EXCROSS

Certification

Certification

Safety certification of embedded systems components among three transportation modes (road, aviation, railway), to improve safety while reducing costs and effort. The topic focuses on the steps and tools used in the certification process that can be transferred in another mode, and on the certification of cross-domain components.

Introduction

Safety certification of embedded systems in the transportation domains represents a relevant aspect to cope with. In addition to being a multi-faced and complex problem by itself, the multi- and cross-domain framework, within which the stakeholders will have to move ever more in the future, introduces further constraints and issues such as the large variety of definitions / interpretations, technology / architectures and regulation / culture levels.

Different transport sectors (e.g. railway, automotive, aviation) have developed their own specific set of standards in the past years, originating a sort of “Babel Tower” effect. A multi-domain approach to support a simpler and quicker certification of components and systems could help improving safety while contemporaneously reducing costs and effort.

Two aspects of the certification research are addressed by the analysed projects:

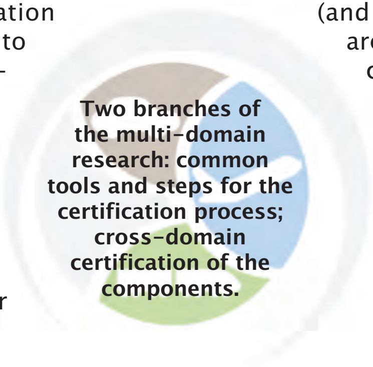
1. Steps and tools used in the certification process, that can be transferred or re-used in another mode; by analysing the process for different domains and by contextualising the analysis itself with reference to the development of a particular product, it is possible to highlight building blocks of the certification workflows for different transportation modes.

2. Certification of cross-domain components: some components can be designed so that they (or part of them) can be already certified and used in more than one transport mode. It typically means that the hardware and software components are highly modular and simplified (though more numerous), so to ease re-use in another mode without need for customisation and with a consequent reduction of costs and time.

Findings

The two aspects highlighted are interdependent and mutually affect each other. Ideally, by reassembling the information and the results, gathered by projects active in different domains and focusing on the two aspects above, it could be possible to depict possible trans-domains benefits concerning:

- The analysis of certification steps (and possible tools for the certification workflow investigation) in order to depict possible common milestones for procedures in different transportation domains;
- The analysis of the production process of embedded systems, in particular with reference to the modular decomposition of hardware and software modules which can be exploited in other transportation modes.



Two branches of the multi-domain research: common tools and steps for the certification process; cross-domain certification of the components.

The certification process of embedded systems could be then fully analysed in its integrity in a trans-domain perspective, allowing to gain cost reduction and to foster re-usability. The harmonisation of business processes in inter-modal transport is the basis to pave the road for the standardisation of inter-modal / cross-modal certification processes. Also, the standardisation of hardware boards / embedded ICT systems (and possibly Operating Systems) is an area in which cross-mode certification could be reached with relatively small effort, and the development of common interfaces for inter-modal communication will support progresses in this area.

Even if the research on certification is already moving into a multi-modal direction, the regulatory framework is still a step back. First of all, the participation into standardisation processes shall be enlarged by facilitating access to standardisation bodies and initiatives. There is also the need to start to define common approaches to technology certification process at EU level and, at the same time, it is important to consider the certification of components for cross-border (EU vs. non-EU) safety. Finally, International or EU inter-modal certification bodies are missing.

A relevant gap emerged from the analysis is the absence of the maritime domain within the cross-modal projects consortia, together with the difficulties in finding certification research projects in the maritime domain. The analysis of the maritime domain certification processes and components should be performed in order to compare the state-of-the-art of this domain with the status of the research in the other domains.

Need for International or EU inter-modal certification bodies and a common approach to technology certification process at EU level.

Success stories

OPENCOSS

Open Platform for EvolutioNary Certification of Safety-critical Systems

Funding scheme: EU FP7
Website: **www.opencoss-project.eu**

OPENCOSS project aims to devise a common certification framework, spanning different transport sectors (automotive, aviation, railway, while maritime is not included), to facilitate the re-use of assurance assets across and between domains, and to establish an open-source platform or safety certification infrastructure.

SAFECER

Safety Certification of Software-Intensive Systems with Reusable Components

Funding scheme: EU ARTEMIS JU
Website: **www.safecer.eu**

SafeCer is targeting increased efficiency and reduced time-to-market by composable safety certification of safety-relevant embedded systems, such as electronics and software systems (i.e. software-intensive systems). SafeCer proposes a workflow approach to certification standards to identify common procedures to different domains, in order to find clusters of procedures in common between domains for the certification of embedded hardware and software.

Hints for

future research

Development of a **multi-domain knowledge base**, useful for stimulating the research on the productive and certification processes, and creation of **political and legislative initiatives** to foster and ease multi-domain standardisation.

Certification of the management of **data ownership** and Intellectual Property Rights in all safety-related matters.

Confidence in safety **certification vs. liability** in case of accidents.

Certification of protection against **cyber-attacks**, in analogy with the Safety Integrity Level described in CENELEC norms (e.g. EN50129).

Certification of **multi-domain components** to allow working in different harsh environments (e.g. icing conditions).

SEVENTH FRAMEWORK PROGRAMME

EXCROSS

Certification

contact persons:
Simone Pozzi, Sara Silvagni
Deep Blue

website:
www.excross.eu
info@excross.eu