safety case: **inconsistent** w.r.t. other safety work products

Up-to-date safety case: **consistent** w.r.t. safety work products, correct, complete

Open question: What does CONSISTENCY w.r.t. safety work products really mean?

Checkable Safety Cases

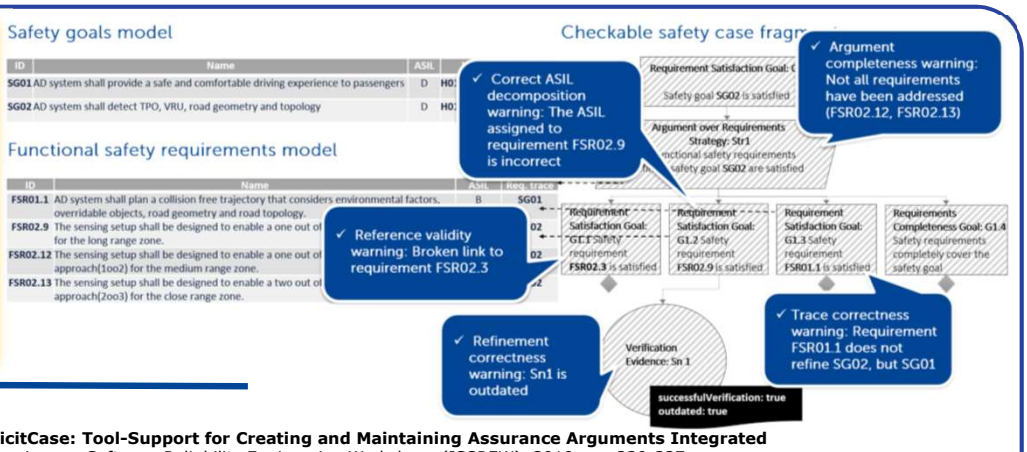
✓ Typed Safety Case Constructs

Re-occurring safety claims, having certain known semantics

Aware of changes in engineering models due to model integration

Annotated with consistency criteria

✓ Consistency Checks



Publications

- ❑ C. Cârlan, V. Nigam, S. Voss and A. Tsalidis, **ExplicitCase: Tool-Support for Creating and Maintaining Assurance Arguments Integrated with System Models** In IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2019, pp. 330-337
- ❑ C. Cârlan, D. Ratiu **FASTEN.Safe: A Model-Driven Engineering Tool to Experiment with Checkable Assurance Cases** In: Computer Safety, Reliability, and Security. SAFECOMP 2020. Lecture Notes in Computer Science, vol 12234. Springer, Cham

Applicability of Checkable Safety Case Models for CSGs – Platooning

- ❑ Modelling the safety case for a platoon
- ❑ Updating the safety given: **Addition of new hazard**, **Deletion of safety goal**, **Modification of requirements**

fortissimo rover

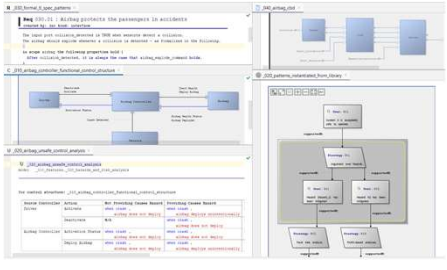
Tool Support – FASTEN.Safe

an open-source environment for the specification, verification and assurance of critical systems

requirements modeling and specification

specification of **architecture** and **design**

safety analysis & **checkable safety cases**



Contact: Carmen Cârlan, carlan@fortiss.org