RCA Beta – Chapter on Modular Safety

Table of contents

V1.0	26.8.2019	B. Rytz	Version for publication after review by the RCA core group

1. Introduction

1.1. Purpose of the document

The publication of RCA Alpha has generated interest among railways and suppliers. Direct feedback and feedback from several workshops have provided insight, where clarifications or additional content would be helpful.

In the document RCA Architecture Overview, there are several mentions of the concept "**modular safety**". This document provides additional information on this topic, which is a key property for a modular architecture with the goal of being able to use components from different suppliers or to upgrade components independently of other components.

This is the very first publication on this topic from RCA and its main purpose is to establish the topic and get discussions with stakeholders in the sector going.

1.2. Definition and characteristics of Modular Safety (MS)

Modular safety is the concept to reduce the overall safety case workload by using modularity, not only for the technical design of components, but also to use modularity to foster independent, re-usable, composable safety cases. Overall it means to reduce the workload of the impact analysis for changes and end2end corrections to a possible minimum.

Today, in current projects, specific safety assessments are a major cost-driver and a big obstacle for a roll-outs and upgrades. Reducing the safety workload is an important contribution to the cost-effectiveness of CCS solutions and is crucial to enable more frequent upgrades.
Note: In previous documents the term "open safety" has been used for "modular safety". In RCA we now exclusively use the term "modular safety".

1.3. Examples

One example is ETCS itself. A vehicle shall get one authorisation in Europe and shall drive through all countries without additional safety cases. This target and the work derived from the 4th railway package show, how 2 independent safe applications (ERTMS onboard, ERTMS trackside) shall interact as a whole system without individual integration safety cases[1].

1.4. Additional material

The following articles provide introductory perspectives on “modular safety”:

- [1] Safety case architectures to complement a contract-based approach to designing safe systems. https://pdfs.semanticscholar.org/b195/787d93d3c534cf70adb01d36f8034735fe26.pdf
- [2] Safety-Related Application Conditions – A Balance between Safety Relevance and Handicaps for Applications. http://www.bitschnet.de/Safecomp2009_BtFeGo.pdf
- [3] Managing Complex Safety Cases. https://www-users.cs.york.ac.uk/tpk/sss03.pdf

The following documents from the context of smartrail 4.0 provide a perspective from the point of view of platform independence. Since they were written before or during the RCA work, it is not yet complexly aligned with RCA terminology:

1. [10] Safety-critical Applications in Data Center in the Railway System SBB http://smartrail40.ch/service/download.asp?mem=0&path=\download\downloads\Safety-critical%20Applications%20in%20Data%20Center%20in%20the%20Railway%20System%20SBB.pdf

Currently an in-depth study about modular safety is running in smartrail4.0, results are expected for the end of 2019.
There is a link to using formal methods since they can contribute to reduce the safety case workload by making dependencies explicit and by reducing the impact of changes in the case of upgrades.

2. Goals of Modular Safety

Modular safety is a key goal for RCA. RCA needs modular safety to enable modularity and exchangeability for components, which are needed to enable upgradability of the CCS system. At the same time RCA enables modular safety, by providing an architecture with well-defined interfaces and dependencies.

Modular safety has the goal of **reducing the safety case workload**. The vision is to come near to a “plug&rail”[2] for safe components, that are developed separately.

In the desired target state of RCA, we have:

1. reasonably small components (low entry barriers for market participants, broad market), that;
2. meet a special interface standard designed in accordance with "modular safety" principles, with;
3. isolated type approvals and isolated proof of compliance Interface requirements (incl. SAC[3]), that are;
4. integrated directly into an existing overall safe application and can be used immediately, without the need for e.g. a new overall inspection of the overall application or proof of the safe integrity of the entire application must be performed.

[1] This process still needs not completely modular, as the reality is that to integrate with Class B systems and National Operational Rules we have still currently to produce a System Integration Safety case.
[2] Plug-and-rail is used here as a “vision” in analogy to the well-known term plug-and-play, see https://en.wikipedia.org/wiki/Plug_and_play.
[3] SAC = safety application conditions, sometimes also used as SRAC = safety-relevant application conditions

This is achieved by a set of measures, including:

- Reducing “SIL4” systems to the minimal functionality (concentrated in the architecture);
- Interfaces with “modular safety” qualities (allows isolated safety case per component), this includes very precise interface definition, including exported requirements, testability, only explicit dependencies;
- Incremental safety case (automated impact analysis);
- Platform independence (including modular safety) using independent computing and communications platforms on the vehicle and trackside;
- Remote and automatable update of safe applications.

3. Applying modular safety in RCA

3.1. Based on safety cases according CENELEC EN 20126

An RCA-based system will apply the categories of a safety case according to EN 50126-2:

- Generic product (GPSC)
- Generic application (GASC)
- Specific application (SASC)

This provides a framework for modularization of the safety cases. According to the norm: “When using a generic product […] or a generic application […] in the context of a specific application, it should be possible for safety acceptance to be based on existing related independent safety assessment.”

When applying these definitions, each of the ‘granular’ RCA modules or components gets its own GPSC (we want it COTS). Applying these products in an environment of an IM will lead to a GASC (when integrating including interfaces, also in the given example of on board and field equipment of ETCS) and applying a product following GA-rules will lead to a SASC for a specific application at a certain location.

3.2. Concentrating SIL4 functions in selected components

As described in “RCA Architecture Overview” a fundamental design principle for RCA components is to separate differing SIL requirements in different components. This requires careful design work but reduces the safety case workload.

3.3. Component Interface quality for modular safety

The interface quality is the foundation for modularity itself and for modular safety. Interface quality includes quality in the sense of well-chosen modularity, as well as in the sense of quality of the interface specification (description).

Important elements for interface quality are:

- Precise specifications with a top-down derivation of requirements to design (MBSE = model-based systems engineering).
- Simple interfaces (modular definitions), reduced complexity (small number of states and stateless transactions).
- Capability-based protocols between components (modular protocols).
- Simple safety related application conditions (SRAC), being an explicit part of the interface specification.
- High degree of testability (testbench and reference systems, test vector, test coverage, white box testing, etc.).
- Object Oriented Design rules (encapsulation, inheritance, etc.).
- Automation of impact analysis:
    - Traceability (embedded in the full process, documentation and code).
    - Analytical self-declaration in the classes/objects.

3.4. Platform independence

For an overview on the concept of platform independence, see the RCA Beta chapter “Platform Independence”.
By handling the platform (safe operating system and communication) as a well-specified, independent component, we achieve modularization of the safety case not only between (logical) components, but also between the (software) implementation of the logical component and its (shared) platform.

4. Where is Modular Safety applicable in RCA?

In principle modular safety is relevant for all safe components of the RCA interface architecture. Interfaces that separate components with different change rates or coming from different suppliers, are especially important. This includes:

- Interface between platform and applications (see platform independence)
- Interface APS-OA to OC
- Interface TMS-PE to APS
- Interface APS-SL to APS-OA

5. Summary and outlook

The RCA group judges that “modular safety” is potentially a very important enabler for RCA goals and that the topic has to be further elaborated, also building on the experience of suppliers.

Next steps:

- The study about “modular safety” (smartrail4.0) will be published at the end of 2019.
- This topic could be a candidate for a S2R project.