RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

Concept: Principles of the safety logic

Document id: RCA.Doc.30

Version: Gamma.1

Date: 31.01.2020

Table of contents

1.	**Introduction**	**3**
1.1.	Purpose of the document	3
1.2.	Definition of “principles of safety logic” and the relevance to RCA	3
1.3.	Scope and maturity of the concept, ongoing work, related topics	3
1.4.	Terms	3
1.5.	Additional material	3
2.	**Principles of the safety logic**	**4**
2.1.	Basic functions of the safety logic	4
2.2.	Basic concepts of the safety logic	4
2.3.	Design Principles	6
3.	**Open Points**	**8**

Version history

Gamma.1	31.01.2020	P. Moosmann / L. Weller	Integrated review feedback from 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 into where clarifications or additional content would be helpful. This document provides additional information about the main safety principles used in the Advanced Protection System (APS). APS is implementing a geometric safety logic.

1.2. Definition of “principles of safety logic” and the relevance to RCA

The main purpose of APS is to guarantee that all movements on the track will be safe at any time. The principles of safety logic describe the major concepts and the rules of safety logic to satisfy this purpose. Those principles could directly impact the RCA components and their interfaces. A common understanding and agreement on the principles of safety logic are required for the development of the RCA specification.

1.3. Scope and maturity of the concept, ongoing work, related topics

This is an early publication on this topic from RCA and its main purpose is to establish the topic and initiate discussions with stakeholders in the sector.

A more detailed description of safety and functional principles can be found in document [7]. This document is a working draft that emerged from the work on an APS prototype in smartrail 4.0 and still work in progress.

1.4. Terms

Request and Demand: On the interface level a difference is made between a Request and a Demand. Before executing Requests, it will be checked that all safety rules are met. If the safety rules are violated, the Request will be rejected. A Demand is a request for which the safety rules have been successfully checked. A Demand will not be rejected in normal operation. Since the verification of the safety rules is done in the SL, Requests are usually issued “above” the SL, Demands are issued “below” the SL.

Geometric safety logic: The safety of Movement Permissions is ensured by geometric calculations. All Movement Permissions will be verified by applying safety rules on the geometric properties of physical objects, like trains, points, but also virtual objects like Usage Restriction Areas or Movement Permissions, etc.

Risk-based safety logic: Risks are calculated and evaluated continuously at runtime. Safety Logic ensures that all risks stay below a defined threshold.

1.5. Additional material

The following RCA document provides further information:

[1] RCA System Architecture, RCA.Doc.35

[2] RCA Glossary. RCA.Doc.14

[3] TMS-PE Subsystem definition and Subsystem requirements definition, RCA.Doc.19

[4] APS-SL Subsystem definition and Subsystem requirements definition, RCA.Doc.21

[5] APS-FOT Subsystem definition and Subsystem requirements definition, RCA.Doc.22

[6] APS-MT Subsystem definition and Subsystem requirements definition, RCA.Doc.23

[7] SR40 APS Core Principles, published on www.smartrail40.ch

2. Principles of the safety logic

In RCA different implementations of the safety logic can be chosen, as long as the interface specifications are still respected. However, the interfaces are based on a few basic principles outlined below.

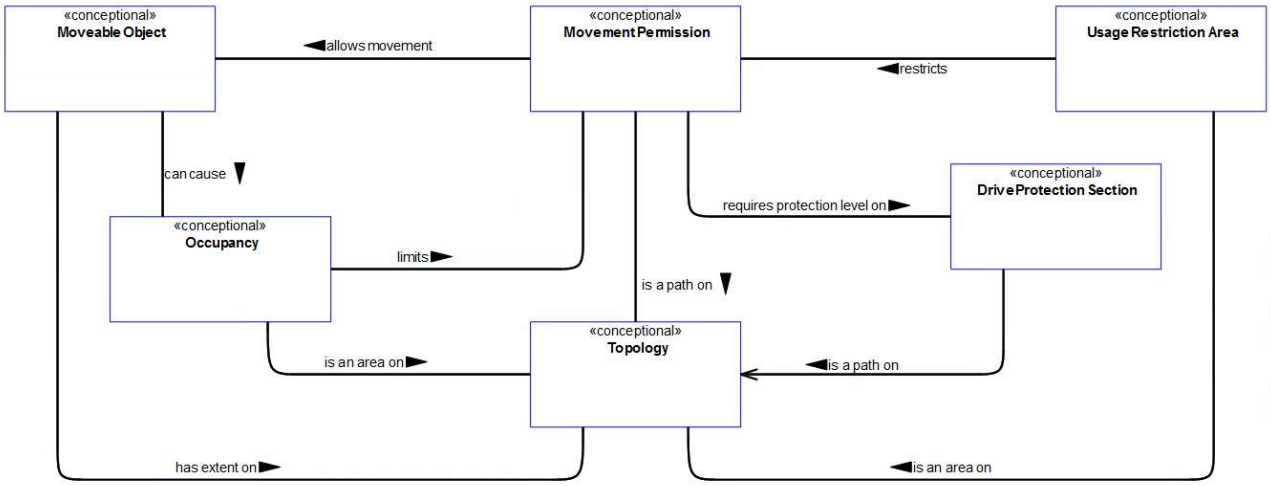
Note: the safety logic of RCA is implemented in the components APS-SL (Safety Logic) and APS-SM (Safety Manager).

2.1. Basic functions of the safety logic

Following is a list of all the main functions, including short descriptions:

- The safety logic in APS-SL verifies whether the requested movement (e.g., train movement) or object-state change (e.g., move the points) is safe. This means that the APS-SL checks that there will not be a collision and that the object is not occupied by another movement or reservation;
- The safety logic APS-SL is the only component allowed to demand a state change of an object (e.g., level crossing). After the safety check of the requested state change (sent, e.g., by the TMS), the APS-SL demands the state change from the corresponding object via the Object Controller;
- The operating state is the "heart" of the whole system. All current states (e.g., moving objects) and demanded state changes are stored in it. The object aggregation deduces the state of the real objects from the information it collects from all the objects (e.g., trains, points, etc.) and stores these states in the operating state;
- The safety logic in the APS-SM monitors all operations on the network through the operating state. If the APS-SM detects a violation of the safety rules, it triggers a measure to minimize the risk (e.g., emergency brake, warning). Following are two examples although there will be other risk minimizing measures:
    - The APS-SM may demand emergency stops if a violation of a safety rule is detected (e.g., train is detected outside the limits of permission);
    - The APS-SM may demand a warning if an object violates a safety rule (e.g., warn a worker who is too close to a train movement);
- The safety logic (in APS-SL and APS-SM) explicitly ensures only safety of movements but does not consider any operational implications (e.g., does this movement lead to congestion or a deadlock). This deliberate design decision enforces a strict separation of concerns, which provides several benefits, like separate lifecycles of the business logic and the safety logic. This enables fast, innovative and cheap improvements of the business logic and reduced development and maintenance costs for the safety logic.

2.2. Basic concepts of the safety logic

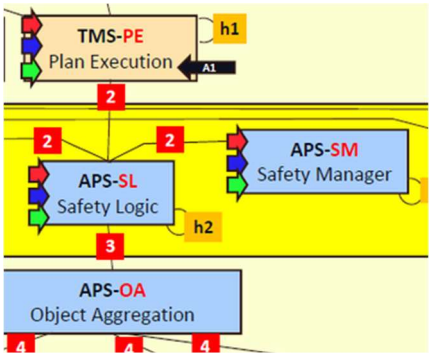


Movement Permission	A Movement Permission is an authorisation for a particular Movable Object to move in a defined direction, with a defined speed, along a defined path on the track network. This includes data on track-conditions as known today in ERTMS/ETCS. The Movement Permission is requested by the traffic management system and verified by the APS-SL. After verification that the Movement Permission is not conflicting, a movement authority is sent to the Movable Object (e.g., Movement Authority in ETCS). A Movable Object shall be supervised in such a way that it never leaves its Movement Permission. Movement Permissions may overlap under certain conditions (e.g., joining).
Usage Restriction Area	It is possible to set a Usage Restriction Area over a certain part of topology (e.g., track segment). A Usage Restriction Area request is typically submitted due to an exceptional situation (e.g., landslide, maintenance work, etc.). This request may be submitted by the TMS as well as by the safety manager APS-SM (watch dog). A Usage Restriction Area and a Movement Permission may overlap under certain conditions (e.g., construction vehicle must enter into a construction site).
Safe Distance	The Safe Distance (in time and space) between two consecutive utilisation permissions (Movement Permissions, Usage Restriction Areas) is needed for safety reasons. To ensure these Safe Distances, Risk Buffers will be set at the boundaries of the utilisation permissions.
Drive Protection Section	Any asset in the field that requires to be controlled before a safe utilisation is possible and therefore may not always be available in a fully trafficable way is represented in APS by a Drive Protection Section (DPS). Drive Protection Sections are typically used for (non-exhaustively): • points • single- or double-slip crossings • derailers • turntables • level crossings • gates Each section that may be trafficable or not, depending of the state of the trackside asset, leads to one distinct and identifiable DPS.

	A set of DPS that cannot change their state independently of each other are grouped together in a DPS group. A DPS has mainly two state attributes: • trafficability, which may be fully given (full), not given at all (none) or only given under certain circumstances (limited) • flank protection, which is either given or not
Occupancy	An Occupancy Section is a not necessarily linear extent of topology which can be reported as vacant or occupied by Train Detection Systems. An Occupancy is created if an Occupancy Section has been identified as occupied, but the identity of the Movable Object causing the occupation is unknown or uncertain (if the Movable Object is known, the occupancy is determined by the Movable Object). Disclaimer: Occupancy is not an agreed concept and may change in future releases. Further work on this subject will be needed.
Movable Object	A Movable Object is a representation of a uniquely identified real-world movable Object. In APS, Movable Objects are track guided (non-exhaustive list): • single vehicles (e.g., locomotives, coaches or construction vehicles) • vehicle groups (e.g., Multi-unit trains, group of coaches) A Movable Object represents the occupational claim of an identified and localised physical object and thus is always of greater extent than the represented physical object. This is because the Movable Objects extent depends on the localisation technology with which the vehicle/ vehicle groups is equipped and, thus, differs in its accuracy.

2.3. Design Principles

Principle: Splitting safety logic into APS-SL and APS-SM



Rationale: See also the component descriptions in “RCA System Architecture” (RCA.Doc.35).

- APS-SL: The main purpose of the APS-SL is to react to requests from the plan execution by either granting them (if safe) and relaying commands to vehicles or trackside objects, or rejecting, based on the safety logic and the knowledge of the operating state. This implementation is expected to be almost universal (except for parameters such as overlap).
- APS-SM: the main purpose of the SM is to observe the operating state and to trigger actions to react to situations becoming unsafe due to external effects (e.g., point lost position, vehicle no longer localisable, etc.).

Therefore, the main reasons for separation are:

- differing activation model: request / reply vs continuous observation
- differing change rates: the SL is expected to have fewer changes than the SM.

It is not the role of the APS-SM to do technical monitoring of the operation of the APS-SL, or to be a diverse implementation of the APS-SL. Both APS-SM and APS-SL must attain their SIL4 rating with built-in mechanisms of their own.

As the figure above shows, the APS-SM is connected through interface 2 to the APS-SL. The APS-SM has neither connections to the APS-OA nor to the lower “device-abstraction” and “device-control” layers. Actions are demanded by the APS-SM over interface 2 and executed by the APS-SL. The difference between “normal” actions requested by the TMS-PE and actions demanded by the APS-SM is, that the APS-SL must execute demanded actions in any case, whereas normal actions can be rejected by the APS-SL.

The separation of SL and SM comes with a price: complexity is increased.

Principle: A Movable Object shall have a Movement Permission assigned to it all the time

Rationale: As a Movable Object registers in the APS, a Movement Permission for that Movable Object is created at the same time. The Movement Permission can be altered afterwards. The extent of the Movement Permission shall always be at least as long as the extent of the Movable Object. Reason: the APS is responsible for granting conflict-free Movement Permissions and safe movements of vehicles. The vehicles (supervised by their OBU) are responsible for staying inside the Movement Permission all the time. Therefore, a Movable Object must have always a Movement Permission. Exception in ETCS Level 1/2: If a vehicle is not registered, trackside assets (TDS) detects the vehicles and creates Occupancy for the occupied track section.

Principle: Necessity of Occupancies

Rationale: The Occupancy concept was introduced for several reasons. In an ideal situation where a vehicle is always connected and registered in the APS, Occupancy might be not necessary. In real situations and during the long migration phase, Occupancy will be necessary in the following situations (non-exhaustive list):

- parked vehicles that are not equipped with (e.g., freight wagons) or have a defective onboard unit;
- vehicles that have not been fully identified (e.g., at start-up when no safe length is provided);
- trains with ETCS onboard units and a localisation tag at the end and/or which use trackside TDS.

3. Open Points

These open points are known at the time of publication of this document:

- Principle “Necessity of Occupancies“: There are currently different views on this principle. Further discussion and consensus will be needed for a final decision. In addition, the definition of Occupancy is not aligned with the traditional meaning.
- Principle “A Movable Object shall have assigned a Movement Permission assigned to it all the time”: There are currently different views on this principle. Further discussion and consensus will be needed for a final decision.
- The concept doesn’t cover non track-guided Movable Objects. Further development will be needed.
- The role of the Safety Manager has currently not been analysed in depth. Further development will be needed.