RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

"A.P.M.": APS / PE / MAP

Advanced protection system, plan execution and map data management

Business strategy, targets, and problem definition

Document id: RCA.Doc.50

Version History

0.2	10.8.2021	Second draft (unfinished)	Steffen Schmidt
0.3	2.10.2021	After review 1 and correction	Steffen Schmidt
0.4	9.11.2021	Alingment with Objectives	Lia Steiner
0.5	26.11.2021	Review comments implemented	Lia Steiner
0.6	28.01.2022	Review comments implemented (TMS experts, ProRail)	Lia Steiner

Release information

Basic document information: RCA.Doc.50, A.P.M Business Targets and Strategy

Version: 0.6

RCA Baseline set: 0.4

Approval date: tbd

Sources

This documents uses, amends and aggregates results from several projects like OCORA, RCA, EULYNX, Linx4Rail, smartrail4.0.

Disclaimer

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. Formal requirements management and change management will be introduced in future iterations. The content may be unfinished, will likely contain errors and can be changed without prior notice.

Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback

For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu

Content

1 Intention of this document, target group

This document explains the motivation, targets, the basis of the business case and basic strategies of the evolutions and innovations of some of the trackside CCS (control-command and signalling) subsystem of the rail system. In the further chapters we will focus on three specific subsystems that will be explained.

The target groups are CCS managers, CCS life cycle and asset managers, CCS technology strategists, CCS procurement managers, CTO and technology innovation strategists.

2 Status of work

“Plan Execution” (PE), “Advanced Protection System” (APS) and “Map” are core projects inside RCA (Reference CCS Architecture) that are generating an architecture description (business and operational requirements, and interface specifications) to be used as a **standard reference tender specification** for enabling of further specification steps and specific implementations. All three together as a concept are called “**A.P.M.**” in this document and offer: “Advanced protection system, plan execution and map data management”.

This document describes the main strategies behind A.P.M and the main business targets. It is part of a set of documents that will form the “A.P.M. concept”. Other documents of the A.P.M. concept describe operational scenarios, system definition and analysis, or functional analysis and logical architecture.

Currently the “A.P.M. concept” as well as this document are work in progress.

3 Use of this document

The A.P.M. concept documentation shall be used as a general description that helps to understand the basic intentions behind the A.P.M.. It will be used for communication and onboarding events, for discussions about product development strategies, or to describe the business expectations for feasibility studies or for the design of prototype projects and pilot lines.

Important requirements on target level are marked with a “#Requirement-Keywords” tag. All tags are listed at the end to give a compressed overview of all requirements.

4 “A.P.M.” – in a nutshell

A.P.M. sits in the middle of the CCS trackside architecture, which has the typical form of an “industrial automation pyramid”.

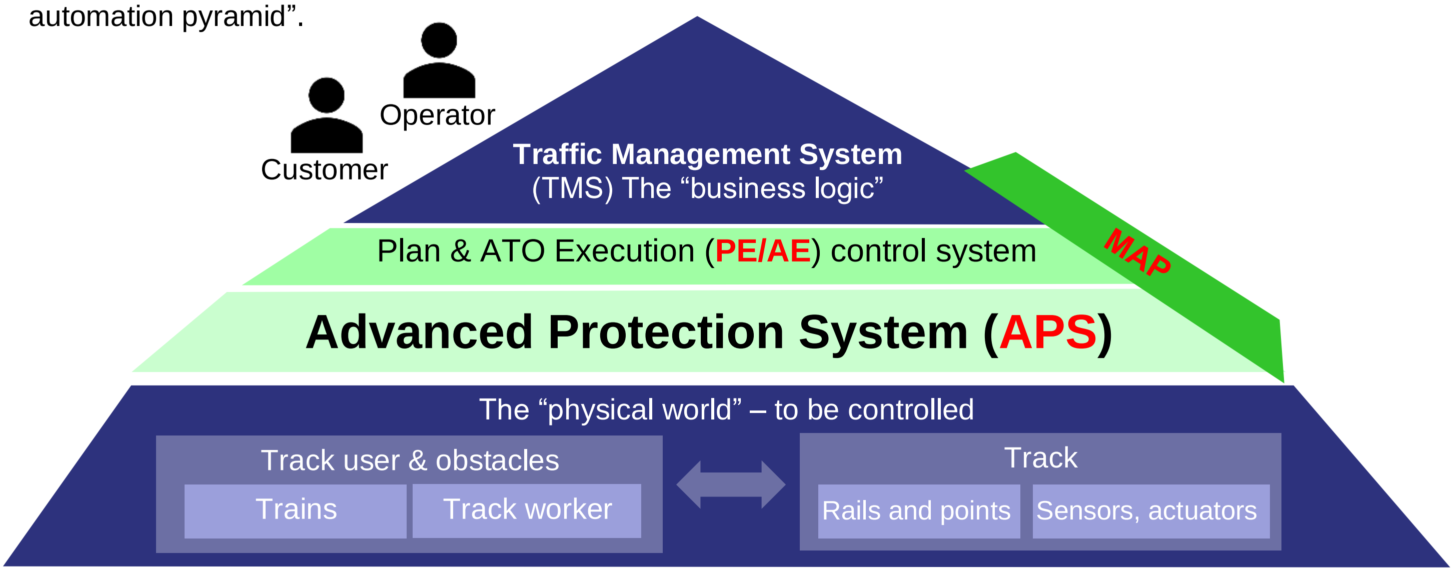

Operator
Customer
Traffic Management System
(TMS) The “business logic”
Plan & ATO Execution (PE/AE) control system
MAP
Advanced Protection System (APS)
The “physical world” – to be controlled
Track user & obstacles
Trains
Track worker
Track
Rails and points
Sensors, actuators

Figure 1: A.P.M. in the middle of the railway production (in green)

The Traffic Management System (TMS) plans and decides “when is what to do”. The Traffic Management System (TMS) continuously re-plans the timetable and decides about measures to optimize the flow of traffic on the network for any planning horizon (short to long-term) and for any type of track usage. TMS is typically a large IT system landscape, which delivers a production plan. The production plan is analysed and executed by “plan execution” control systems that send commands to train (trackside automatic train operation systems, AE) and trackside (PE). The APS assures as a gatekeeper, that the plans and commands of the TMS and AE/PE create a safe traffic flow and then executes them. APS assures safe track usage and uses the sensors and actuators in trains, mobile track user devices (maintenance teams) or trackside assets to control and supervises the railway production. MAP provides reliable, validated topology and topography data (Map Data) for all operational RCA subsystems, including safety-critical components. Another important goal is to control the distribution of the Map Data from a single source to the relevant subsystems. A.P.M. must fulfil very high availability, safety and security standards.

A.P.M. is a generic term for functions of the future railway system architecture that are today located for example in centralized trackside control systems (CTC), interlockings (IXL), radio block centres (RBC) and trackside functions needed for controlling automated train operations. Or in other terms: A.P.M. is the trackside part of CCS without including TMS or the trackside assets.

The term “advanced” in A.P.M. shall only be used in the case that the requirements described in this document are fulfilled. Otherwise, the term “trackside protection systems” is used. This document does not describe all customer requirements for a railway CCS, the new and advanced features of A.P.M. are focused.

A.P.M. does not stand for a certain technology; it stands for a set of **challenging business targets** and requirements that are described in this document. The concept of A.P.M. describes a quantum leap of innovation in this area but potential technical solutions for all requirements are known.

APS itself is only usable in conjunction with PE since the functionality split and scope is completely different compared to today's interlockings. To keep the "SIL4-related functionality" as small as possible APS only contains the minimal necessary functions to assure a safe production. Every other function else is shifted to PE or TMS (shop, planning, overall optimization, …).

5 The business case of A.P.M.

Today's CCS systems are based on older technology structures. The business goals behind A.P.M. are to endorse optimal use of the physical track capacity (real-time, precise), allowing a very high grade of automation for the production with high reliability, safety and security. Modern automation technology concepts can create a quantum leap when they are introduced into the CCS area.

A in detail calculated (and checked by external experts) business case proves, that the economic impact of the improvement of CCS based on an ideal protection system is large. The potential cost reduction (asset cost, maintenance cost, railway operational cost, less tracks) can reach a dimension of up to 40 Mio€ cost reduction per 1.000 km track and year (depending on the initial grade of automation in the base case, the legacy technology, target safety level, target reliability level, local price level, traffic density / CCS asset density).

Additional effects are the safety automating coming with the continuous speed supervision and full dynamic supervision of shunting and track workers, and the higher reliability because of the lower amount of trackside assets and systematic redundancy for central CCS functions based on modern IT technologies.

To achieve these business goals, A.P.M. at first stands for a **challenging set of customer targets** for the next generation of trackside protection and control systems. The following table references the A.P.M. relevant goals out of all identified RCA goals (RCA.Doc.48 Realization of RCA Goals).

A.P.M. #business target indicators (direct effects and indirect effects)

A.P.M. Goal	**Description of the target**
Decreased whole life cycle cost (Capex + Opex) (G1) #35% LCC reduction	Up to 35 % reduction of the life cycle cost of the CCS Infrastructure: ▪ reduction of up to 65 % - 70 % of trackside assets ▪ support increased automation for activities such as engineering, maintenance, planning (during whole lifecycle from migration/implementation to depletion) ▪ modular system architecture with LCC dependent split
Increase capacity (G6) #15-30% capacity improvement	Increase of 15 – 30% (example SBB) to be used for increased traffic volumes (in combination with a more sophisticated TMS) while avoiding / reducing investments in tracks / points.
Improved Performance (G7) **(availability / reliability / operational stability/ recovery)** #50% RAM improvement	Increase of punctuality and available customer service through: • 40 – 50 % reduction of trackside device failures (through asset reduction) • Improved maintenance (Condition based maintenance, devices better designed maintainability) • Timetable stabilization, by having more reserve time between the trains, through increased capacity. • Reduced manual errors

A.P.M. Goal	Description of the target
Increase safety / Reduce collisions (G8) #safety improvement	Increased safety for shunting and of construction sites through localisation and “full supervision” at all times.
Increased Security (G14) #security state of the art	Security is an integral part of the system design (“security by design”, IEC 62443)
Speed of rollout (G10) #50% faster rollout	Industrialised rollout: Accelerate commissioning and putting into operation by 50 %. Necessary to handle upcoming replacement peaks. Also contributes to cost reduction (see above). This is depending also on other innovation projects (e.g. EULYNX).
Customer information (G11)	Precise customer information based on detailed, precise and automatically provided production status
Reduced journey times (G12)	Acceleration effects are supposed to be low and reduced journey time is invested in stability of the network. Not explicitly part of all IM’s business cases.

6 The frame conditions and technical characteristics of A.P.M

From the perspective of the users targets a “trackside CCS system is an A.P.M.”, when it fulfils the customer targets listed in this document. In the terminology of RCA the A.P.M. is only then an A.P.M. if all of its RCA standard interfaces are implemented (to TMS, trackside assets, train, track worker safety systems, other signalling systems).

The default configuration is built on the following #frame conditions:

- based on radio-based ETCS (Level 2/3) without lineside light signals
- applicable for different types of railways lines (regional, low density, urban, main line, high speed)
- supports modular migration (independent “modules” TMS, APS, PE, MAP, trackside assets)
- allows flexible migration of fleets concerning ETCS equipment versions/functions
- supports Automated Train Operation (ATO) Grad of Automation (GoA) 2-4 and operation in GoA 0 and 1
- support for standardized interfaces to trackside assets (EULYNX)

The A.P.M. approach is at first an initiative for a worthwhile innovation, whereas its standardisation is just one aspect of this approach. In the course of this document it will get obvious, that the standardisation of the A.P.M.-external interfaces is anyway a prerequisite to fulfil the customer targets (life cycle optimisation).

7 Operational strategy

The operational strategy with the usage of A.P.M. is based on #unified operational processes within the Single European Rail Area (SERA) for normal operation and degraded situations for the target systems. These unified operational processes are the main prerequisites for the successful technical standardisation improved interoperability and a big enabler of fundamental change in operation. They will enable the smart usage of technical solutions from the thinking of the operational purpose This must become possible for #cross-border operation in European corridors.

A.P.M. supports a limited operational freedom to choose necessary functions and parameterize them. An optimum between standard and adaptability on operational needs shall be assured. This enables in addition the reaching of several business goals for the overall system:

- #high grade of operational automation (also for shunting or degraded modes)
- #low rate of wrong decisions and risks
- #fast recovery from incidents and short usage of degraded modes for operation
- #flexible operational alternatives in case of deviations from operational normal states

The main idea is, that all train movements (on demand, short-term to long-term, strategic, conceptual, operational) are considered within the operational plan (#plan-based). Part of the planning process is the #intelligent incident handling as well as the processual and #functional assistance of construction works, that enables a smooth operation.

Deep granularity and efficient performance on the operational plan is gained through the availability of any needed #detailed information for the Traffic Management System (like precise speed profile, breaking performance, train-specific track usage conditions). Each train movement shall use the infrastructure as best and efficient as possible. This means also to protocol a sum of possible running characteristics e.g. specific speed profiles per different train categories available for specific piece of tracks as well as to ensure an ongoing precise data exchange between all systems.

In addition, operation is stabilized by minimizing driving variance through the support of ATO in the Grade of Automation (GoA) as needed for the specific movement and suitable from Infrastructure Manager perspective. This means operation can be chosen on the GoA level needed from the operational context.

Operational targets are ensured and reachable by:

- #enable the TMS/PE to precisely steer rail operation on track and train
- more capacity through #shorter headway by better usage of infrastructure considering the details of the running train formation and the precise occupation information
- #faster adaptation of infrastructure to operational needs based on the reduced complexity and standardised solutions
- supporting #automation of infrastructure and vehicle operation (up to GoA 4 depending on needs, no operational staff needed on-board, all functions are executed automatically)
- concentrate on minimal needed functions and processes for enabling structured approaches within the technical solutions to be changed or developed
- less energy consumption and wear & tear optimization for trains
- enabling an appropriate #migration strategy reaching a unified technical base

Today, operators in control centres need to be trained on different complex legacy systems and are partly supported by automatization. In the case of partly automated operation the staff is on the one hand not involved for the automated parts and on the other hand faces a high demand for actions in case of deviations and incidents. This asks for good training and a high skill sets to take on responsibilities from the system. By changing the operational approach and the technical system the aim is to get #more assistance by the system for the operators. The more automated and transparent systems should help to reduce personal decision making under pressure and enable a simple training as well as usage of the learned proceedings. In addition, the development shall consider a changed level of skills per person in general and enhance the attractiveness of the operator job as a full automation won't be reached in near future.

Operational implementation compared to today

To explain the practical impact of this strategy the following mission statements shall describe as examples, what A.P.M shall achieve on an operational level:

1. There shall be #no movement categories necessary like "shunting" with special modes or rules, if the implemented configuration and fleet equipment allow this. There shall only be movements with a high grade of supervision. If a train does not deliver enough information to enable full supervision (temporary or in general) A.P.M shall handle the mix of human and technical supervision safely and efficiently.

2. A.P.M shall #not generate needs for voice communication (even in degraded modes) or manual steps if the implemented configuration (TMS, PE, train systems, trackside systems) allows a full or a high grade of automation and therefore no more needs voice communication including exchange of written orders.

3. A.P.M shall support a high grade of automation of processes in operation centres and operational work to increase productivity, reduce reaction times and to manage complexity. For this the APS/PE interface shall offer an open, standardised and flexible interface for several (and perhaps unsafe) automation systems.

4. A.P.M shall allow #"rich" degraded modes which means that even in a situation with reduced availability of reliable information the best reduced production shall be allowed that is still safe based on this information

5. A.P.M shall support a high efficiency and grade of automation for ETCS operations, especially for processes like 'start of mission', 'transitions' and 'mode changes' as well as 'joining/splitting'.

Operational scope

A.P.M shall handle #all railway operations for highspeed, mainline, regional, or urban railways in an efficient way. The operational scenarios are described in the A.P.M models as "functional chains" and operational sequences.

Guideline for the definition of detailed operating rules

#APS does not support a traditional logic for lineside signalling (and does not connect to the signal interface of EULYNX) since lineside signals are not part of the standard APS configuration. For special lineside signals for example at the border to foreign areas or special signals in stations (wagon crossing) the APS information about movement permissions can be used for signalling simple information.

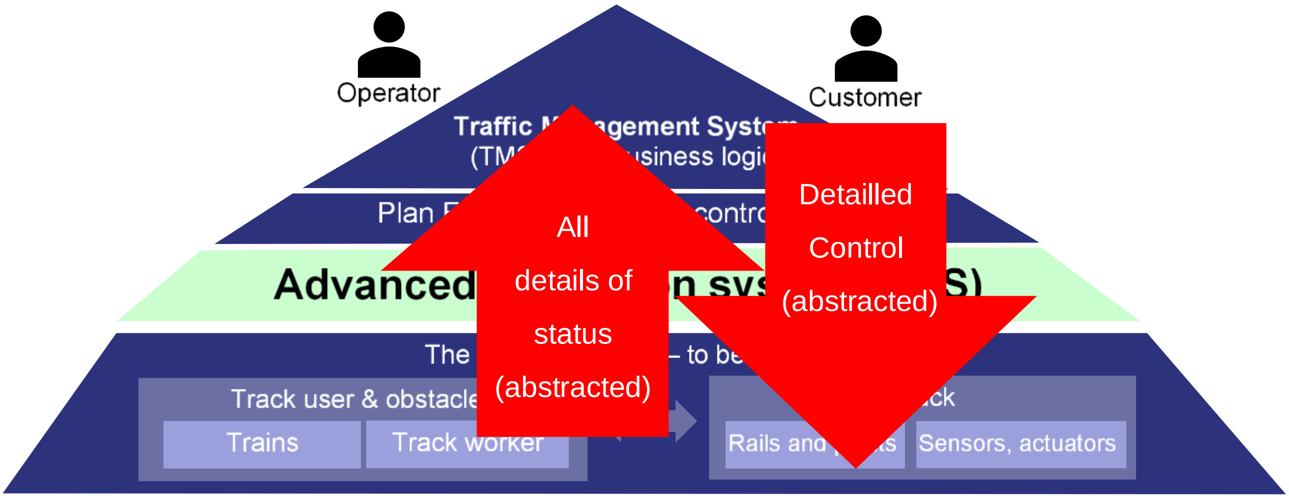
#A.P.M implements the ERTMS operating rules (TSI CCS Appendix A) with some important enhancements and exclusions:

a) Less or no manual interaction between driver and signaller (to be substituted)
b) support only of ETCS Level R (CR 1234)
c) capitalize the TSI CCS enhancements “always connected” (e.g. UNISIG-CR 1350) and “cab anywhere” (e.g. UNISIG-CR 1367)
d) support technically supervised shunting
e) support connectionless communication also via FRMCS
f) support ATO over ETCS operating up to GoA4
g) capitalize continuous precise on-board localisation
a. support digital automated coupling

8 Architecture, system and asset management strategy

8.1 The basic aspects of the A.P.M asset management strategy

A.P.M shall support a high grade of automation by transporting the #detailed production status to PE/TMS and by #allowing PE the detailed but supervised control over all actuator capabilities (based on hardware abstraction mechanisms)



#Decouple different types of life cycles (modularisation) and different types of major functionalities (e.g. concerning safety or availability requirements) with #standard interfaces to reduce integration effort (for suppliers, integrators, customers) and to #create the potential for a broader market offer by more specialized companies or subcontractors of the industry

Use #modern and proven ICT architecture, maintenance, and deployment strategies whenever useful (like automated upgradeability, continuous deployment, remote maintenance, integrated standardized diagnostics, scalable microservice architectures, etc.)

Apply #architecture layering, #hardware abstraction, #strong independency management, #adaptable intelligent interface strategies (exchangeability, lose coupling for downwards and upwards compatibility, etc.)

Use common-of-the-shelf components or common cross-sector solutions whenever possible and rational.

#small safe components: Allocate all functionality with no safety relevance outside of the safe systems in other architecture layers (allocate them in Traffic Management System or Plan Execution system)

#reduce the technical skill demand on the side of the users (specification, application design, operation, maintenance, etc.) by smarter safety-logics, automates high-quality tool chain, avoiding complex technology mixes and supporting platform services (like “software as a service”)

#reduce the safety case effort by decoupling component safety cases and their mutual safety relevant interaction (change impact reduction, automated change impact analysis, preparation as generic as possible)

#Provide high usability for GUI and don't distribute user interfaces to many other systems. A.P.M itself shall mostly be a "hidden" functionality (except services or interfaces for the reliable display of the actual production status to e.g. TMS).

8.2 Architecture strategy for A.P.M: Business targets for the main functions

A.P.M shall implement the major functionalities with the following business targets

a. **"Plan execution":** In PE all automation functions (split a plan to single commands at the right time), that today typically reside in interlockings or centralized control systems but have no or minimal safety relevance, shall be allocated to #reduce the size of the "SIL4 layers". The business target behind PE is to offer simple OR also sophisticated interfaces to traffic management systems that accept simple operational plans (just like a list of planned movements A to B), or very precise optimized operational plans (making use of train specific properties and speed optimisation).

b. **"MAP":** This centralized function shall provide actual and reliable MAP data (layered data structure with geometry and object layers) for several functions at the same time (#data preparation synergy) and based on a data exchange standard. This also shall #reduce interface complexity and manual work for data conversion processes.

c. "**APS Feature - Safety Logic**": #generic standardized safety check function with a generic safety approval, in every installation the same, no special configuration that #only needs actual topology and train information (functions, properties, status) to check reactive, if actions (like new movement permissions) requested by systems like PE/TMS are fulfilling (configurable) safety constraints like the minimal distance between track users or the allowed relation between distance/speed/protection of track users.

d. **"APS Feature - Safety Manager":** #generic risk pattern recognition function that actively identifies configurable patterns in the overall status and sensor information coming from trains, track users or trackside assets

   - for **safety events** like a fault of point machines,
   - and for **operational risk events** like detected persons on neighbour track). It creates information or action requests for the Safety Logic, PE or TMS functions (TMS includes for example incidence management)

e. **"APS Feature - Object Aggregation"**: This #sensor-aggregation-function shall allow to connect multiple types of on-board (trainside), mobile or trackside sensors and information systems to retrieve and combine information about production objects (like trains, persons on track, trackside assets) like identities, status or occupation, and to aggregate, store and forward the status history. The function shall allow to #split/copy/distribute a single command from the Safety Logic to several receivers for which the command is relevant (like a movement permission) by using abstracted addressing.

f. **Device abstraction Layer, 3 main functions called "transactors" (**"Movement Authority Transactor" to the train, "Fixed Object Transactor" to the trackside assets, "Mobile Object Transactor" to track worker safety systems or mobile devices): This layer divides the low number of more central production IT systems from the physical world with a high number of expensive assets (train, trackside). The business targets for the 3 main functions in the device abstraction layer are:

- #device function abstraction which means that even different forms of device (train, trackside) implementations with a proven compliance to the standardized transactor interface shall be a working replacement for other implementations without effort
- #protocol translation of different protocols or protocol releases to be able for example to mix older and newer ETCS on-board unit (operation) system versions on a line or different releases of EULYNX protocols or interface variants of trackside assets
- Protocol translation (from generic protocol inside A.P.M. to the specific protocols of devices, like ETCS) shall also allow to reduce the risk of large system impacts coming with the evolution of ERTMS.
- #capability-matching: Protocol translation shall allow the retrieval of abstracted device capabilities on runtime (or in degraded modes) so that matching protocol variants can be used by the transactor >>> Allow the connection of devices with “much or less” capabilities, reduction of planning and configuration work

Other functions of A.P.M. shall be implemented along the state-of-the-art objectives especially concerning integrated identity and access management, integrated diagnostics, integrated configuration management, and integrated workbench platforms.

8.3 Architectural environment for A.P.M.: Interfaces and migration

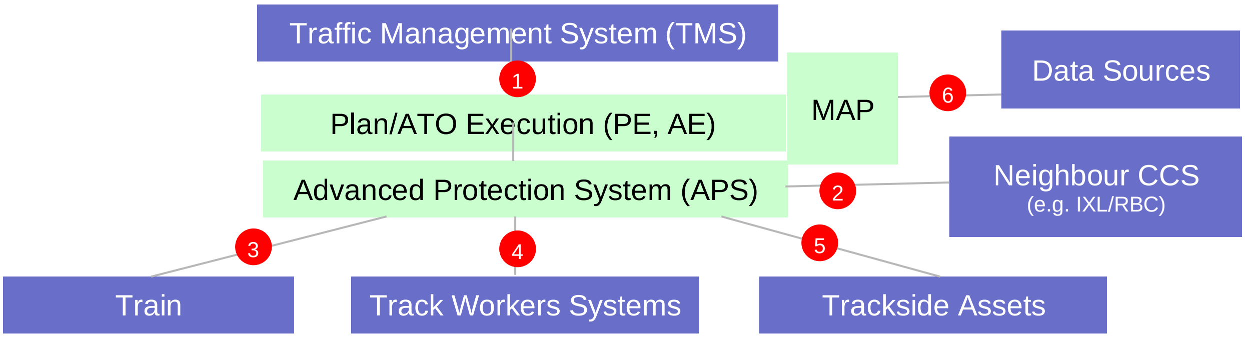

Traffic Management System (TMS)
1
Plan/ATO Execution (PE, AE)
MAP
6
Data Sources
Advanced Protection System (APS)
2
Neighbour CCS
(e.g. IXL/RBC)
3
4
5
Train
Track Workers Systems
Trackside Assets

Figure 2: A.P.M. and its 6 main interface partners

1. #APS shall only have one future oriented interface to the Plan Execution Systems (PE) that follows the future design and requirements. #Migration support for existing TMS**:** PE/AE shall handle the migration aspects for connecting to older/today's "route-based" Traffic Management Systems or central train control systems by offering standard interfaces for older TMS.
2. #Interface to traditional interlockings/RBC and to other APS. In terms of migration APS must handle the interaction with other APS with a new standard interface and (#Migration support to connect to existing interlockings/RBC) to today's interfaces to interlockings (based on EULYNX standard) and RBCs (based on the TSI CCS interface definition).
3. #TSI CCS compatible especially for the enhanced features coming with TSI 2022 but also for future improvements (postponed TSI CCS change request like for onboard localisation). #Migration support for existing ETCS onboard units: APS shall be as backward compatible as the TSI CCS and its transition rules define, excluding compatibility to Baseline 2.
4. #Standard interface for trackworker safety systems and mobile safety devices. Migration support: There is no generic interface concept that is realistically preserving old interfaces compatible to a new standard interface since existing trackworker safety systems have a wide variety of proprietary interfaces with very different solutions and information flow.
5. #Standard interface for connecting trackside assets based on EULYNX: APS shall be compatible to the EULYNX interfaces to point-machines, trackside detection systems, level crossings and generic IO for baseline 3 or higher. Migration support for non-EULYNX compatible trackside assets is not included in the APS functionality.
6. The MAP function shall offer a standard API, UI and import functionality without adding migration adapters. The API shall support the multichannel validation of data to #achieve reliability for the MAP data for safe applications.

9 **RAMSS Strategy** (Reliability, Availability, Maintainability, Safety, Security)

Scalability and cost optimization

Generic functions, rule based configuration adaption (e.g. configurable pattern matching in the safety surveillance) and configuration features (software redundancy configuration, trackside configuration, APS computing system structure) as well as operational standardization shall support a cost-efficient optimization of RAMSS. Thus a #LCC-oriented RAMSS scalability shall be a major objective for A.P.M..

Modernisation and Security (see also: RCA security guideline)

The stepwise modernisation of the railway system leads to a wider usage of IT-based parts in the system. Based on the principles of ISO 27001 and IEC 62443 an appropriate mitigation strategy for #assuring security and avoiding damage from cyberattacks shall be applied. This especially means:

a. implementations based on “security by design”

b. implementation of multi-level security zones

c. broad implementation of security monitoring functionalities

d. implementation of state-of-the-art identity and access management

e. implementation of self-secured data flows (end-to-end security)

f. deep analysis of used third party components

Completion of safety considering in overall CCS, modular safety

Current system suffers on inequality on safety consideration. This means some parts of CCS are developed in a very safe manner to ensure an overall safety level where other long-term existing parts are developed in the past as being safe-enough compared to older systems in the past. Sometimes systems are named as “safe” but without any possibility for quantification of the exact level.

The full standardization and specification covering the full CCS architecture and end-to-end process enables a complete consideration of safety in the CCS domain. This enables to lift also (less) safety needs in some technical domains due to a better balancing of parts of the CCS domain and a real calculation of a comparison to the targets of the overall operational performance.

The safety related development within a safety organisation shall support a RAMSS-compliant standardisation by gaining technical compatibility as an additional essential requirement and operational interoperability not restricted by safety mitigations.

This includes drafted set of deliverables according to CENELEC development phase 4 for generic application as a tool-box principle for further detailing:

- System Requirements (functional, non-functional requirements)
- Interface Specification
- #Digital Safety Case including risk analysis based on unified operational processes

Considering the formal documentation, a #generic hazard management for the generic application shall be ensured on European level leading to a minor necessary specific handling for the various Infrastructure Managers including the National Safety Authorities.

RAM considerations

From a business perspective, a compatibility regarding the RAM requirements between products facilitates their integration and subsequent life-cycle phases compared to today’s CCS system.

The reliability of the system depends on the robustness of the components minimising random failures, and the diligent application of quality management process during the system’s life-cycle minimising systematic failures. The reliability is also considerably influenced by the reliability of the computation platform and transmission network which enable time-based data transmission with low latency.

A low level of down-time of the system and its constituents due to faults and maintenance activities provides the conditions for a high overall availability. Nonetheless, all constituents must be considered with certain non-availabilities and monitored if needed. A major factor to recover from a degraded situation is the possibility to perform maintenance activities promptly due to improved accessibility and independence of constituents enabled by the highly modular approach to the system architecture.

For the provision of quantities and frequencies of processed data towards Monitoring, including RAMS performance values, that are gathered in service during operational and maintenance phases are recorded in order to check if there is any deviation from theoretical and expected RAM figures. This further improves the coordination and planning of RAMS activities by the respective Infrastructure Manager.

The strategic definition of RAM shall enable a high system safety by operation on the highest possible safety level but shall avoid that the RAM parameters become an essential part of the safety demonstration because this would necessitate a system-supervision not being possible by the current technical solution. Additionally, the RAMS documentation and approach must enable an immediate update according to security threats with less effort for approval. Thus, RAMSS requirements must be balanced according to different needs from the early beginning of system design.

10 Development and implementation strategies for A.P.M.

The development is based on the one hand reflecting an appropriate RAMSS strategy and on the other hand deriving the correct needs. The development shall be a task in close partnerships of different stakeholders:

- Infrastructure Managers
- Railway Undertakings as “users” of the infrastructure
- Rail Industry
- Research Institutes
- Authorities and Inspection Bodies

The stakeholders shall participate for enabling a best-fit of knowledge and experience as-well a distribution of tasks to be performed in development phase. This will enable:

- best share of competence and experience by coordinated work with all stakeholders
- best use of capacities of persons in the overall rail sector

- shorter (supplier) specification phase by enabling formal split between standardisation, customer requirements/industry specification and design of products
- simple adaption including re-certification as consequence of an overall system definition respecting not only the technical solution by taken operation and processes into account

There are several implementation strategies for A.P.M., that can fulfil a part, or all of the targets listed in this document. It may be an evolution of existing systems (interlocking, RBC, etc.) or a completely new development without refactoring any legacy. It could just be a new software suite on already existing hardware platforms. The pros and cons for the development strategy are not discussed in detail in this document.

It shall only be noted here that the characteristics of APS allow a very slim, simple, flexible and powerful implementation of a trackside protection system, if this is done from scratch and resembles the development method used in the past for safe RBCs, based on a track usage management with geometric algorithms. Feasibility studies and Rete Ferroviaria Italiana (RFI) showed that this implementation strategy has a very good chance to fulfil the APS targets listed in this document for a reasonable price and with a fast amortisation. Other implementation strategies may struggle to fulfil all targets because of legacy constraints but can do early and fast evolutional steps. Therefore, the characteristic of the recommended implementation strategy is

- #use existing modern (safe) hardware environments that allow centralized and decentralized system topologies. #build on common communication technologies.
- Use partnership models that are successful for distributed software development.
- Use public reference implementations (e.g. digital twins) for very important core elements of the application that reduce the compatibility and life cycle risks for this development. Market product USP shall take place in the non-core functions and the integration services
- Set a high priority for a high-quality architecting process that leads the development and assures the targets of this documents
- #simplify the RAMSS controlling for the development process und the RAMSS change impact analysis for changes inside of the life cycle
- Implement a “continuous testing and deployment” process for the architecture

11 Resulting characteristic of A.P.M.: A challenging set of customer targets.

The following customer targets and requirements are the result of a long period of project analysis in large railway CCS digitization and automation programs. The selection here excludes the ATO discussion in this document release and excludes also aspects that need innovations for which no solution is expected in the next 10 – 20 years.

11.1 Reduce the cost of capacity, enable high performance traffic management

High capacity can be achieved with nearly all old and new technologies by just increasing the asset density and the grade of automation. But this is done often for a very high price. APS shall give information and means of precise control to TMS for a low price by making the full use of the features of radio-based ETCS. In legacy architectures these features are often not or only partly capitalized.

11.1.1 A.P.M. shall offer a very precise real-time train control interface to TMS

Today’s trackside protection systems create a lot of “sunk capacity” (reserves).
Tomorrow: Establish a fine-tuned optimal flow of trains fitting to the actual production situation (TMS acts via APS which controls the ATO/ATP process).

a. #Enable TMS to control the precise optimal speed (curve) of every train depending on the overall situation to create a perfect traffic flow (higher capacity and punctuality)	Static speed limits --> trains hinder each other (less flow)	APM enables TMS	Every train drives optimal in relation to other trains (“zipper”, “riding on green wave”, etc.)
b. #Movement permissions are requested and granted in that moment when they are really needed (based on A.P.M. information)and do not block unnecessarily capacity. Points are prepared in advance.	Too early routes block station capacity	APM enables TMS	Movement permission in the moment where the train should start to move
c. Prognosis calculation gets precise because of #exact train data getting available (speed, position, type)	Plan reserves to compensate unsharp prognosis	APM enables TMS	Reduced plan reserves
d. #Scheduled speed mix (train mix) and form of usage of a track layout can be changed even on runtime without losing the optimum of capacity usage	Fixed optimization of the CCS layout for one form of usage	APM enables TMS	Speed mix and traffic flow can be matched to the track layout dynamically
e. #No unnecessary use or worst-case safety constraints in the operational process (“Risk calculation on runtime”): Train flow optimizers can use situation specific advantages.	Trains drive always along worst-case rules	APM enables TMS	A train „alone in the station” or “with better status” can get more speed freedom
f. #Increase the traffic density by reducing the train ahead times needed for safety	Long distance needed because of unprecise information	APM enables TMS	The physically shortest safe distance can be used as train ahead time
g. #Allow an instant network wide continuous improvement of the trackside CCS subsystem configuration for better performance	Configure CCS behaviour of a station once in 20-40 years	APM enables TMS	Optimize the safe CCS behaviour of the station every day without much effort
h. #Flexible safety pattern configuration: Do not block capacity by safety rules that do not fit in the case of	Static safety rules for every railway block capacity	APM enables TMS	Optimised capacity by configurable safety pattern matching, incl. a static “basic safety”

every railway. Safety can be achieved by CCS systems, other technologies, logically or by humans. Since higher safety of CCS processes downgrades capacity and reliability and is a large cost driver, the CCS systems needn't be always the best place to achieve safety depending on the type of railway production. Because of this the safety niveaux of a CCS behaviour shall be configurable. But the function/software of a CCS system shall anyway be standardized.			
i. #"Locally scalable" investment for mixed traffic densities. In a large station for main line railways with high traffic densities today a high performance CCS system is needed for all tracks although many of them perhaps have only a very low density traffic (like a regional line) that could be done with a low-end CCS system. "Locally scalable" shall mean that the technical effort for the APS can be scaled "per single position" in the track layout or network, and can be changed very fast, if necessary dependant on the usage.	Larger area is managed by one type of CCS category	APM enables TMS	The CCS effort can pe scaled "per position" on the track
j. #Highly efficient platform track usage or shunting without special installations (short platform change times, dense occupation by multiple trains/units. These "short distance coexistence" production processes today need additional CCS equipment, very low speeds plus observers or operative effort. Shunting can be enabled by only a different risk-based operation without any additional installations compared to train runs.)	Short distance coexistence manoeuvres are slow or need additional systems	APM enables TMS	Every type of movement is handled with the same high performance that the physical track allows
k. #New train types and their specific detailed constraints, properties, weakness or strength concerning the safe production (e.g. breaking capacity) can be introduced in the full network in one (central) step and can be validated or measured on runtime, can be taken into account by the runtime optimizers of the TMS.	Static train type categories, rough description, much reserves	APM enables TMS	New detailed train type description can be introduced to all CCS systems in one step.
l. #No unnecessary loss of capacity at points on the track where the speed limit changes Because of the static block-logic of today's CCS safety systems these points are often a strong bottleneck for the traffic flow.	Speed changes on the track create unnecessary capacity loss	APM enables TMS	Traffic flow on the point of speed changes is optimized in advance, dynamically and precise
m. Early capacity improvement by mixed production of ETCS Level 2 and 3 including moving block – #capitalize directly the capacity advantage of new trains that already know their integrity and safe length.	„Pure" ETCS lines: Wait until all trains fit to the line mode.	APM offers TMS	A an old "ETCS L2 train" can already drive near behind a new "ETCS L3 train reporting integrity and reliable length".
n. #Shorter maintenance and construction possessions (blocked tracks) with less impact on the bypassing traffic on other tracks including a high safety standard for trackside workers. The processes around maintenance (with/without blocked tracks) or construction are full of voice communication steps between track workers and signallers. Digitized interaction can shorten these processes much and would allow to execute more maintenance	„Slow voice communication and generic speed reductions.	APM offers TMS	Fast digital interaction and speed reductions fitting to the actual state of a construction site More maintenance safely possible under production

under production without blocking a track. The speed limit impact of construction sites on neighbour tracks could be reduced if the dynamic status of a construction site is digitally known to the APS.			
o. #The A.P.M. shall support TMS with a detailed information how every part of the network can be used (precise topology state)	The „actual CCS configuration of the network“ is today often hard to retrieve	APM offers TMS	All forms of allowed usage of the network can be retrieved by TMS from APS with detailed parameters
p. The APS shall support “rich” degraded modes (production reduced as less as possible the case of system faults).	System faults often lead to a full stop and then “manual” train operations	APM offers TMS	APS allows the use of the still working part of the systems in a safe way
q. #A.P.M. shall allow the installation of new network or train elements in small steps “nearly on the fly”. Rollouts “station by station” or “line by line” are not the most efficient ones. Network wide preparation programs e.g. with single changes of trackside assets that go directly into production would often be the best choice for the early usage of the new technical capacity. Because of the overhead of CCS construction projects that comes with the characteristic of todays CCS systems this choice today is not often possible.	CCS change or replacement projects „line by line”	APM offers TMS	Early/fast/simple use of new single installations by installing “asset by asset”.
r. #Better traffic flow near to construction sites by seamless integration of mobile / temporary CCS assets (e.g. occupation sensors) to optimize the traffic flow in unequipped network areas	Worse traffic flow near construction sites without the right trackside CCS trackside assets	APM offers TMS	Seamless and fast change of the track capacity by using additional temporary / mobile CCS systems

11.1.2 Making real time optimisation smart needs detailed historical CCS data as a learning basis.

An additional future-oriented customer target and feature of A.P.M. shall be to #enable smart TMS optimizers to tune the traffic flow dynamically by using algorithms based and detailed production data recording (speed relation tracing, asset performance, combination of traffic flow influenced by parameters like train types or station capabilities, etc.).

A combination of sophisticated algorithms today can assure the perfect speed mix control parameters in real-time.

11.1.3 Making production visible en detail shortens processes

#A.P.M. shall offer detailed production data to various automation systems. This requirement results from the fact that today's systems create many manual tasks because of not available status or property data (e.g. actual speed or breaking behaviour or exact track occupation position of trains) or missing detailed properties of trackside assets or vehicles and train sets.

Manual human operations are not only expensive and more unsafe, the communication slows down or hinders the production on all sides – they extend maintenance windows, occupations for shunting manoeuvres, or start of missions. Missing detailed information about the traffic flow lead to too generic planning methods that generate unnecessary capacity reserves in the schedule.

The need is to make current behaviour of the system and data automatically available for other entities in the system. This includes the specific braking capabilities of vehicles and train sets consider them in the full phase of scheduling and re-scheduling. An additional advantage is given, if also hidden parameters in the vehicles from today's safety approval can be made visible for trackside and in addition trackside reduces due to standardisation the need of different braking levels for different lines where at the end the vehicle must apply the maximum value leading to unnecessary margins in other lines.

In case of any change is needed for the movement including handling of degraded situations the processes must be shortened and stable with tool-based assistance as much as possible. All manual documentation and exchange beginning from route compatibility check, pre-planning of movement, detailed planning of movement and operational rescheduling must be automated.

11.2 Asset management perspective: Jump to state of the ICT art

#A.P.M. shall introduce the asset management excellence of digital systems. The todays CCS architecture is historically grown and contains because of this a large package of unnecessary legacies. In addition, the main parts of CCS are a complex combination of functions for securing the train run and in additional operational functions for traffic management. Operational needs are mostly fixed implemented by technical solution and only a minor choice of possible implemented configuration e.g. train routes are possible for operational flexible usage.

Cleaning this up means to reduce the amount of needed assets by over 50% and allows the automation of many complex asset life cycle processes.

In the following customer target description, a traditional "Todays CCS" and "APS" are compared:

Today's CCS	A.P.M.
➔ Legacy line side signalling, or ETCS L1 or L2 implementation	➔ Only for ETCS L2/L3 implementation (mixed)
➔ Based on traditional block based interlockings / RBC	➔ Based on the very new abilities of APS (described below) including moving block
➔ Based on **typical traditional electro-technical life cycle strategies**, routines, methods and market structure (build once, use for long, avoid changes)	➔ Mainly **ICT typical live cycle strategies** (modular software/hardware, continuous integration, automate change and keep everything updated)
➔ Traditional handcrafted planning, construction and maintenance of single in-	➔ ICT-typical high automation of change and deployment in shorter cycles. Decouple life cycles for components (strong dependency reduction as the main strategy) or system layers (central sys-

11.2.1 Life cycle cost reduction for the trackside CCS installations

The sum of CCS life cycle cost (design and planning, construction investment, maintenance, operators technological fixed costs, technology driven skill assurance costs, system operations cost, etc.) correlates in first place to the number of physical trackside assets and in second place to the grade of process automation for planning, construction, maintenance, etc.. The pure purchase price of single asset components is normally not a significant cost driver (typically < 20 % of the life cycle cost). But the effort to plan, install, operate and use them is strongly depending on their functional richness (e.g. configuration automation), upwards and cross compatibility (dependencies limit life span), and on non-functional properties like robustness.

This leads to the requirements that describe solutions which #avoid physical trackside assets as much as reasonable possible and increase the grade of automation of CCS asset life cycle processes.

A third cost driver is an indirect effect in the case that an infrastructure is used at its capacity limit. High performance CCS (requirements described in 11.1) can reduce the number of needed tracks and points in general (depending on several factors, like structure of the schedule) or enable an operation not in general given at the capacity limit e.g. for enabling maintenance windows of for additional traffic in peak hours.

11.2.1.1 Reduction of trackside assets more than 50 % (explained later in detail)

Reduced asset category	Strategy for reduction
#No lineside light signals (except for example at network borders)	Cab Signalling ETCS L2/L3 with operation not needing a second signalling layer with light signals
#No shunting signals	No distinction between shunting and train movements in the signalling layer, but only by different risk measures (e.g. different speed), enable enhanced cab Signalling

	ETCS L2/L3 incl. operation in Full Supervision
#Much less trackside train detection systems (reduction of > 80% on long term)	More usage of train with integrity detection and reliable length information
#Much less ETCS balises (factor 5 - 10)	Precise onboard localisation of trains
Less tracks and points in dense traffic nodes in general	Capacity effect of APS described in 11.1 by supporting denser traffic

To achieve these reductions via radio-based ETCS its economic parameters, a reliable return on a safe investment and the application simplicity shall be improved.

11.2.1.2 Reduce the need to change CCS installations

Trigger for trackside CCS changes	Strategy to reduce the number of changes
Complete replanning of CCS configuration because one element (e.g. one point-machine) in station with older CCS installation changes and new safety regulations shall be applied for the full area/CCS installation.	#APS shall be safely assured with the ability to assure dynamically the same necessary safety level for every type of topology or function layout of the track. The function and the topological data needed in APS is separated and not fixed implemented as a bundle in the code. APS will always only allow movements that are safe compared to the situation, functional track layout and necessary safety level – so #every change of track or CCS functions is proven as handled safe by APS in general.
One single CCS component gets obsolescent and all connected components must be replaced because of compatibility or high safety case dependencies	#Strong functional and technical decoupling of components in the architecture and abstracting on different layers with no need to explicitly change all layers in case of any adoption. #Automated integration for changes, functionality and interfaces with automated downwards/upwards-compatibility mechanisms, implementation of a #“modular safety” strategy that isolates as much as possible the homologation of single replaceable components or simplifies and automates the safety integration process.
Technical obsolescence	#Obsolescence shall lead most often to “simple exchange” from the standard interface perspective instead of “change of configuration”.
Capacity optimisation by CCS investments (like investing into more signals or shorter trackside train detection section)	#Capacity shall in terms of CCS only be dominated by the abilities of the trains and the physical track layout. The #A.P.M. shall use modern dynamically scalable computing resources for central functions. The radio and fixed network communication shall be based on technologies with enough capacity reserves (e.g. FRMCS as part of the Railway Mobile Radio (RMR) for radio-based transmission). Trackside train detection systems that create high costs for higher train densities shall be more and more replaced or amended by onboard localisation. In this long-term target the A.P.M. approach allows that CCS systems have no relevant influence on the capacity anymore.
Functional change needed	The change of CCS system functionality is usually caused by these aspects: Simplification of systems

	(cost reduction), better operational support by CCS systems (automation, safety, performance, usability) or integration requirements (e.g. coming with new components). To reduce the amount and size of functional changes the A.P.M. strategy shall implement a very simple and #dynamically scalable architecture, a pure and #harmonized operational concept (e.g. shunting is no special movement any more) and a high grade of #cheap upgradeability.
Improved neighbour components have improved and not backwards compatible interfaces	Even in a perfectly upgradable world of always up to date systems the development life cycles of components will create the situation, that components implement different releases of interface standards. Because of this the compatibility of interface standard releases has a very high importance for the reduction of migration dependencies ("#old compatible with new"). The smaller the steps of migrations can be the low the migration cost. #Strong architectural rules to increase the interface release compatibility (incl. functional compatibility) shall be implemented (interface segregation, lose coupling, minimal standard that always works, etc.).
Safety incident or identified safety gap, or reliability to be increased	Every year an amount of safety relevant functional amendments is done, also in form of additional or changed assets. A.P.M. shall reduce this amount by implementing three strategies: • #Closing the existing gaps in the full supervision by functions and not by operational specific measures (like shunting), • simplify the change of logic functions (#software upgradeability for central and decentral components), • #simple addition of single components under production and the "modular safety" strategy (automated and reduced change impact effort), • #guarantee high reliability by redundant central systems and • reduced number of trackside assets.

11.2.1.3 Reduction of integration effort by upgradeability and dependency reduction

Integration means combining existing components to an application that fulfils a set of requirements for the lowest possible life cycle cost (incl. anticipating the changes in the life cycle). **Architecture**

tries to design the components behaviour (at their interfaces) in a way that makes integration (compatibility) simple even if usage, requirements, or constraints change for some components during time.

The #reduction of integration effort is a major target and every optimization step about this has a high value. This is not influenced by the question, who the integrator is in a single case (customer, supplier, service company), when in the life cycle (from development to divestment) the integration effort takes place or if the reduction can halve the effort versus bringing it completely down to “plug and play”. It is always worthful. With a reduced integration effort potentials are made available:

- Life cycle costs are reduced significantly
- #smaller components have a lower complexity (better to manage, faster to develop)
- #changes can be done for smaller parts of installations (less sunk cost in replacements)
- investments are safer (broader market possible, lower obsolescence risks)
- critical lock-in situations can be avoided for mission critical installations
- #workload can be divided better between more and specialized partners
- innovation speed can be increased (if the standards are flexible enough)

A standard can have a negative impact when it is too static and forms a bad architecture.

Modularisation or compatibility does not happen only because a standard is established for one point in time. Standardisation is a prerequisite, but does not already assure, that all components fit together in the life cycle or migration and that they form a high-quality architecture. Every standard and the standardized components will evolve in development releases over the years (optimization process, adaption because of changed environment, security adaption, changed operational needs etc.), while asset managers try to keep old asset versions as long as possible (reduce cost, reduce risks because of changes).

The result is (for every point in time) a mix of components with different releases using different standard releases. This is an inevitable situation in a digitized landscape. Neither freezing standards for long nor changing assets always all together is an economic solution strategy. Avoiding changes of standards is a worthful but limited ambition since it shall not hinder the optimisation of the CCS system. Also, the fast-increasing amount of security threats will force every CCS system anyway to change often, as well as the interface standards shall evolve for that. In addition due to a better usage of the CCS system operational needs can be derived and implemented in short circles. This is a continuous and never stopping process for evolvement of standards based on new functional needs, safety aspects and security threats.

The first strategy aspect: Upgradeability

One important target is addressed with the term “upgradeability”: Reduce integration effort for example by #impact resolution automation, by smaller component sizes, by #remote and automated deployment and administration and certain interface mechanisms that allow the communication between old and new for a “seamless migration”.

Even complex dependency structures are no problem when the process of handling the #impact of changes is automated or strongly supported by automated toolchains and recognisable by the safety supervision departments of the operator and the authorities as well.

The second strategy aspect: Dependency reduction

The even more important strategy is #dependency reduction between components in general from a functional and safety level point of view.

Independency of solutions, companies and life cycles is a dominant economic factor. It is multiple times more important than for example avoiding redundancy of functionality or data. A complex dependency network between installations can multiply the cost for CCS (repeated sunk cost for early depreciation, high integration cost, incompatible new innovative products on the market, etc.).

In the CCS area the strategies of the ICT sector should be applied (see for example the SOLID, KISS or encapsulation principles), that were learned in the past decades to reduce dependencies between components. This includes for example:

- #Components should retrieve on runtime what service is possible by other components and be flexible to make use of different service offers or to combine them.
- #Components should expose the minimal and necessary information to other components (encapsulation).
- #interface segregation: Interface specifications and standards shall be split into smaller pieces, especially in stable and dynamic parts of the interface.
- #Large platforms shall be avoided as well as central functionalities with large interfaces (except for hardware or runtime environments) because their lifecycle would dominate all other components
- Granularity of interface standardisation (life cycle cost versus integration complexity)
  - The granularity of standardisation (size of standard products) shall evolve over the years in an iteration (big interfaces first, step by step going deeper).
  - The increase of granularity (split up component) in an iteration shall reflect real-world demands of asset managers or integrator companies and the realistic market potential that specialized component companies would be able to really offer
  - The long-term target is to reduce the size of standard components (standardize interfaces inside of exiting components) to the best minimum where the integration cost reduction is higher than the decoupling cost.
- Components should be polymorph which means that they are able to “act in older standard versions” if necessary and “use their new features if possible and allowed by partner components”.
- Standard interfaces should be located at a place in the overall system where it is simpler to avoid dependencies (“#simple splitting point”)

To make the full use of these strategies also in CCS domain some paradigms shall be changed:

- For economic comparisons the full life cycle cost approach for the change and integration cost inside of the life cycle shall be used instead of the calculation of the first pure investment. Major focus must be given also on life cycle costs for safe supervision of the correct behaviour of the system and keeping all authorisation certificates and permissions up to date. In a digital CCS landscape, the costs happen more in the life cycle for operation and maintenance compared to a high amount for first implementation and built for legacy systems.

- The dependency structure inside of the architecture shall allow an automated component change or upgrade every year.

- Major #changes in safety cases shall not be mandatory or necessary when a change of component versions happens. Generic safety compatibility principles shall be applied that allow for example the “use as before” if components have a proven standard backwards compatibility (or a certain behaviour). Generic safety cases shall be used to prove the safety of the combination of interface standards for components of different sources and enabling having a correct safety documentation on a daily base available.

- Safety architectures shall use #hardware abstraction mechanisms (paradigm “device driver”, safety based on availability and reliability of data”) to avoid expectations (dependencies) about the connected hardware.

It is assumed that changes in strategy like this will increase the initial cost and development effort for CCS Systems, but the amortisation will happen fast due to reduction for the operational phase and make a base of documentation usable for different types of installation of different operators.

11.2.1.4 Reduce planning, engineering, and authorisation effort for single CCS installations

Today CCS projects need up to 5 years of manual planning, design, detailed engineering, data preparation and preparation of the safety case. The skill requirements and the complexity are high (especially for ERTMS projects) because of complex optimisation challenges and safety rules. The complexity is coming also from the fact, that a mixed and dynamic traffic flow with continuous behaviour must be predicted and mapped to control systems and sensor/actuator structures, that divide the tracks into specific segments that are controlled by layout-specific decision trees and commands. Improvements are introduced in parallel stepwise and leads in the most case not to a 100 % usable based for authorisation process. A variety of projects runs in parallel needing additional well skilled persons.

These have to be developed and proven to be safe gaining reduction effects from starting on the scratch up to getting the approval for getting into operation.

The target for the A.P.M. shall be to #reduce planning, engineering, and authorisation effort by more than 50 %.

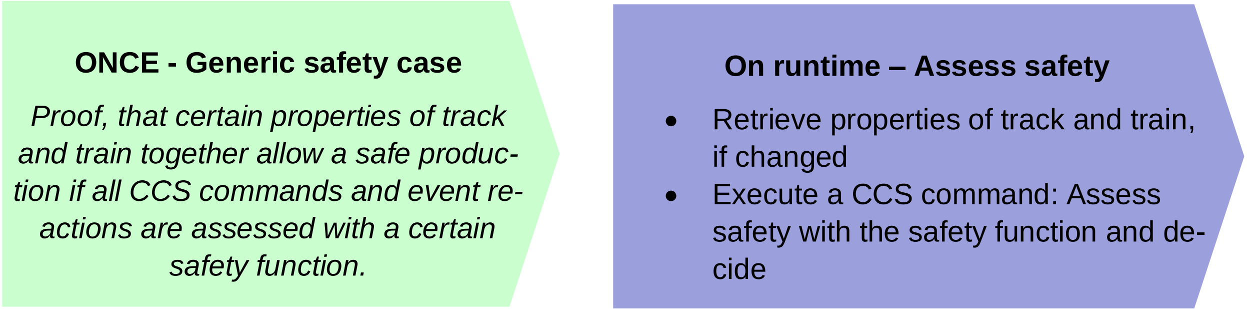
The main strategies are:

- Less engineering because off less trackside assets and because of CCS standardisation based on operational standardisation. Only focus on data preparation covering topological changes using safety processes and toolchain.

- #Safety is assessed and assured mainly on runtime on the basis of a generic safety function for every installation in the same way. No specific safety case per single installation, that assess specific design aspects (like track layout) covering the full installation, is needed.

- #The safety logic of APS shall have a generic approval and authorisation in which it is proven that it just needs a reliable input of topology information and train information (track asset behaviour and states, train behaviour information and states), and will assure safety on this basis.

- The functional combination and suitability of specific trackside assets and train is proven by a standard compliance and limits the need of compatibility check and specific authorisation of vehicle considering the lines to be operated.
- #The safe combination of specific trackside assets or train is assessed and decided on runtime too, as well enabling an automated route compatibility check.
- The optimisation of the track layout is just done because of capacity reasons, not any more for safety reasons and performed simply by topological changes.



ONCE - Generic safety case

Proof, that certain properties of track and train together allow a safe production if all CCS commands and event reactions are assessed with a certain safety function.

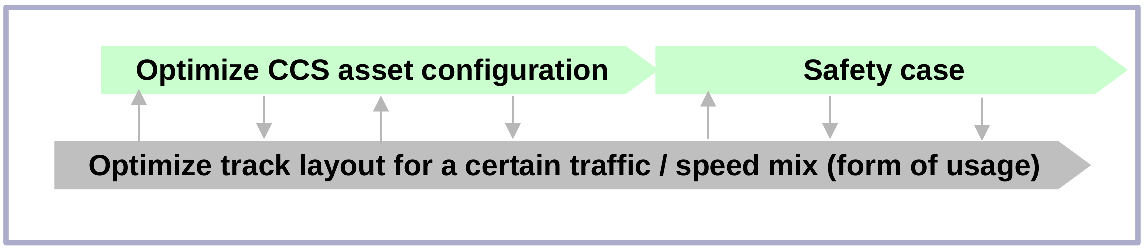
On runtime – Assess safety

- Retrieve properties of track and train, if changed
- Execute a CCS command: Assess safety with the safety function and decide

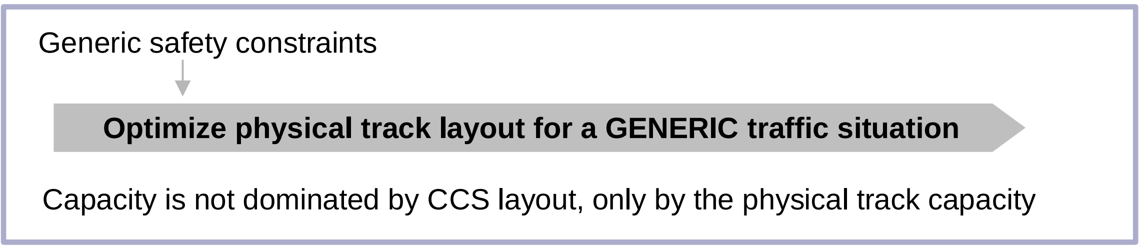
Figure 3: Basic safety strategy - proof safety once.

Comparison of project steps in a specific project:

Today:


Optimize CCS asset configuration
Safety case
Optimize track layout for a certain traffic / speed mix (form of usage)

With A.P.M.:


Generic safety constraints
Optimize physical track layout for a GENERIC traffic situation

Capacity is not dominated by CCS layout, only by the physical track capacity

11.2.1.5 Much less trackside train detection installations

Depending on the traffic density there are 5 to 10 times more trackside train detection installations than trains. Therefore, shifting the function and responsibility of occupation detection (train localisation) in general from track to the train reduces the amount of detection systems by this factor 5 to 10. This shift needn’t happen by 100 % since trackside train detection systems also have some advantages in certain applications (like for stabling areas).

The prerequisite to use (partly) track areas without trackside train detection shall only be, that trains are able to deliver their train integrity and reliable length information together with a safe train position report to APS, when they want to occupy these parts of the track. APS shall be able to assure a safe production based on an active train surveillance instead of passive trackside occupation sensors.

In addition, the change of using less trackside train detection installations and using innovative location systems leads to an operational considering of occupation where needed. Nowadays covering different rules, the train detection systems is placed in example at a point covering the switchable part, including safety signs. This means only if a wider part compared to the only relevant switch blades is cleared, the point can be changed in position. A safe localisation of the train passage can enable an early clearance and change of position of switchable field elements as side effect.

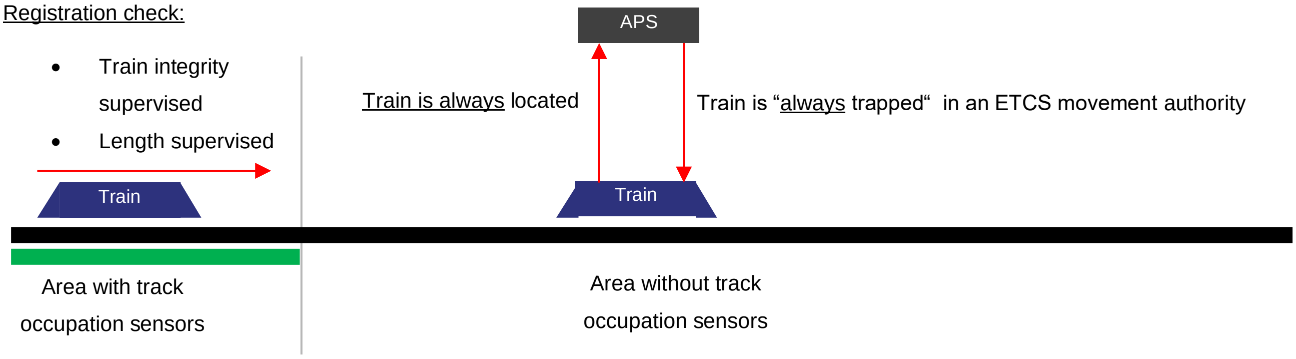

Registration check:
Train integrity supervised
Length supervised
Train
Area with track occupation sensors
APS
Train is always located
Train is "always trapped" in an ETCS movement authority
Train
Area without track occupation sensors

Figure 4: ETCS Level 3 without trackside train detection in a part of the track

11.2.1.6 Freely scalable A.P.M. setup without special configuration work

As described before on the long run the capacity (maximum train density) shall not be limited by the CCS systems and assets, but only by the physical track layout. A.P.M. shall be able to make use of the maximum physical track capacity if the trains offer precise position and integrity information.

11.2.1.7 Automate and simplify the design and change of CCS installations

Today the grade of automation supporting the change of CCS installations is low. The target is to simplify deployment, construction, and maintenance by using IT deployment strategies like continuous integration based on reliable automatic configuration and test procedures.

The A.P.M. configuration work shall be reduced to an automated process that just acquires the topology and its CCS functionality. The topology shall by automatically synchronized between APS and other CCS systems. The design of the layout of still existing trackside CCS assets (like balises) shall be created by an automated and standardized algorithm derived from the physical track layout.

11.2.1.8 Reduce safety case effort

Today every installation needs a single safety case with a deeper analysis (large effort). With APS low safety case cost shall be possible (only configuration compliance validation) because a generic safety case for all installations has proven that APS is assuring safety for any topology if the configuration fulfils certain rules. This generic approach enables in addition a simple supervision of the safety performance and adaption, without deep knowledge of specific safety demonstrations of various safety argumentations within a network. Cost reduction effects refer to the safety organization also.

11.2.1.9 Scalable and cost efficient (mixed) sensor configurations

Depending on the traffic and operational requirements a free mix of onboard and trackside train detection and localisation technologies shall be useable by APS. #APS allows to combine different sensors to get the full occupation and speed information for a train (e.g. flexible and dynamic combination of axle counters and ETCS onboard position reports for train localisation). Point based, section-based or continuous position-related sensors shall be combined by APS. Also, sensors of different precision or reliability shall be combined to get a scalable cost/RAMS (reliability, availability, maintainability, safety) bandwidth for the CCS design. Sensors could be used at its best considering the environmental condition, e.g. tunnel sections, and are not limited to one technology only suitable or assessed for system use.

11.2.1.10 Safe production with the same (or a scalable) safety level on every topology layout

A safety responsible user or a NSA shall be able to rely on the fact, that APS assures a safe track usage as long as the systems configuration, topology data and train data are compliant to the safety relevant application requirements of the generic safety case covering APS.

This shall allow for example to change older stations stepwise even if they do not fulfil typical physical requirements (like flank protection). #A.P.M. shall compensate missing capabilities automatically by for example reducing speeds or avoiding too small distances between trains. This shall also automatically be used in the case of a failure of trackside assets or train capabilities.

11.2.1.11 “Plug one or thousands of assets & rail”

#A.P.M. shall support the replacement of a large set of trackside assets for large areas (e.g. keeping track of the asset test status over months or supporting forward-and-backward switching of lines) in one step as well as #“on the fly” replacements (also for new installations) or maintenance work under production (“asset by asset”). Processual approach is even the same, if only one asset is changed or a big replacement is planned.

11.2.1.12 Reduction of the amount of on-site testing for new CCS installations

A.P.M. shall support the strategy of “#reduced onsite testing” by simulation and “remote test in the loop” capabilities, and especially the fast switching between existing configurations and the test of new configurations within the CCS domain. #By applying a full standard, the pure check between correct deployed on-board and trackside systems must be possible for the first time.

11.2.1.13 Decentralized or centralized system topologies, modern configuration maintenance

A.P.M. shall allow different system layouts from decentralized to highly centralized safe computing with virtualization and container technologies, n-modular redundancy, fast disaster recovery, multi-tenant and multi-company cloud structures etc.

#The software-to-hardware-dependency for central A.P.M. systems shall be reduced to a level to decouple this relation (life cycle) where it is economically reasonable.

11.2.1.14 Seamless integration of track worker safety

#A.P.M. shall support to integrate track worker safety as an efficient automated process seamless into the production CCS process. This means that #track workers shall be automatically detectable (if locatable) and that #communication for track worker access to the track or trackside assets shall be automated.

11.2.2 Safe investments, upwards compatibility, flexibility to allow continuous modular change, optimization, and innovation.

11.2.2.1 Smart interfaces

The interface design of A.P.M. shall implement features that allow an independence of lifecycles and release steps on both sides of the interface (“connect old to new”). The negotiation shall not only compare releases but shall also be able to #compensate (temporarily) missing capabilities of a system by a reduced form of interaction (e.g. minimal necessary system interaction).

This point is especially important for connecting to a #mix of different ETCS baselines and system versions or to different EULYNX baselines.

11.2.2.2 Assure fast and simple upgradeability of the trackside ETCS functions and function versions (maintainability)

A.P.M. shall be upgradeable to newer system versions or to be used functions e.g. of ETCS by an automated process.

11.2.2.3 Decouple component dependencies to allow more component-wise replacements

For the reduction of sunk cost in replacement processes the dependencies between A.P.M. and its environment shall be reduced to an optimal minimum (e.g. by device abstraction).

11.2.3 Support optimised, flexible procurement and continuous supply improvement

Today protection systems are very different in the countries which leads to high fixed costs per country on all sides (Infrastructure managers and industry). The business target and procurement strategy are to standardise and open the international market for trackside protection systems by endorsing specialised companies to offer modular products fitting to standardised interfaces. This scaling reduces unit and integration cost for customers, integrators and suppliers and allows higher development investments per component that supports automation.

This requirement does not imply to shift the integration responsibility to the operator or customer. It just points out to reduce the integration effort per se and to create a broader market of specialized companies that can deliver components.

11.2.4 Close the safety gaps, less costs of safety, more continuous improvement

11.2.4.1 Today the functional size of safe systems is unnecessary large (historical effect). Tomorrow: Reduce size of safe systems. Shift functions to normal IT systems (like TMS), that are not safety relevant.

Since the development and the life cycle cost of safe systems are very high, their #functionality shall be reduced to an absolute minimum of necessary safety functions. The approach shall be to implement #APS only as a "gatekeeper check function for safety" and to #implement all preparation and automation processes in the architecture layers above APS. For example, the preparation of the trackside assets for a movement permission of a train shall be done by the plan execution system whereas APS afterwards just checks if the movement permission is compatible to the track assets status concerning safety.

Today safe systems in the CCS domain are a complex mixture of real safety functions or operational functionality including various adaptions for handling degraded situations. In addition, the functions in one system belong in some cases to functions within the neighbouring system not only from functional purpose but also in kind of risk mitigation.

For simplification a #strong split between functions needed in safety systems and operational functions to be placed in the field of TMS is needed. Thus, not only safety functions can be reduced but also the architecture can be simplified to a certain degree. Architecture can respect specific Railway Safety domain parts with a higher need on Hardware and Software as well all further parts to be intended for usage of standard IT products with specific Software solutions.

Restructuring creates the possibility to get a better overview on the safety functions enabling a quick and sufficient safety argumentation and considering.

11.2.4.2 Safe integration without new detailed safety case or long integration testing

Today safety integration tests create large efforts when changing assets. Tomorrow the exchange of components or connection of new subsystems under production shall happen without large safety case or preparation processes ("plug and rail", "modular safety", automated impact analysis. Like in ETCS: A homologated vehicle can drive everywhere without local integration test).

An efficient safe integration is a fundamental need. Nowadays integration of components and subsystems in the system Rail need too large integration test campaigns. This contradicts the principle of having confidence of the results of former development phases and is mainly based on the following facts:

- unclear and interpretable specification
- gaps in specification
- safety ensured by a high amount of SRACs, operational and integration conditions
- generic fault tree analysis and failure mode effect analysis based on incomplete specification with weakness for demonstration of unrestricted validity in each specific application and less possibility of easy maintaining in case of changes
- various variants of technical solution in field not harmonized and not respecting a single reference architecture for any safety argumentation considering reference systems as a fundamental base of comparison
- unclear and wrongly followed processes of development, engineering and proof

- incomplete supervision by inspection bodies, responsible for system integration and authorities due to the grown complexity

Modular safety based on clear requirements and automated impact analysis in case of changes will decrease the amount of integration tests within the real or test environment significantly. This can be compared with the defined target for ETCS, that a developed vehicle can run after Route Compatibility Check (pure check between infrastructure and vehicle register) on a line fitting automatically.

11.2.4.3 Advanced situation specific safety-pattern recognition

Because of the high cost that safety requirements cause the optimisation of the implementation of safety is key. On the one hand system variety shall be avoided, on the other hand the optimisation compliant to local safety requirements and available sensor information is necessary. Today, patterns of unsafe situations and their national criticality assessment are coded “fix” in the software of safe systems which creates large amount of system diversity. Tomorrow: #Advanced situation specific safety-pattern recognition is used (high safety, but only where it is needed), that is configurable by the users for specific locations or vehicle types by configuration.

.

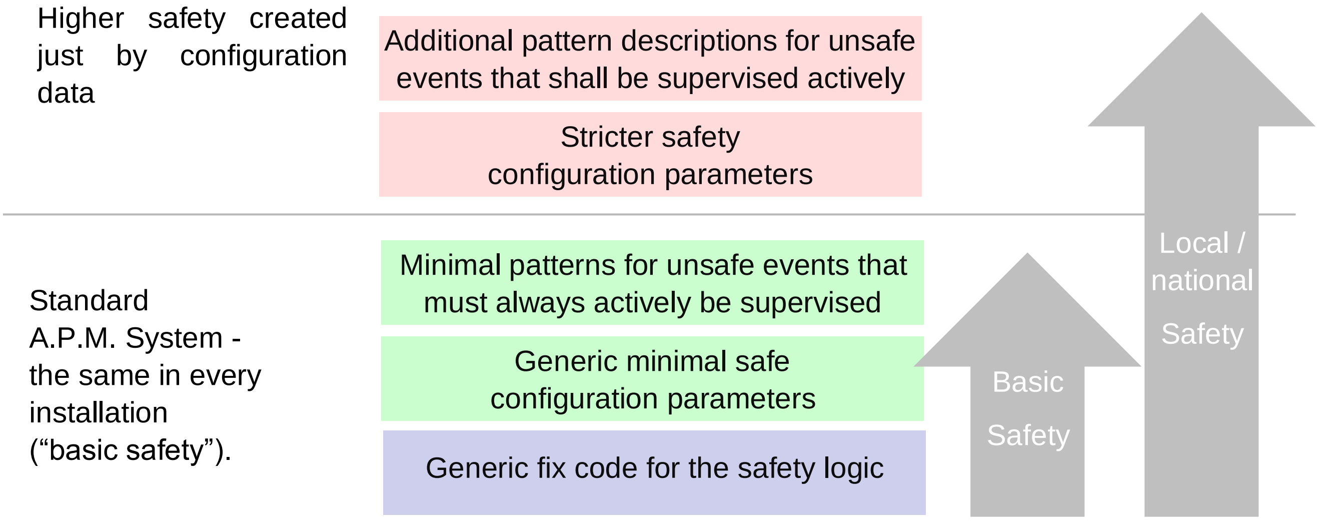

Higher safety created just by configuration data
Additional pattern descriptions for unsafe events that shall be supervised actively
Stricter safety configuration parameters
Local / national Safety
Standard A.P.M. System - the same in every installation (“basic safety”).
Minimal patterns for unsafe events that must always actively be supervised
Generic minimal safe configuration parameters
Generic fix code for the safety logic
Basic Safety

Figure 5: Implementing basic and extended safety as a “stack”

The generic code of APS shall implement a generic pattern recognition system (e.g. event patterns like ‘fault of a point’), that supervises all events coming from train sensors, trackside sensors or any other systems or users (standard APS interface) that are connected. Event message patterns shall be configurable as data including the description of the necessary reaction to the event pattern. The temporary increase (stricter) of safety configuration parameters (e.g. the minimal train distance, the maximum speed for on-sight movements or the length of slipping risk buffers) shall also be a possible reaction to event patterns. Event patterns could also have a pure availability relevance or can be reports from the train like “water on the neighbour track”.

Local safety pattern recognition shall not harm the standardisation of operational processes. To achieve this, three strategies shall be implemented:

1. The standard operational processes shall base on the implementation of the basic safety,

2. Additional local safety constraints (patterns, e.g. not allowed processes) shall always be visible on runtime for all users including early warning (driver, signaller, track worker)
3. If a track user (train, track worker, etc.) cannot fulfil additional safety patterns, A.P.M. must always automatically offer a track usage with “basic safety” and perhaps stricter safety configuration parameters.

11.2.4.4 Support Full Supervision for all type of movements (safety for shunting, manoeuvres)

Operation is mostly divided into two categories:

- Train runs based on train routes with high safety mitigation measures
- Shunting/manoeuvre movements based on simple routes or as free manoeuvres

This leads to less safety in case of shunting is performed and a high amount for securing train runs while keeping the interaction between train runs and shunting in mind.

Shunting is in the most cases assured by manual processes and the major risk lowering fact is handle the situation with reduced speed. Often voice communication in this process creates unwanted efforts and processes duration times.

While also in automated operation train fitting and simple change of tracks must be assisted, the optimization of shunting from an operational and safety point of view is one of the main targets. Shunting shall be performed not different compared to train runs. This means a high grade of supervision – like the Full Supervision Mode in ETCS – must be enabled and usable for shunting movements. Only specific configuration like less braking capability shall be reflected by adopted speed profiles for ensuring the same level of safety.

As a result, #any movements shall be performed on the highest level of supervision and only risk mitigation measures shall be taken into account for securing the movement itself and further movements based on the capabilities of the train set.

11.2.5 High reliability, less faults

11.2.5.1 Reduced number of assets, cheaper redundancies

The reduction of assets, the (possible) centralization and high redundancy of control systems shall improve the reliability and availability of APS just because of the quantitative effect of having less points of failure.

11.2.5.2 Support rich degraded modes, detailed degraded status, automatic incident management and fast dynamic recovery to normal production

APS shall implement “rich” degraded modes which means, that a minimal production is still possible even when system failures occur. The dynamic risk calculation, the adaptive speed reduction and the sensor aggregation (or logical compensation of missing sensor information) are possible strategies for this requirement.

Modern fast recovery technologies (e.g. by virtualisation) and optionally high redundancy shall support short recovery durations.

11.2.6 Efficient long-term maintainability by reduced complexity for customers

11.2.6.1 Offer efficient and automated functionality for maintenance processes (on the track) to interact with the CCS process

#Requests of any (by TMS) authorized system or person to change or reserve track elements shall be possible in an automated way (via TMS to A.P.M). #A.P.M shall provide reliable information about the production status around persons on the track for their local safety systems and #PE&APS shall support warning functions for track workers.

11.2.6.2 Offer integrated diagnostic features for CCS for fast root cause analysis and remote maintenance

A.P.M shall support automated root causes analysis for system faults, automated field-force and maintenance management (ticketing), integrated diagnostic systems for large CCS configurations, service-flow oriented diagnostic user interfaces and automated analysis of larger historical diagnostic data.

Annex: List of requirement key phrases

Business TargetsFälle