IRSE///
Institution of Railway Signal Engineers

The location and control of assets in smartrail4.0

Steffen Schmidt
SBB, Switzerland

This, the fourth paper in the 2018/9 Presidential Programme, was presented in Zurich on 26 October.

The programme smartrail4.0, which is driven by the Swiss railway sector, has the goal of making railway operation significantly cheaper and more efficient by means of modern technologies.

The targets of smartrail4.0

All so-called "CCS game changers" (cab signalling with moving block, safe mobile localisation, high end radio, automatic rescheduling, automatic train operation, etc.) are combined in a modern, lean and open standardisable architecture.

smartrail4.0 is an open concept whose specifications are released for open use in the product market or in self-developed products after completion (see www.smartrail40.ch). Basic available technologies from different industry sectors are combined to develop requirements and concepts for new high-performance products and to develop innovative vendors in the marketplace.

The main aspects of the business case for smartrail4.0

smartrail 4.0 will feature full digitisation with fewer trackside assets with possibly only switches and crossings left. The architecture will be simple, but powerful with a reduced amount of safety critical functions. Higher capacity will be delivered by a high performance and precise train control and dynamic optimisation, which blocks only the necessary minimum of track for each train movement.

Automation of the CCS (control command and signalling) asset lifecycle processes, especially data preparation and safety cases, will be a key feature, along with automation of scheduling and production planning. Higher grades of automation for both existing operation centres and train operation will contribute to less energy consumption. Modular CCS vehicle architecture with high upgradeability will result in lower life cycle and safety cost, along with increased safety by using a generic and redundant protection architecture. Cheaper and faster migration will also be possible with minimised loss of CCS investment capital.

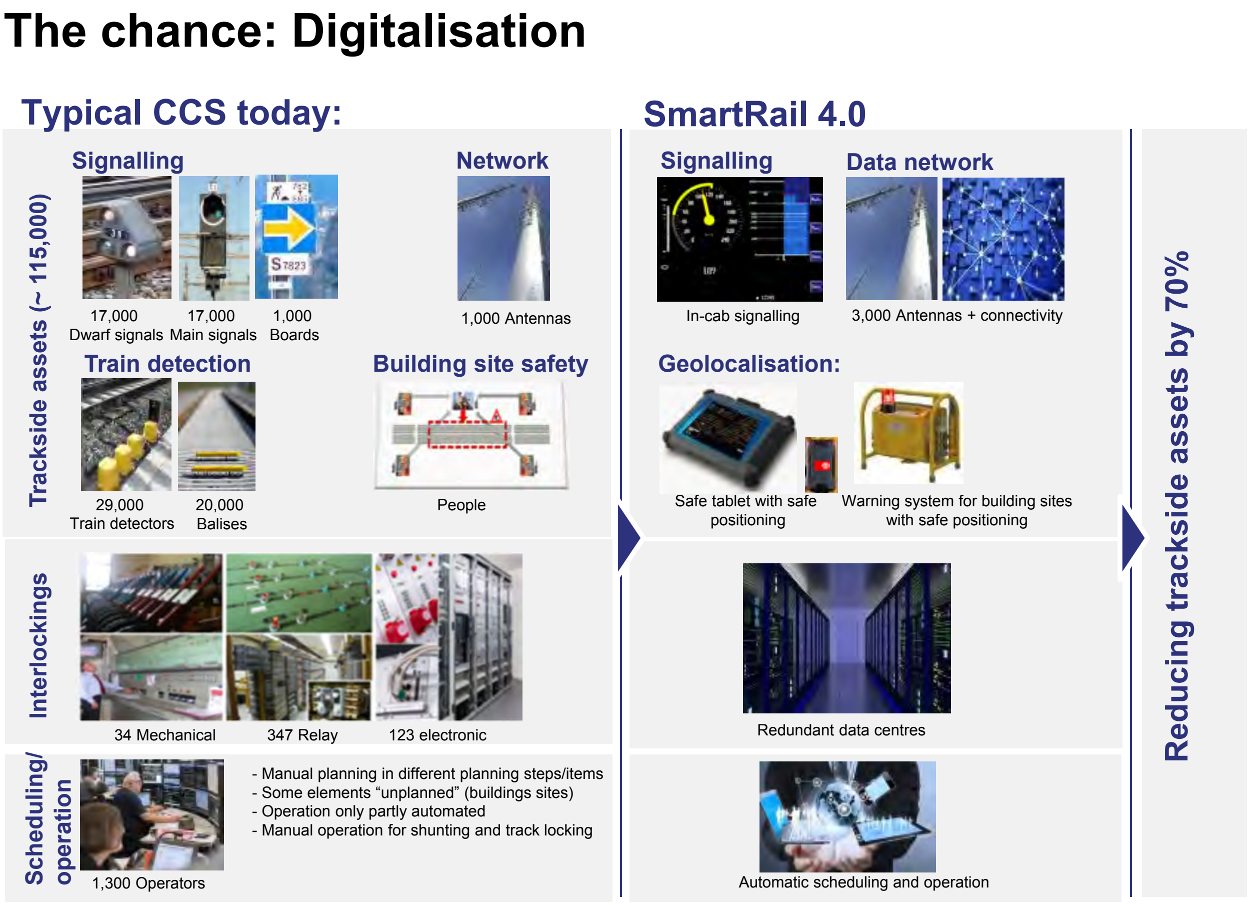
If all 30 projects of smartrail4.0 succeed, the operating cost reduction will have a volume of several hundred million euros every year. All the so called "CCS game changers" will combine to achieve these goals. There are two key elements of the concept. Firstly the methods, architectures and technologies for the localisation of trains on the track together with the function, logic and secondly the flexibility of the trackside safety system. This controls the safety of all types of movements and changes of the state of the trackside assets, such as switches. These are discussed in the article.

A lean but powerful CCS architecture

There are many dependencies between the "CCS game changers" that make it hard and expensive to install them one after the other. But installing them all in one step leads to a very lean and at the same time very powerful architecture. It could be used for high speed lines, for main line or for metro.

The three main layers in this basic architecture, shown in Figure 2, are:

1. The TMS (Traffic Management System) centralises all business logics as a real time optimisation system including automatic rescheduling and adaptive control of the traffic flow. It steers the underlying processes with geometric precision. It changes the switch positions or chooses between options to solve a conflict situation (for example lower speeds without flank protection or higher speeds and longer overlaps).
2. The APS (Advanced Protection System) is a "gatekeeper" that checks the safety of TMS commands going to the trains and to trackside assets. APS has a very small amount of generic safety critical check functions, everything else is done in the TMS. Its hardware abstraction layer allows the combination of different types of mobile or fixed train detection systems or train integrity monitoring systems.
3. The bottom layer, the physical world, is simplified and digitised by the means of modern communication and localisation technologies. Here the innovations are happening today. Having precise positions with high and safe reliability gives the ability to digitise every trackside signal and sign, and puts this information on the screen in a train. This can reduce the amount of trackside assets up to 70%, which is a really good business case.



The chance: Digitalisation

Typical CCS today:

Trackside assets (~ 115,000)

Signalling

17,000 Dwarf signals

17,000 Main signals

1,000 Boards

Network

1,000 Antennas

Train detection

29,000 Train detectors

20,000 Balises

Building site safety

People

Interlockings

34 Mechanical

347 Relay

123 electronic

Scheduling/ operation

1,300 Operators

- Manual planning in different planning steps/items
- Some elements “unplanned” (buildings sites)
- Operation only partly automated
- Manual operation for shunting and track locking

SmartRail 4.0

Signalling

In-cab signalling

Data network

3,000 Antennas + connectivity

Geolocalisation:

Safe tablet with safe positioning

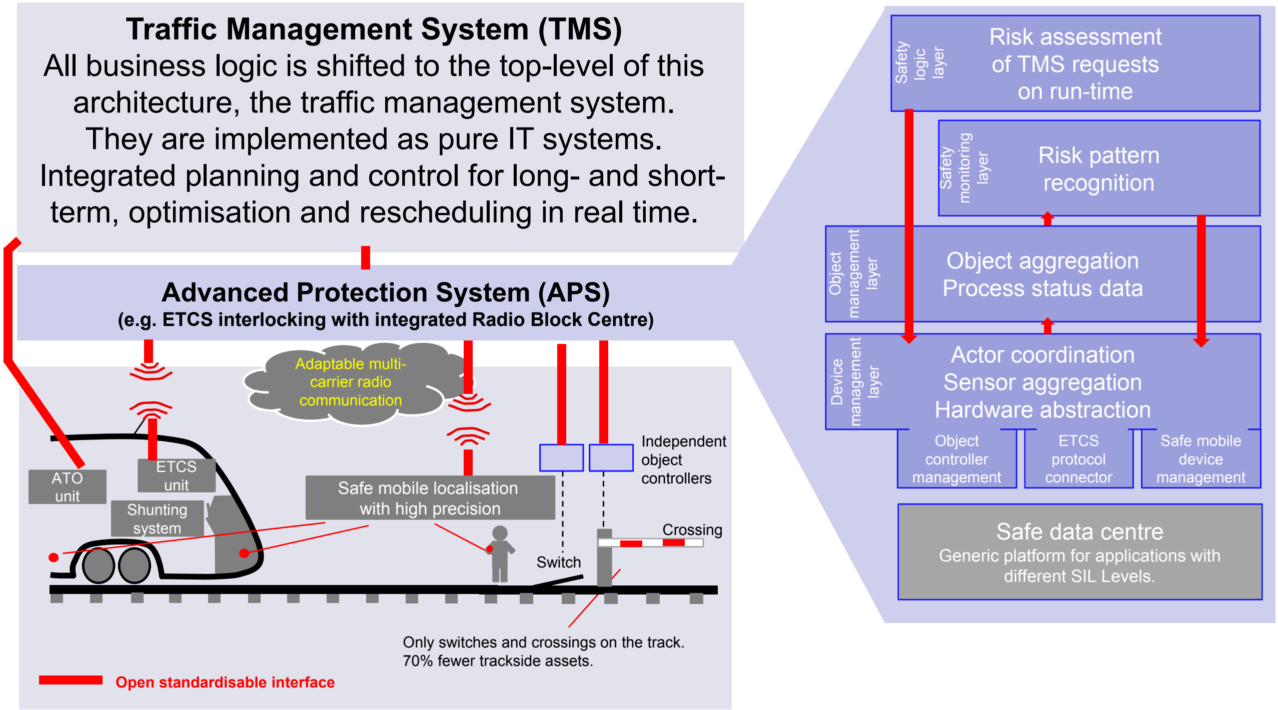
Warning system for building sites with safe positioning

Redundant data centres

Automatic scheduling and operation

Reducing trackside assets by 70%

Figure 1 – The opportunity: digitalisation.



Traffic Management System (TMS)

All business logic is shifted to the top-level of this architecture, the traffic management system. They are implemented as pure IT systems. Integrated planning and control for long- and short-term, optimisation and rescheduling in real time.

Advanced Protection System (APS)

(e.g. ETCS interlocking with integrated Radio Block Centre)

Adaptable multi-carrier radio communication
ATO unit
ETCS unit
Shunting system
Safe mobile localisation with high precision
Independent object controllers
Switch
Crossing

Only switches and crossings on the track. 70% fewer trackside assets.

Open standardisable interface

Safety logic layer
Risk assessment of TMS requests on run-time
Safety monitoring layer
Risk pattern recognition
Object management layer
Object aggregation Process status data
Device management layer
Actor coordination Sensor aggregation Hardware abstraction
Object controller management
ETCS protocol connector
Safe mobile device management

Safe data centre

Generic platform for applications with different SIL Levels.

Figure 2 – The three layers of the basic architecture.

Advanced Protection System

Interlocking and Radio Block Centre in one function and system

In order to avoid major system and configuration redundancies, distributed safety algorithms with complex system states and unused fine-tuning options for the ETCS cab signalling, interlocking and RBC are combined functionally. In the integrated APS safety logic routes from interlockings and movement authorities from ETCS RBCs merge to one "movement permission", for which trackside assets are locked and which are sent to the trains to control their movements. As a result, there is only one safety system – the APS (similar to an 'ETCS Interlocking') – which manages only geometrically defined movement permissions, checks them before passing them on to the train and locks the associated tracks.

Lean generic SIL 4 level and risk assessment at run-time

The relocation of all non-safety-relevant functions to the higher-level TMS creates a generic and operational process-independent architecture level with SIL 4 requirements. The APS primarily executes a generic check function for requests from the TMS, e.g. an extension of a movement authority or the change of a point machine status. If TMS requests lead to a safe subsequent status, they will be accepted. Even the preparation of a route is in the TMS (leading to requests for changes of switch position via APS), only the test of the suitability of a track for a movement authority (MA) remains functionally in the APS.

Part of the generic track layout and process independent test algorithm is the geometrically evaluated isolation of the movement authorities and danger zones or the parameterised testing of generically considered risk distances – an overlap length is only one special case of a risk distance. The generic risk assessment of risk distances at run-time is based on a pairwise assessment of two topologically adjacent risk objects (trains, localisable obstacles, restricted areas, locatable persons, etc.) and their safety-determining parameters (geometric distance, speed, object type, gradient, protective elements in the track, etc.).

The generic safety case for the APS will need some more work for the proof that a generic risk assessment on run-time is complete and correct, but the idea behind this assessment function is simple. When geometric train positions and geometric topology data is correct at run-time, the function can simply calculate the safety of a change triggered by a TMS request, e.g. new movement authority or changing a switch. This is shown in Figure 3.

A run-time generic risk-checking function of this kind makes it possible to safely use any given track topology – even very old and unfavourably constructed layouts. The change of old topologies is no longer required for reasons of safety, but only for capacity sizing. This eliminates a major investment risk.

The parameters of the risk function could be changed more easily and can also take into account additional information like weather, track status, train defects or train type to go into "safer modes".

The basic state flow of APS has the form shown in Figure 4.

Other safety rules like not exceeding speeds or checking the safe status of a trackside asset stay of course unchanged in the safety logic, like they exist in an interlocking of today.

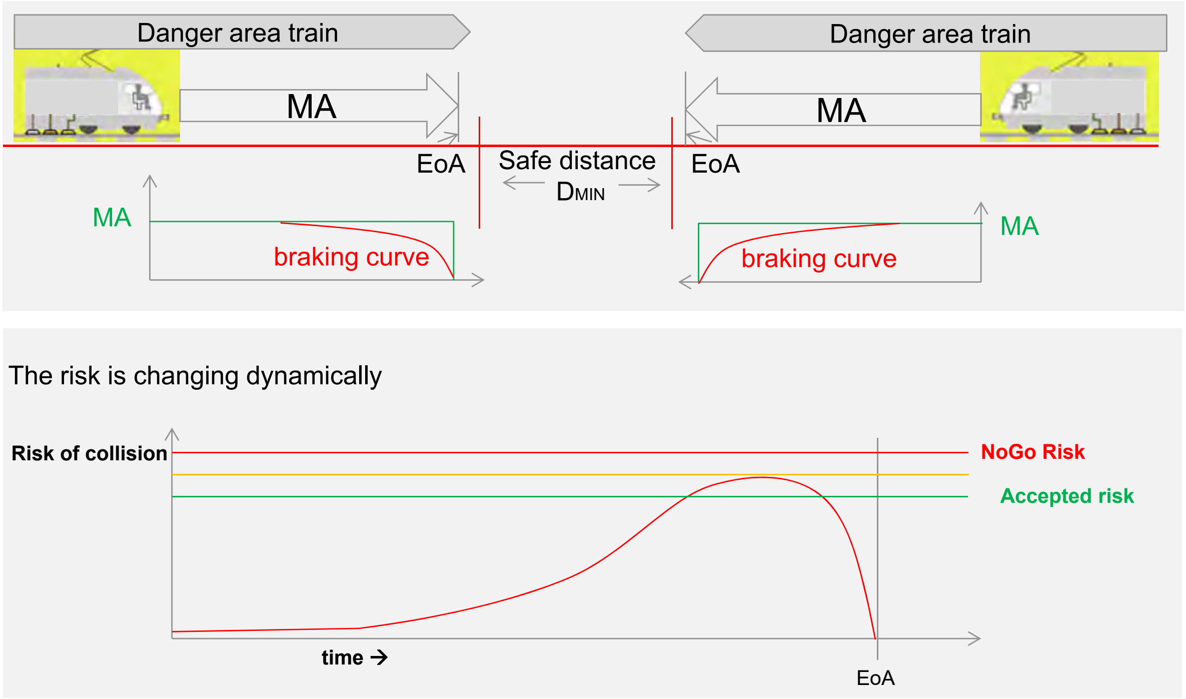
Geometric interlockings will be easy to plan and install

The generically applicable risk assessment at run-time has yet another significant effect – if the APS is approved as a generic application, no costly project planning of the safety and no comprehensive safety case for the behaviour of the single plant is required for the replacement or modification of the interlocking. If the topology has been precisely recorded and the system has been technically tested, the system can be safely used. This reduces the configuration effort and significantly shortens the lead times for interlocking projects.

Flexible combination of localisation technologies

A geometric safety logic has also another important advantage: it is upwards compatible to nearly every train detection system of the future because it can map every sensor information to a geometric

Figure 3 – Example of the APS in use. Two trains approaching each other, 'geometric' interlocking carrying out risk assessment at run-time.



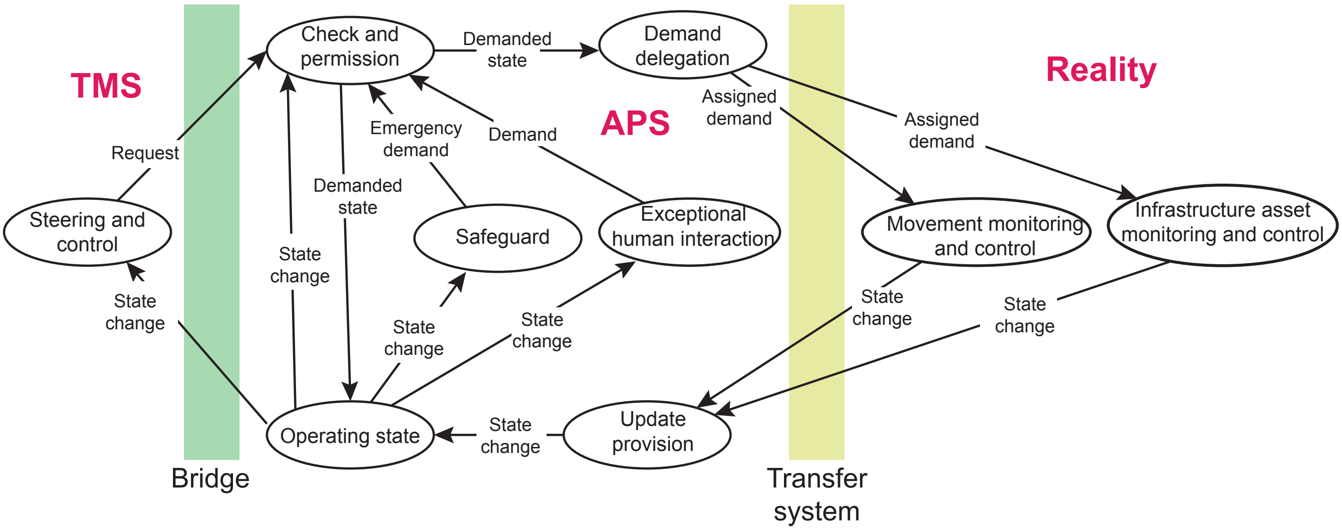


Figure 4 –The basic state flow of APS.

representation. Today's interlockings normally do not have this feature.

Traditional interlockings can simulate this flexibility by using virtual block, but this generates quite a lot of data preparation and configuration work. It is very important to be flexible for mixed migration scenarios with trains, that have different abilities, on the same line. Flexibility means safe investments and low migration cost.

Considering the future, it may happen that we stop numbering ETCS levels. For a communication based train protection architecture there exists a number of possible combinations of trackside and onboard localisation technologies – too many to give them a specific number like "Level 2" or "Level 3". The prices of high quality inertial measurement units (the primary localisation system in military applications) are coming down and there are algorithms for a sensor fusion with odometry, GNSS (satellite navigation), RTLS (real time localisation systems) or video localisation. Fibre optic sensing is a start. 5G may assist as an additional sensor channel. Even innovations like LGPR (localisation by ground penetrating radar) may surprise us in the future. The results of the feasibility studies in smartrail4.0 for a precise virtual balise with a reliability that is high enough for a SIL 4 application are very positive.

The important point is that the business case coming with a safe and precise mobile localisation system is really large (reduction of trackside assets). It makes sense to invest. Safe localisation is the basis of the big digitisation step of the railway operation process, as it is necessary in many applications. But analysing the decision processes in product companies shows another picture up to now: there is a paradigm, that a virtual balise or mobile localisation system should not cost more than the odometry of today. This is a mistake that blocks a big business case.

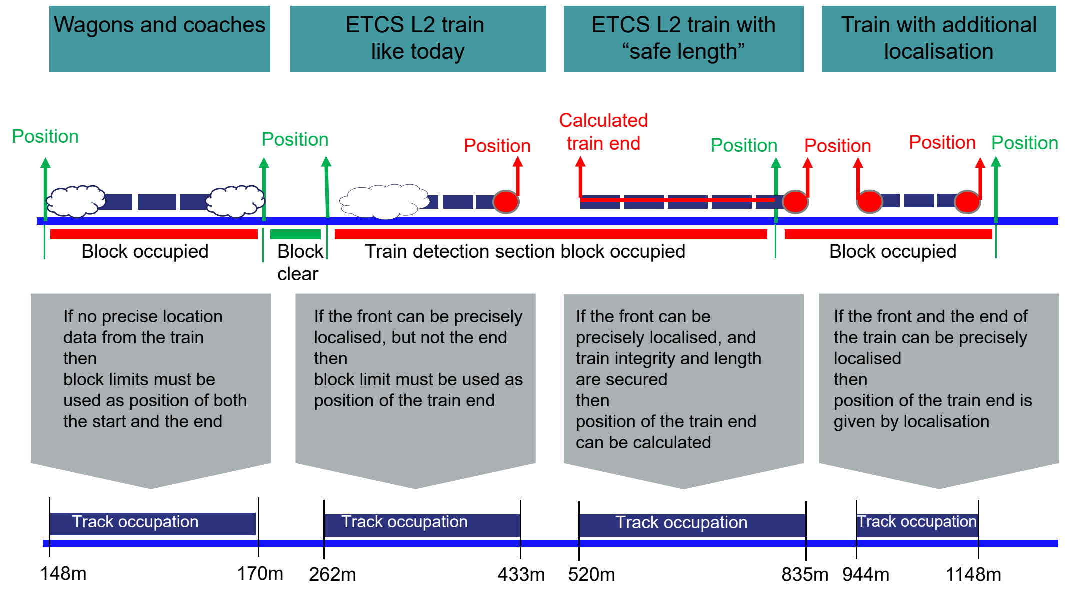
The fear that moving block is a completely new operational process triggering a really big change normally calms down when the operational analyst checks the real differences. It is normally just no more than a higher resolution of the train detection system, just a change of technology creating higher precision. While the block today is 'jumping' in big steps, it will still jump tomorrow in smaller steps determined by the time between repeated radio messages. For the safety logic it is not relevant if the localisation (full track occupancy) information comes from the train or from the trackside. Even the degraded modes are not so different as one may think, as the hazard analysis shows. The loss of communication to an ETCS Level 3 train and to an axle counter have a lot of similarities. It is an advantage if the operational processes for different combinations of localisation systems are not different as this allows an easy migration.

The "virtual track occupation" (real occupation + precision reserves) of a train is the result of the quality of the actual available localisation devices. When this mix of sensors changes the virtual track occupation may change instantly in both directions. A modern safety logic that can handle this new requirement needs algorithms for new types of localisation transitions. There are algorithms to achieve this, but a geometric safety logic is a prerequisite for them.

Only one 'production brain': TMS

The advantage of the shift of functions to the Traffic Management System (TMS) is not only that the software scope of the expensive safety systems can be reduced to approx. 20-30%. The main advantage is that operational processes only have to be mapped in the TMS, since the generic safety check function of the APS works in the same way on every topology and in every operating process and process state. The APS can therefore be used in any country and on any topology with the same functionality. The mathematical parameters of the generic risk assessment function are configurable so that different levels of security can be set for different types of traffic or regulatory requirements. Thus, the APS can be used both at high traffic densities as well as cost-effective for secondary lines. Only the amount and type of trackside assets or the quality of the vehicle equipment decides on what traffic densities are possible – the interlocking is always the same. With centralisation of the interlockings into safe data centres, the parameters of the risk assessment function can be changed simultaneously for an entire network, or can be set specifically for certain train categories.

As a pure IT system, the TMS can now carry out detailed, optimised fine-tuning of the traffic flow, like precise industrial measurement and control systems do. It can opt for either higher speeds with full flank protection or alternatively for less flank protection and lower speeds. Depending on the current conflict situation it may now opt for short movement authorities and slightly reduced speeds (better total capacity in the conflict zone), or equip individual trains with longer



If no precise location data from the train then block limits must be used as position of both the start and the end

If the front can be precisely localised, but not the end then block limit must be used as position of the train end

If the front can be precisely localised, and train integrity and length are secured then position of the train end can be calculated

If the front and the end of the train can be precisely localised then position of the train end is given by localisation

Figure 5 – Track occupancy can be determined by different sources depending on the equipment fitted to a train.

movement authorities and higher speeds (prioritisation). Simulations show that this precise adaptive fine-tuning can greatly increase the performance of a station and greatly reduce the capacity-damaging effect of speed changes. Short train ahead times with ETCS cab signalling, accurate automated driving and precise localisation are all part of the solution – but without an interlocking functionality that can take full advantage of them, their effectiveness is very limited.

Features of the system architecture

Hardware abstraction, investment protection and upward compatibility

More than 80% of the invested capital of the CCS investments lies in the trackside assets. For the protection and optimum use of this investment capital, an interlocking must have several specific characteristics that are not customary today in traditional interlockings.

The first important optimisation is the introduction of hardware abstraction. As in any modern operating system, specific properties of "end devices" (here trains or interlocking systems) may not be processed in the central application control (safety logic) or anchored in specific hardware. They must be abstractly and generically described and processed. Otherwise, a change in the safety logic and a new complete safety certificate must be made with every change of the trackside technology.

Therefore, the safety logic has to be separated from the end devices by a hardware abstraction layer (HAL). The safety logic only knows the necessary functions and status of the systems. Above the HAL in the safety logic it is only important to know whether and how an trackside asset is currently passable as a topology element and not whether it is a railroad crossing or a point machine and how it is technically equipped. Only their abstract functions and status need to be known.

Another key role of the new HAL is sensor aggregation and automated actuator coordination. Sensor aggregation means track occupancy that can be determined by many different sources of information – depending on the equipment of a track section or a train. Actuators are for example, driver interfaces at the trackside or onboard concerning a movement authority for a train. Puristic approaches such as ETCS levels, which numbered only some of the possible hardware constellations, do not represent an optimal solution and are unnecessary. More economical and easier to migrate is the constantly evolving mix of different sensor types, with which the interlocking must deal. In stabling or shunting areas, circuits or axle counters may last longer, but on the line they will become more and more obsolete due to self-locating trains. Behind one train which can precisely locate itself geometrically (e.g. via ETCS Level 3), another train can closely follow, even if other trains are still localised by axle counters (Figure 5). Pure configurations lead to expensive migrations.

An important functionality for a cost-effective migration to ETCS cab signalling is the ability of the new object controller to connect a single trackside asset simultaneously to the old and the new interlocking. The switchover is remotely controllable and enables the industrial preparation of large network segments including commissioning in one step, without incurring high costs for numerous temporary interfaces or necessitating a costly complete set of indoor and outdoor installations.

The APS as a prerequisite for asset reduction and cost optimisation

Trackside signals are eliminated by ETCS cab signalling. However, a favourable migration through specific interlocking technologies must be made possible, which allows the conversion in large segments, a favourable project planning and the reuse of the existing trackside assets. Shunting signals may also be eliminated by cab signalling. This requires an interlocking that can integrate mobile cab signalling systems and alternative localisation systems into the security process.

Today's train detection systems and the growing number of fixed location balises are eliminated by self-locating trains, i.e. by providing secure mobile localisation of the train's geometric track occupancy including integrity status. This requires a new interlocking logic that can handle geometric occupancy information and the various degraded modes of upcoming mobile localisation technologies in all combinations.

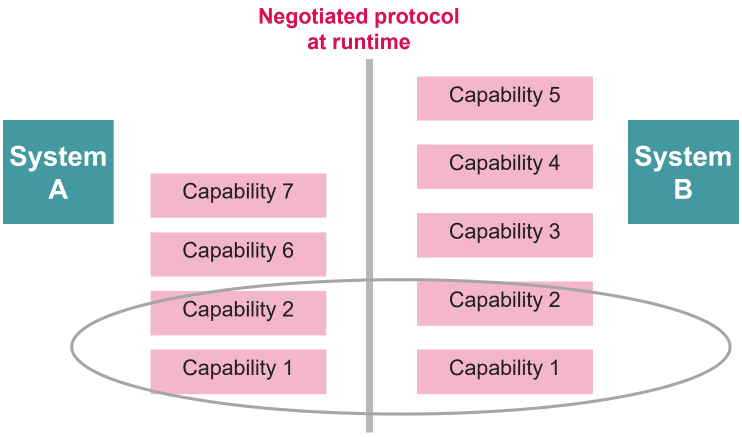


Figure 6 – Achieving high interface quality requires upwards and downwards compatibility via context sensitive protocols for each of the 50 to 100 important onboard and trackside interfaces of a CCS system.

Rule based pattern matching eliminates software releases and specific products

It is also a very important requirement to reduce the cost of safe software development and its releases. This goal can be reached by using formal methods and checker on run-time. It is an old discipline in computer or mathematical science to proof single rules and to combine them to higher rules. Safety cases for safe software are expensive when they must be repeated for every change. There are some ways to automate the software impact analysis, but this is not a requirement that is easy to achieve. Another important method lies in the "rule based systems". A basic system is developed with a generic safety case. Specific behaviours are implemented afterwards as certifiable rules, proofed at run-time with the formal methods that were part of the generic safety case.

Rule based customisation of safe systems by users at run-time sounds like a nice dream. But from a mathematical point of view a formal proof at run-time is possible and there are already existing products that are coming very near to this feature.

Of course, the harmonisation of railway processes would be the best idea. But this is not easy to achieve. The railway sector is not even able to use the same language in operations, which is a small and simple part of the problem. It is not only a problem of habits. There will always be other differences because not every railway can afford to reach the same safety target, can eliminate its national laws, can automate the same function or has the same ability to change, integrate or digitise. Operational processes are stored in the logic of thousands of interlockings today and are part of their safety cases. So the harmonisation will take a while and systems should be flexible to handle many different types of processes. To avoid small customer specific systems that will always have a reduced quality and low grade of automation, it is important to increase flexibility and to improve customisation features without triggering new safety cases.

'Open safety'

For the sanity of the digitalised railway sector it is highly important to copy the change of principles of the IT sector to handle new expensive and complex dynamic systems. Otherwise the life cycle cost will follow an exponential curve. One of the most important methods is to split the whole CCS architecture into independent components and to get rid of complex integration safety cases. There are technological fields in some countries, where they are not affordable anymore which leads to a complete stagnation – which was not really the idea of digitisation.

The idea of 'open safety' is to reduce the complexity of an interface so far that the behaviour of a certified system at its interface can be validated at run-time (plug & play) using the formal methods that were derived from a generic safety case for the integration.

Capability based protocols for interfaces

Writing down the specification of a protocol and committing it as a standard does not always mean that it will live for a long time. Protocols have very different qualities. One of the most important qualities is the release structure of a protocol and its negotiation features.

Protocols that are only released as full baselines often have bigger problems with upwards and downwards compatibility. Flexible high quality interfaces like USB or Bluetooth are structured in profiles or capabilities, that allow an intelligent negotiation of the cooperation of two systems at run-time (Figure 6).

Actual status and conclusion

Various studies, second opinions and proof of concepts for smartrail4.0 are currently being prepared, and will be complete by the end of 2019 in parallel with the first specifications and tender preparations for prototypes, products or development cooperation. The results so far confirm the feasibility, so that the programme team assumes today that the concept can be realised with the described advantages.

The railway system needs a big economic optimisation to assure its competitiveness in the coming years. Small evolutionary technological steps may be too small this time, since it will take again a long time to deploy them. The development manpower in the CCS sector should focus on the bigger economic steps described in this article. Products that are implementing such ideas may be disruptive, but this does not mean that they are not possible.

The smartrail4.0 programme will proceed to prepare this disruptive step and to encourage innovative industry companies to start a cooperative development.

About the author ...

Steffen Schmidt has worked as a technology, automation and process re-engineering consultant in the media, military and logistics sector. He joined SBB in 2001 and was member of the executive board of SBB infrastructure between 2004 and 2010. Since 2011 he focusses on specialised rapid innovation projects, especially since 2015 on the design of smartrail4.0, where he is the lead architect and responsible for the department that develops the next generation CCS.