Das „ETCS-Stellwerk“

The “ETCS Interlocking”

Steffen Schmidt | David Grabowski

Das Branchenprogramm smartrail 4.0 hat das Ziel, die Bahnproduktion mittels moderner Technologien deutlich kostengünstiger und leistungsstärker zu gestalten. Hierzu werden alle sogenannten „game changer“ (ETCS Führerstandsignalisierung, sichere mobile Lokalisierung, FRMCS, automatic rescheduling, ATO etc.) in einer modernen, schlanken und offenen Architektur kombiniert. smartrail 4.0 ist eine offene Konzeption, deren Konzepte und Spezifikationen nach der Fertigstellung zur offenen Verwendung im Produktmarkt oder in Eigenentwicklungen freigegeben werden (Publikationen siehe www.smartrail40.ch). Dazu werden heute verfügbare Basistechnologien branchenübergreifend kombiniert, um die Entwicklung neuer leistungsstarker Produkte und innovativer Anbieter im Markt zu fördern. Das „ETCS Stellwerk“ ist eines der sechs Programme des Schweizer Branchenprogramms smartrail 4.0. Es strebt eine vollständig neue Stellwerkgeneration an, mit der eine Reduktion der streckenseitigen Außenanlagen um bis zu 70 %, eine starke Zentralisierung der Innenanlagen und eine Halbierung des Projektierungsaufwandes angestrebt wird. Entsprechend groß ist der damit zu erreichende Effekt in der Kostenreduktion, die je nach Ausgangslage ebenfalls bis zu 70 % des Jahresbudgets für die Bereitstellung der Leit- und Sicherungsanlagen ausmachen kann.

1 Ausgangslage

Auch wenn man von verschiedenen Prognosen zur zukünftigen Wettbewerbssituationen der Bahn ausgeht – es besteht bei keiner davon der Zweifel, dass ein dringender Handlungsbedarf zur Kostensenkung für das Bahnsystem besteht. Im Umfeld der Leit- und Sicherungstechnik (CCS trackside) und des CCS-Anteils in der Fahrzeugausrüstung (CCS onboard) ist aber in den letzten 20 Jahren ein signifikantes Kostenwachstum zu verzeichnen. Die Digitalisierung brachte kürzere Lebenszyklen und häufigere Anlageneingriffe mit sich. Die digitale Vernetzung verschärft die proprietäre Kompatibilitätsfrage zwischen allen Komponenten, die den Beschaffungsmarkt weiter einschränkte, und sie erzeugte häufigere Auslöser für das Lebensende vernetzter Technologien und Systeme. Die stark forcierte Akademisierung der Sicherheit der letzten 20 Jahre erzeugte umfangreiche Prüfungsdienstleistungen, Nachweispflichten und Projektoverheads, neben denen der eigentliche technologische Entwicklungs- und Planungsaufwand für ein Projekt heute nur noch eine untergeordnete Rolle in der Kostenkalkulation einnimmt.
Insgesamt wächst das funktionale Anforderungsgerüst für die CCS-Architektur jedes Jahr und gleichzeitig steigt damit die Komponentenmenge und ihr Vernetzungsgrad. Für ERTMS, das aufgrund Europäischer Standards zur kontinentalen Pflichtbeschaffung geworden ist, steigen aufgrund der hohen Nachfrage die Projektkosten immer weiter an. Erschwerend kommt hinzu, dass weder der Automatisierungsgrad der verfügbaren Produkte (Lebenszyklusprozesse) noch die Bauweise eine effiziente Einführung neuer ERTMS-Komponenten ausreichend unterstützen.

The smartrail 4.0 industry program aims to make railway production significantly cheaper and more efficient through the use of modern technology. To this end, all the so-called “game changers” (ETCS cab signalling, safe mobile localisation, FRMCS, automatic rescheduling, ATO, etc.) have been combined in a modern, lean and open architecture. smartrail 4.0 is an open concept whose specifications are released for open use in the product market or in self-developed products upon completion (see www.smartrail40.ch for the publications). The basic technologies available today have been combined across the industry’s sectors to help develop new high-performance products and innovative vendors in the marketplace. The “ETCS interlocking” is one of the six programs in the Swiss smartrail 4.0 industry program. It aims to achieve a completely new generation of interlocking systems, which will enable a reduction of trackside assets by up to 70 %, a high degree of centralisation of the indoor facilities and a halving of the development costs. The resulting cost reduction is correspondingly high in that this can also account for up to 70 % of the annual budget for the provision of control and safety systems depending on the initial situation.

1 The initial situation

Even if one assumes different forecasts for the railway’s future competitive situations, there is no doubt that there is an urgent need to reduce costs in the railway system. However, significant cost growth has been recorded in the field of command and control systems for infrastructure (CCS trackside) and the CCS share of the vehicle equipment (CCS onboard) over the last 20 years. Digitisation has resulted in shorter lifecycles and more frequent intervention in the equipment. Digital networking has compounded the proprietary compatibility issue between all the components and this has further constrained the procurement market and created more frequent triggers for the end-of-life of networked technology and systems. The strongly enforced academisation of safety in the last 20 years has produced extensive audit services, obligations to provide proof and project overheads, while the actual technological development and planning costs for a project now only play a subordinate role in the cost calculation.
All in all, the functional requirement framework for the CCS architecture is growing every year, while the numbers of components and the degree to which they are networked are also increasing at the same time. The project costs are constantly rising for ERTMS, which has become a continental obligation as a result of European standards, due to high demand. To make matters worse, neither the degree of automation (lifecycle processes) nor the design of the available products adequately support the efficient introduction of new ERTMS components.

ETCS ist im Kern nur eine standardisierte „Sprache" zwischen Systemen und macht ansonsten keine Vorgaben zu den Systemen selbst. Der hohe Aufwand (Life Cycle Cost) der ETCS-Implementierungen ist nicht auf die „Sprache" ETCS zurückzuführen, sondern hauptsächlich auf den geringen Reifegrad der ersten noch wenig automatisierten Produkte (Lebenszyklusprozesse) und auf die „gepatchten" Altarchitekturen, in die sie heute integriert werden. Mit einer vorgegebenen rein ETCS basierten Gesamtarchitektur würde sich die Situation deutlich verbessern.

2 Business Case

Letztlich benötigt die optimale Steuerung der Bahnproduktion streckenseitig hauptsächlich nur noch Bahnübergänge und Weichensteuerungen. Alle anderen streckenseitigen Anlagen sind mit heute verfügbaren Technologien „digitalisierbar" und werden nach der Digitalisierung nur noch sehr selten auf der Strecke benötigt. Das Eintauschen von bis zu 70 % der festen streckenseitigen Anlagen (in den SBB heute 115 000) durch mobile Anlagen in wenigen tausend Zügen ist ein belegbarer wirtschaftlicher Quantensprung, dem basistechnologisch heute nichts mehr im Wege steht (Bild 1). Die Produkte, die dafür die verfügbaren Basistechnologien zielgerichtet einsetzen, sind allerdings noch nicht in voller Reife verfügbar. Die Entwicklung dieser Produkte muss zielgerichtet und aktiv gefördert werden. Durch den Einsatz solcher Produkte könnte der jährliche Aufwand für die streckenseitigen Sicherungsanlagen je nach Ausgangslage um bis zu 70 % reduziert werden, während die notwendige Erweiterung der Fahrzeugausrüstungen für Neufahrzeuge bei richtig gewählter Architektur (Upgradeability, Offenheit, Standardisierung, inkrementelle Nachweisstrategie) und Beschaffungsmethodik vergleichsweise geringe Kostensteigerungen mit sich bringen. Muss eine Bahn jährliche Ausgaben von mehreren hundert Mio EUR für Erneuerung, Unterhalt und Ausbau von Sicherungsanlagen (CCS scope trackside / onboard) aufbringen, so wird klar, wie groß das Amortisationspotenzial für solche Entwicklungen ist.

The ETCS is essentially only a standardised "language" between systems and it places no specification requirements on the systems themselves. The high cost (life cycle cost) of ETCS implementations is not due to the ETCS "language", but is mainly due to the low degree of maturity in the initial insufficiently automated products (lifecycle processes) and the "patched" legacy architectures into which they have been integrated today. The situation would improve significantly with a prescribed purely ETCS-based architecture.

2 The business case

Ultimately, the optimal control of railway production on the trackside mainly only requires level crossings and point controllers. All other trackside systems are "digitisable" with technologies which are available today and are rarely needed on the line after digitisation. The replacement of up to 70 % of the fixed trackside assets (currently 115 000 at the SBB) with mobile systems in a few thousand trains is a verifiable economic quantum leap which is no longer blocked by the basic technology (fig. 1). However, the products which target the available base technologies are not yet fully mature. The development of these products must be targeted and actively promoted. The use of such products could reduce the annual outlay for trackside safety systems by up to 70 % depending on the initial situation, while the necessary expansion of vehicle equipment for new vehicles with a correctly selected architecture (upgradeability, openness, standardisation, an incremental homologation strategy) and procurement methodology requires comparatively low cost increases. If a railway operator has to spend several hundred million euros annually on the renewal, maintenance and expansion of safety systems (CCS scope trackside / onboard), the amortisation potential for such developments soon becomes apparent.

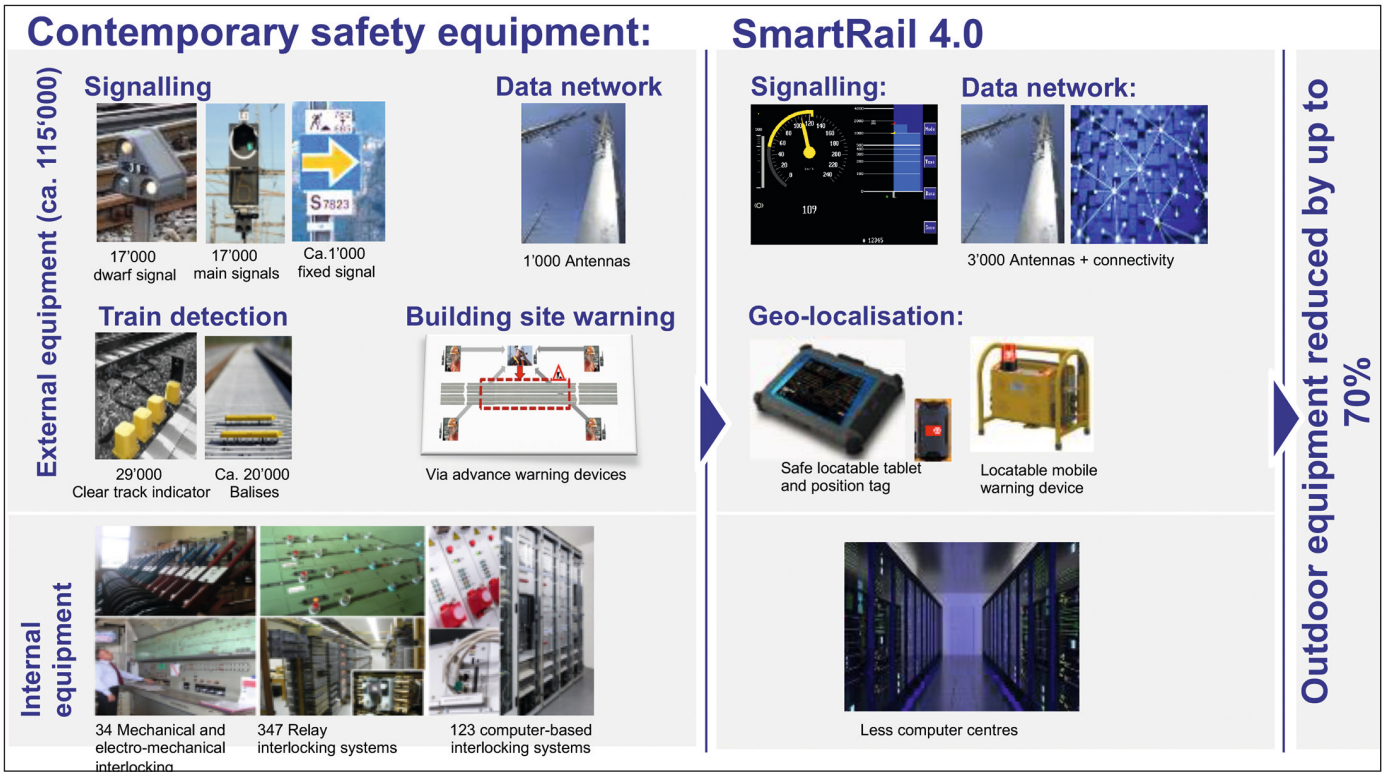


Bild 1: Die Digitalisierung der Command and Control Systeme führt zu einer starken Reduktion der Mengengerüste.
Fig. 1: The digitization of the command and control systems leads to a high reduction of the amount of assets.

3 Die Bedeutung von Stellwerk und Radio Block Center in der CCS-Gesamtarchitektur

Das Stellwerk (zusammen mit dem Radio Block Center, RBC) sitzt in der Mitte der CCS-Architektur und kann damit als das Betriebssystem der Automatisierungspyramide der Produktion angesehen werden. Es entscheidet darüber, welche „end devices" der Automatisierungspyramide (Infrastruktur und Zug; darin jeweils Sensoren und Aktoren) angeschlossen und kombiniert werden können und bestimmt damit den Freiheitsgrad für den mit Abstand größten Kostenblock des CCS-Beschaffungsportfolios. Es liefert das aktuelle Betriebsabbild an übergeordnete Traffic-Management-Systeme (TMS), je nach Bauweise in unterschiedlicher Qualität und Genauigkeit. Es dominiert damit die Voraussetzungen der Automatisierbarkeit der Produktion.
Seine Sicherheitsalgorithmen entscheiden darüber, wie effizient die „end devices" der Produktion ausgenutzt werden. Seine Flexibilität ist ein maßgeblicher Kostentreiber für die gesamte CCS-Architektur: Dieses betrifft z. B. offene Schnittstellen, die Hardwareabstraktion für eine leistungsstarke Aufwärtskompatibilität und für den flexiblen gemischten Einsatz verschiedenster Marktprodukte, die Erreichung eines bereinigten und minimierten Funktionsumfangs auf „SIL 4-Niveau", die Parametrierbarkeit für unterschiedliche Anwendungsfälle, die Modularisierbarkeit der Zulassung von Komponenten (Vermeidung von wiederholten Komplettprüfungen) oder die funktionale Unabhängigkeit der Sicherheitsalgorithmen von Betriebsprozessen und Anlagen-Layouts.
Entsprechend dieser Zusammenhänge wurden im Branchenprogramm smartrail 4.0 die Anforderungen an die Konzeption eines ETCS-Stellwerkes gewählt. Details zu der Konzeption des ETCS-Stellwerkes sind im Publikationsverzeichnis auf www.smartrail40.ch verfügbar.
In den folgenden Abschnitten werden einige der wichtigsten Architekturanforderungen des ETCS-Stellwerks vorgestellt.

4 Schlanke Architektur, ausgerichtet auf reine ETCS-Führerstandsignalisierung (Bild 2)

Mit dieser Prämisse für die neue Architektur entsteht sofort eine starke Vereinfachung, denn sie bringt drei große funktionale Unterschiede mit sich: Züge werden nun direkt, kontinuierlich und online gesteuert und nicht mehr nur zeitlich punktuell, auf komplexe Weise indirekt über die Infrastruktur (Signale). Sicherheit kann nun über eine generische Funktion bewertet werden – im Wesentlichen über Abstand und Geschwindigkeit – und erfor-

3 The importance of the interlocking and the radio block centre in the CCS architecture

The interlocking sits in the middle of the CCS architecture (together with the radio block centre, RBC) and can therefore be regarded as the "operating system" for the automation pyramid of railway production. It decides which "end devices" in the automation pyramid (the infrastructure and the train, including sensors and actuators) can be connected and combined and therefore determines the degree of freedom for the largest cost block in the CCS procurement portfolio. It delivers an up-to-date operating image to the superordinate traffic management systems (TMS) at varying levels of quality and accuracy depending on the design. It therefore dominates the prerequisites for the automation of production.
Its safety algorithms decide how efficiently the "end devices" of the production are used. Its flexibility is a significant cost driver for the entire CCS architecture: this involves, for example, open interfaces, hardware abstraction for powerful upward compatibility and for the flexible mixed use of various market products, the achievement of an adjusted and minimised functionality at the "SIL 4 level", the ability to parameterise the equipment for different applications, the modularisation of the approval of the components (the avoidance of repeated comprehensive testing) or the functional independence of the safety algorithms of the operating processes and track layouts.
The requirements for the design of an ETCS interlocking were selected in the smartrail 4.0 program in line with these relationships. Details on the design of the ETCS interlocking are available in the publication directory at www.smartrail40.ch.
The following sections introduce some of the key architectural requirements for the ETCS interlocking.

4 Slim architecture focused on pure ETCS cab signalling (fig. 2)

This premise for the new architecture immediately creates a significant simplification, because it brings three major functional differences with it: trains are now controlled directly, continuously and online and not only from the point of view of their punctuality, but in a complex way indirectly through the infrastructure (signals). Safety can now be evaluated using a generic function - essentially distance and speed - and does not require a complex track-layout or process-dependent case distinctions or hundreds of individually programmed additional

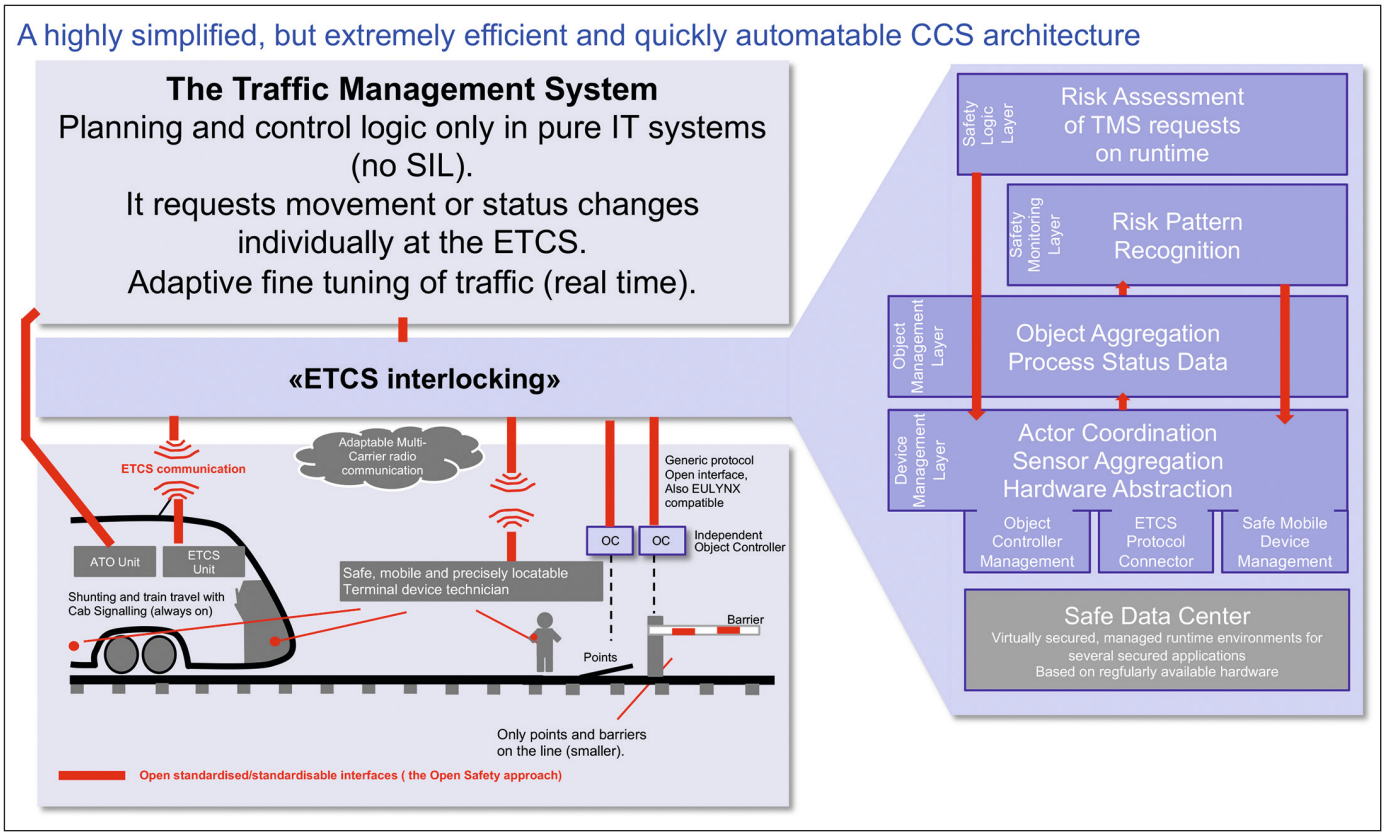


Bild 2: Die Architektur basiert auf einer rein auf die Führerstandsignalisierung ausgerichteten generischen Sicherheitslogik.
Fig. 2: The architecture is based on a safety logic purely designed for cab signaling.

dert keine komplexen anlagen- oder prozessabhängigen Fallunterscheidungen oder hunderte von einzeln programmierten Zusatzfunktionen mehr. Auch der komplexeste Teil der Funktionalität der Sicherungsanlagen, der Umgang mit Störungen (degraded modes), kann ebenfalls deutlich vereinfacht werden. Man kann in einer optimierten „always-online"-Architektur mit geeigneter Redundanz und Verfügbarkeit dem Hauptproblem und Hauptrisiko der Bahnproduktion sehr gut begegnen: fehlende Informationen, insbesondere in der Störungssituation.

5 Zusammenfassung von Stellwerk und RBC

Zur Vermeidung von größeren System- und Projektierungsredundanzen, von verteilten Sicherheitsalgorithmen mit komplexen Systemstati und von ungenutzten Feinsteuerungsmöglichkeiten der ETC-Führerstandsignalisierung werden Stellwerk und RBC funktional zusammengefasst. Die heute übliche komplexe Dualität der Verwaltung von „Fahrstraßen" (Stellwerk) und „Movement Authorities" (RBC) wird beseitigt. Im Endergebnis gibt es nur noch ein Sicherheitssystem „ETCS-Stellwerk", das nur noch geometrisch definierte Movement Authorities verwaltet und vor ihrer Weitergabe an den Zug entsprechend prüft und die damit verbundenen Fahrwege verschließt.

6 „Schlanke generische SIL 4-Ebene" und eine „Risikoprüfung zur Laufzeit" (Bild 3)

Durch die Verlagerung aller nicht sicherheitsrelevanten Funktionen in das übergeordnete TMS entsteht eine generische und betriebsprozessunabhängige Architekturebene mit „SIL 4"-Anforderungen. Das Stellwerk führt primär nur noch eine generische Prüffunktion für Anfragen des TMS aus, die z. B. eine Verlän-

functions for special cases. Even the most complex part of the functionality of the safety systems, the handling of faults (degraded modes), can also be significantly simplified. The main problem and main risk of railway production, i. e. a lack of information, especially in the event of a fault, can be met very well in an optimised "always-online" architecture with suitable redundancy and availability.

5 The interlocking and RBC in one function and system

The interlocking and RBC are functionally combined in order to avoid major system and configuration redundancies and distributed safety algorithms with complex system states and unused fine-tuning options for the ETCS cab signalling. The currently complex duality of the management of "routes" (the interlocking) and "movement authorities" (RBC) will thereby be eliminated. As a result, there is only one "ETCS Interlocking" safety system, which manages the geometrically defined movement authorities, checks them before passing them on to the train and locks the associated tracks.

6 The "lean generic SIL 4 level" and a "risk assessment at runtime" (fig. 3)

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 interlocking primarily only carries out a generic check function for the requests of the TMS, i. e. it may include an extension of a movement authority (MA) or a change in a point machine status. If the TMS requests lead to a subsequent safe

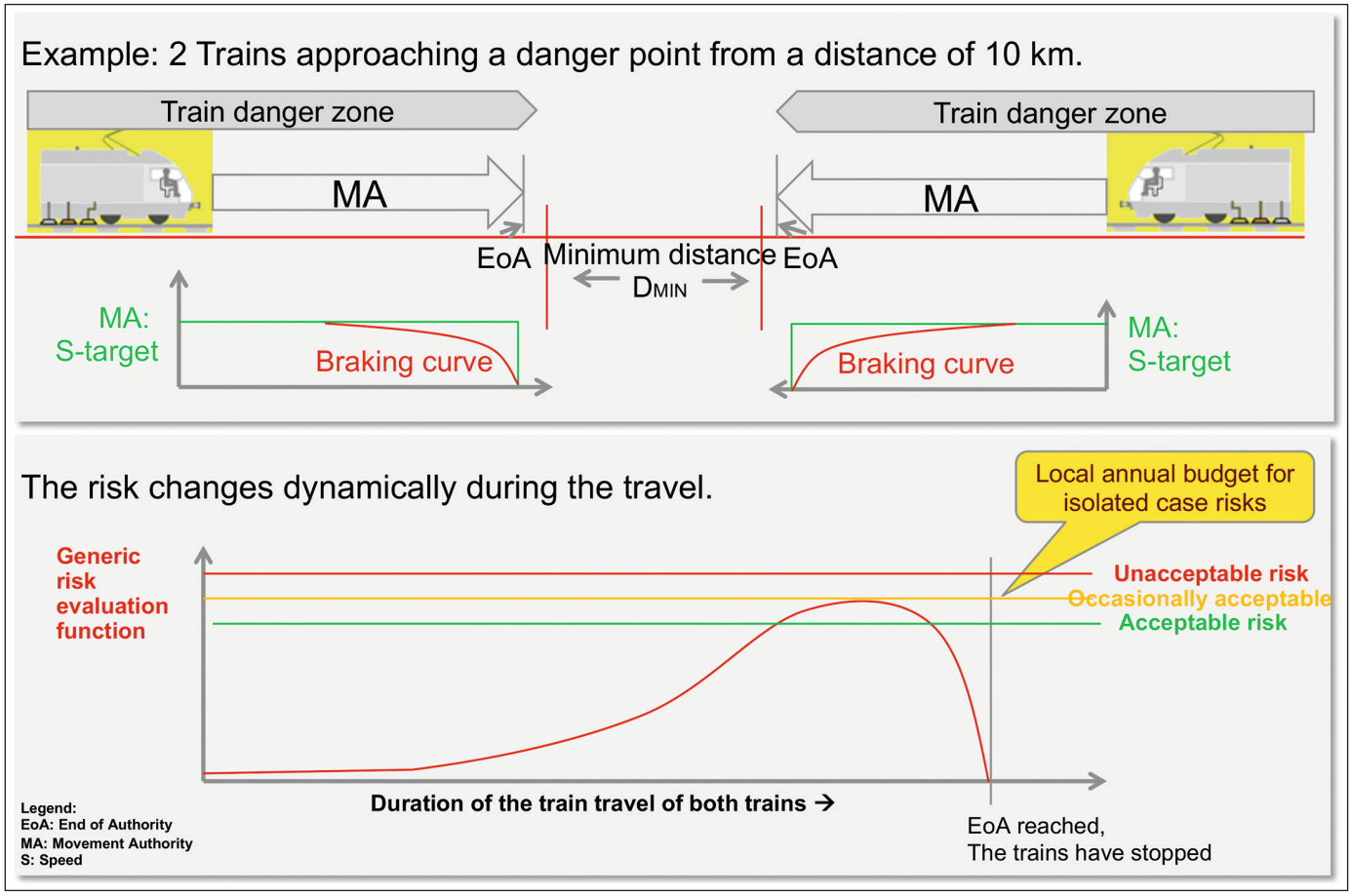


Bild 3: Bei einer Anfrage des TMS (z.B. veränderte MA) wird deren Sicherheit durch eine generische Risikobewertungsfunktion bestimmt.
Fig. 3: The safety of a TMS request (e.g. changed MA) is calculated on the basis of a generic riskfunction.

gerung einer Movement Authority (MA) oder das Stellen einer Weiche beinhalten können. Führen Anfragen des TMS zu einem sicheren Folgezustand, so werden sie zugelassen. Auch die Vorbereitung eines Fahrweges erfolgt im TMS (führt dazu Anfragen via ETCS-Stellwerk aus), nur die Prüfung der Eignung eines Fahrweges für eine MA verbleibt funktional im ETCS-Stellwerk.
Teil des generischen anlagen- und prozessunabhängigen Prüfalgorithmus ist die geometrische bewertete Isolation der MA und Gefahrenzonen oder die parametrisierbare Prüfung von generisch betrachteten Risikoabständen – ein Durchrutschweg ist hier-

status, they will be admitted. Even the preparation of the track is undertaken in the TMS (it executes requests via the ETCS interlocking to this end) so that only the track suitability test for a MA remains functionally within the ETCS interlocking.
Part of the generic track layout and process-independent test algorithm includes the geometrically evaluated isolation of the MA and the danger zones or the parameterizable testing of generically considered risk distances; a slip-over distance is only one special case for a risk distance. The generic risk assessment of the risk distances at runtime is based on

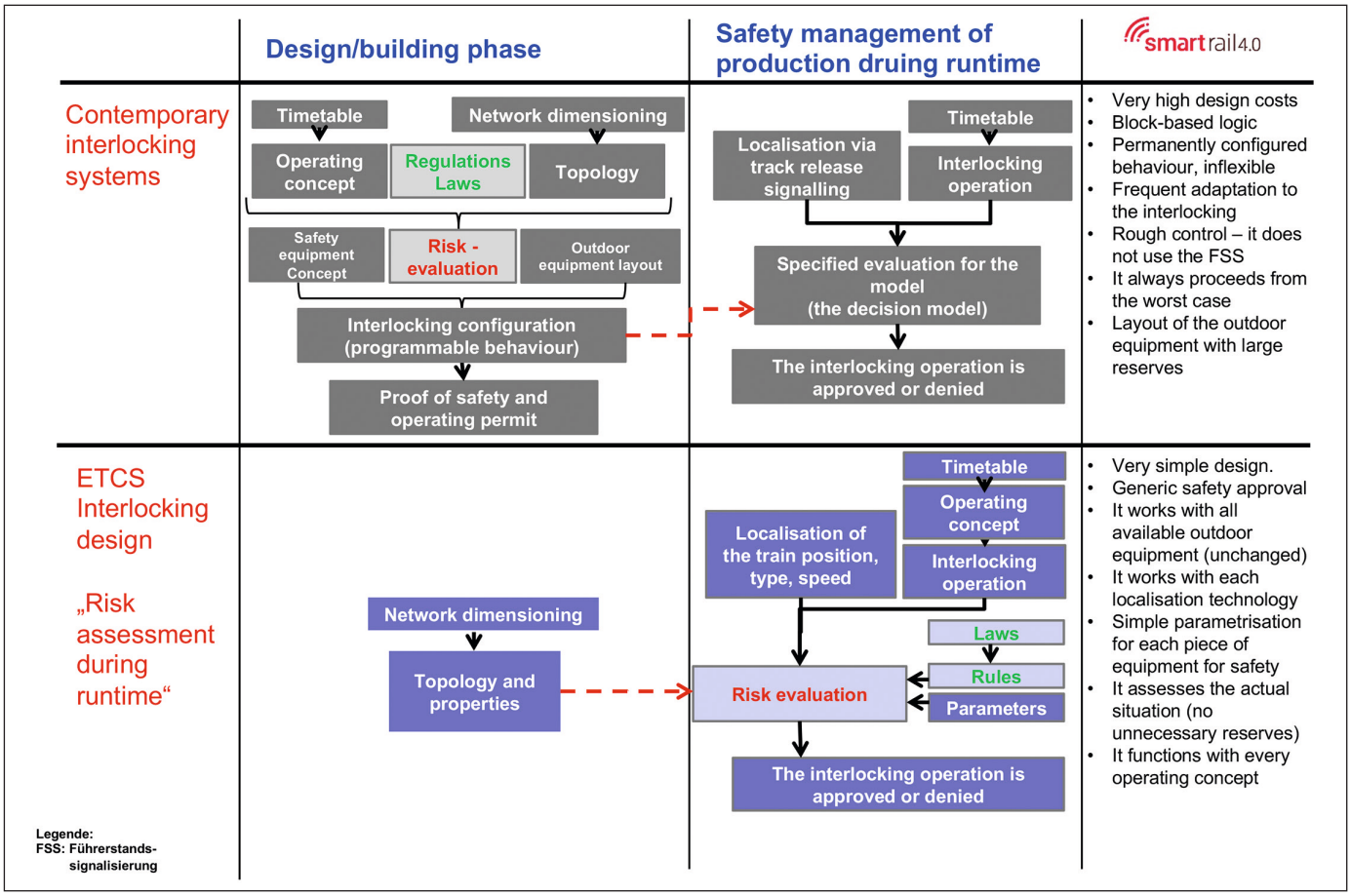


Bild 4: Eine „Risikobewertung zur Laufzeit" eröffnet die Chance, die Projektierungsprozesse stark zu vereinfachen.
Fig. 4: "Risk calculation on runtime" offers the chance to simplify the engineering processes.

bei nur ein Spezialfall eines Risikoabstandes. Die generische Risikobewertung von Risikoabständen zur Laufzeit basiert auf einer paarweisen Bewertung von zwei topologisch direkt über einen befahrbaren Pfad benachbarte Risikoobjekte (Züge, lokalisierbare Hindernisse, gesperrte Bereiche, lokalisierbare Personen etc.) und ihren sicherheitsbestimmenden Parametern (geometrischer Abstand, Geschwindigkeit, Objekttyp, Gefälle, Schutzelemente im Fahrweg etc.).

Eine zur Laufzeit erfolgende generische Risikoprüfungsfunktion dieser Art erlaubt es, jede beliebige Gleistopologie gleich sicher zu nutzen – auch sehr alte und unvorteilhaft gebaute Anlagen. Die Änderung von alten Topologien muss nicht mehr aus Gründen der Sicherheit erfolgen, sondern nur noch für die Dimensionierung der Kapazität. Damit fällt ein großer Investitionsauslöser weg.

Die generisch anwendbare Risikoprüfung zur Laufzeit hat noch einen weiteren bedeutenden Effekt: Ist das ETCS-Stellwerk als generische Anwendung zugelassen, so ist bei Ersatz, Änderung oder Neubau eines Stellwerkes keine aufwendige Projektierung der Anlagensicherheit und kein umfangreicher Sicherheitsnachweis für das Verhalten der Einzelanlage erforderlich. Wurde die Topologie präzise erfasst und die Anlage technisch geprüft, so kann die Anlage sicher genutzt werden. Dieses senkt den Projektierungsaufwand und verkürzt die Vorlaufzeiten für Stellwerkprojekte erheblich (Bild 4).

Der Vorteil der funktionalen Verlagerung hin zum TMS (Bild 5) liegt nicht nur darin, dass der Softwareumfang der teuren Sicherheitssysteme auf ca. 20-30 % reduziert werden kann. Der wesentliche Vorteil liegt darin, dass Betriebsprozesse nur noch im TMS ab-

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.).

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

The generically applicable risk assessment at runtime has yet another significant effect: if the ETCS interlocking is approved as a generic application, no costly project planning of the equipment safety and no comprehensive safety case for the behaviour of a single piece of equipment is required during the replacement, modification or installation of a new interlocking. The system can be safely used, if the topology has been precisely recorded and the system has been technically tested. This reduces the configuration costs and significantly shortens the lead times for interlocking projects (fig. 4).

One advantage of the functional shift to the TMS (fig. 5) involves the fact that the software scope of expensive safety systems can be reduced to approximately 20-30 %. The main advantage is that operational processes only have to be mapped in the Traffic Management System, since the generic safety check function of the ETCS interlocking works in the same way in every topology and in every operating process and process state.

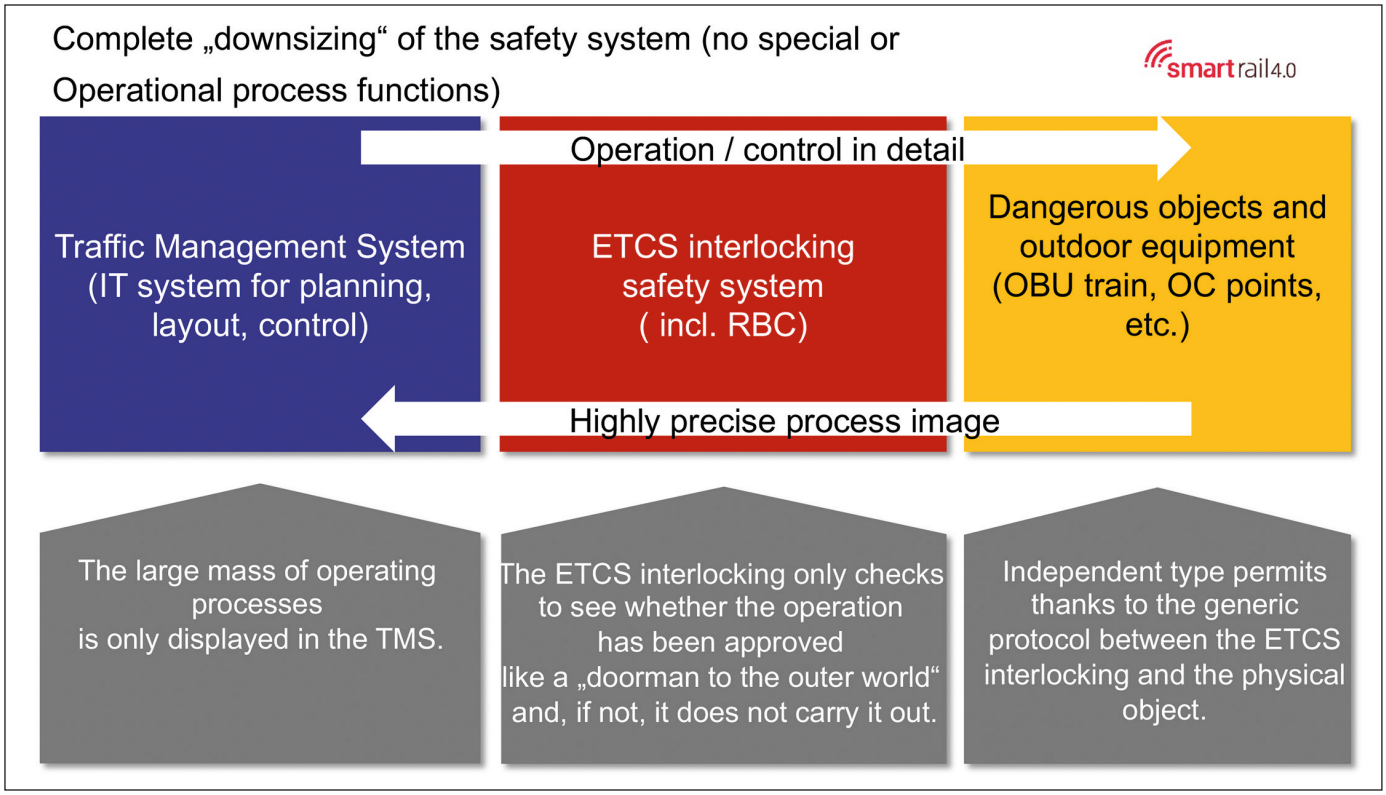


Bild 5: Das Designziel ist eine „schlanke prozessunabhängige SIL4 Ebene“ in der CCS Architektur.
Fig. 5: The design target is a “slim and process independent SIL4 layer in the CCS architecture”.

gebildet werden müssen, da die generische Sicherheitsprüfungsfunktion des ETCS-Stellwerks auf jeder Topologie und bei jedem Betriebsprozess und Prozesszustand in gleicher Art und Weise funktioniert. Das „ETCS-Stellwerk“ ist damit in jedem Land und auf jeder Topologie mit gleicher Funktionalität einsetzbar. Die mathematischen Parameter der generischen Risikobewertungsfunktion sind konfigurierbar, sodass unterschiedliche Sicherheitsniveaus für verschiedene Verkehrsarten oder regulative Vorgaben eingestellt werden können. Damit ist das ETCS-Stellwerk sowohl bei hohen Verkehrsdichten als auch kostengünstig für Nebenstrecken einsetzbar. Nur die Ausstattung mit Außenanlagen oder die Qualität der Fahrzeugausrüstungen entscheidet noch darüber, welche Verkehrsdichten möglich sind – das Stellwerk ist immer das gleiche. Die Parameter der Risikobewertungsfunktion sind aufgrund

The “ETCS interlocking” 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 ETCS interlocking can be cost-effectively used both in high traffic densities and on secondary lines. Only the amount and type of trackside assets or the quality of the rolling stock decides on what traffic densities are possible; the interlocking is always the same. Due to the centralisation of the interlocking systems (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 (such as transports of dangerous goods).

der Zentralisierung der Stellwerke (sichere Rechenzentren) für ein ganzes Netz gleichzeitig veränderbar oder können spezifisch für bestimmte Zugkategorien (wie Gefahrenguttransporte) eingestellt werden.
Das TMS kann nun als reines IT-System detaillierte optimierte Feinsteuerungen des Verkehrsflusses vornehmen. Es kann sich z. B. entweder für höhere Geschwindigkeiten oder alternativ für weniger Flankenschutz und niedrigere Geschwindigkeiten entscheiden. Es kann sich abhängig von der aktuellen Fahrkonfliktlage wie ein präzises Mess- und Regelungssystem nun für schnell zu aktualisierende kurze MA und etwas reduzierte Geschwindigkeiten entscheiden (bessere Gesamtkapazität in der Konfliktzone) oder einzelne Züge mit längeren MA und höheren Geschwindigkeiten ausstatten (Priorisierung). Simulationen zeigen, dass diese „präzise adaptive Feinsteuerung" die Performance eines Knotens stark anheben und den kapazitätsschädlichen Effekt von Geschwindigkeitsschwellen stark reduzieren kann. Kurze Zugfolgezeiten mit ETCS-Führerstandsignalisierung, präzises Fahren mit Automatic Train Operation (ATO) und präzise Lokalisierung sind hier Teil der Lösung – ohne eine Stellwerkfunktionalität, die sie voll ausnutzen kann, ist ihre Effektivität jedoch sehr begrenzt.

7 Hardwareabstraktion, Investitionsschutz und Aufwärtskompatibilität

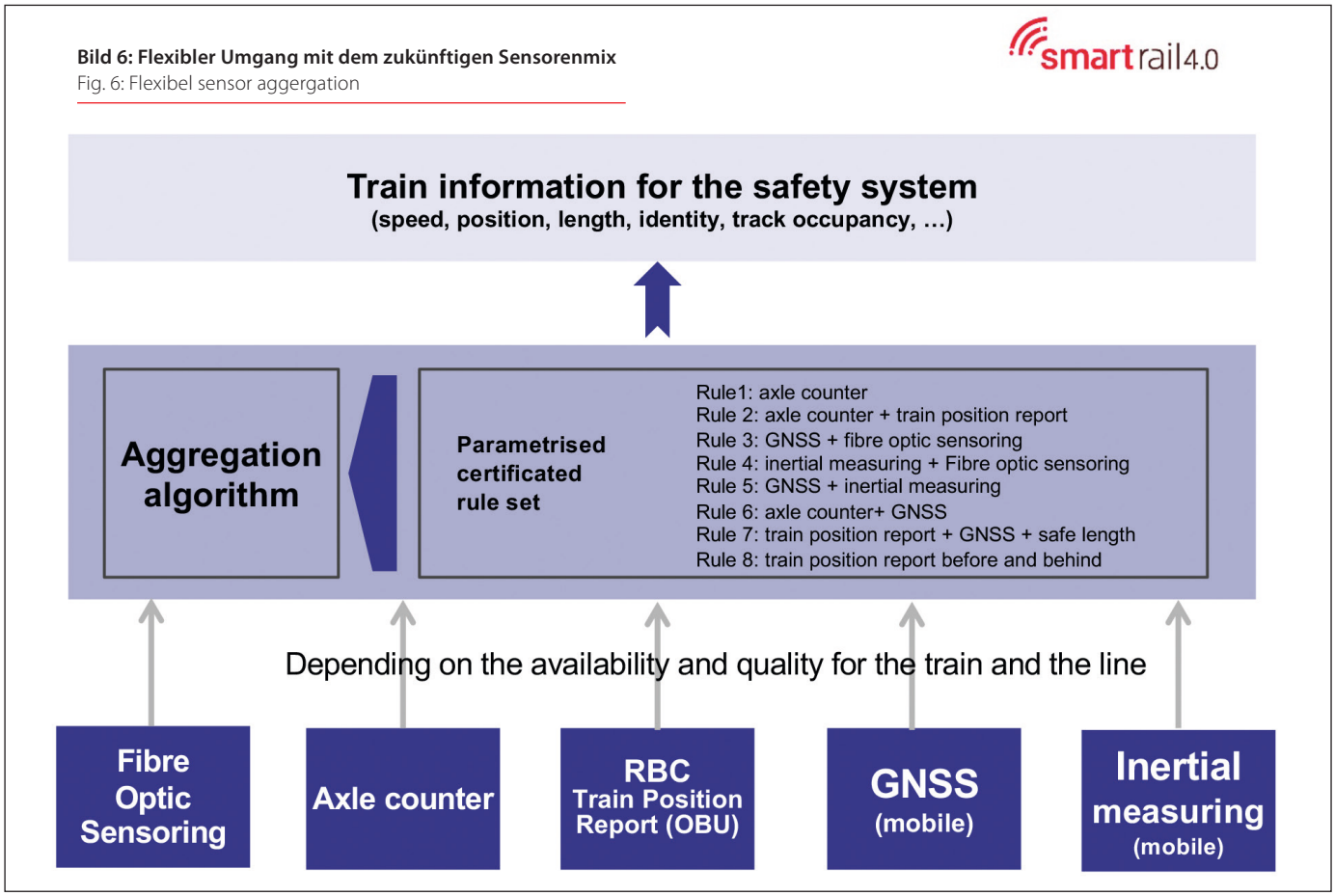
Mehr als 80 % des investierten Kapitals der CCS-Anlagen steckt in den Außenanlagen. Zum Schutz und zum optimalen Einsatz dieses Anlagenkapitals muss ein Stellwerk mehrere spezifische Eigenschaften aufweisen, die heute in traditionellen Stellwerken nicht in dieser Form üblich sind.

As a pure IT system, the TMS can now carry out detailed, optimised fine-tuning of the traffic flow. For example, it can opt for either higher speeds with full flank protection or alternatively for less flank protection and lower speeds. It can now opt for short MA and slightly reduced speeds (better total capacity in the conflict zone) or equip individual trains with longer MA and higher speeds (prioritisation) depending on the current driving conflict situation like a precise industrial regulation and control system. Simulations have shown 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 ATO (Automatic Train Operation) driving and precise localisation are all part of the solution, but their effectiveness is very limited without an interlocking functionality which can take full advantage of them.

7 Hardware abstraction, investment protection and upward compatibility

More than 80 % of CCS investments are in trackside assets. In order to protect and optimally use this investment capital, an interlocking must have several specific characteristics which are not currently customary in traditional interlocking systems. The first important optimisation involves the introduction of hardware abstraction. As in any modern operating system, the specific properties of the "end devices" (in this case, the trains or the interlocking systems) may not be processed in the central application control (safety logic) or anchored in a hardware specific manner. They must be described and processed abstractly

Bild 6: Flexibler Umgang mit dem zukünftigen Sensorenmix
Fig. 6: Flexibel sensor aggergation



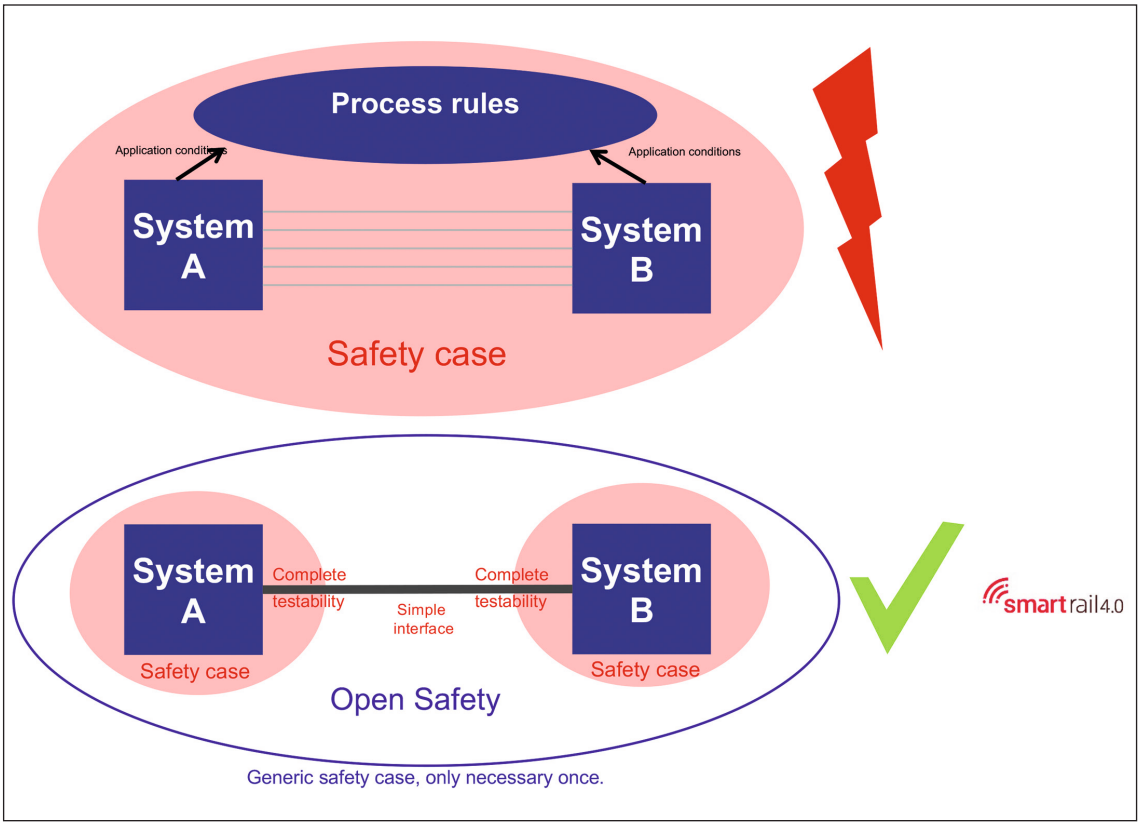


Bild 7: Anwendungsbedingungen müssen minimiert werden. Generische Integritätsnachweise müssen ermöglicht werden.
Fig. 7: Application conditions must be minimzed. Generic integrity safety cases must be possible.

Die erste wichtige Optimierung ist die Einführung der Hardwareabstraktion. Wie in jedem modernen Betriebssystem dürfen spezifische Eigenschaften von „end devices" (hier Züge oder Stellwerkaußenanlagen) nicht in der zentralen Anwendungssteuerung (Sicherheitslogik) verarbeitet werden oder hardwarespezifisch verankert sein. Sie müssen abstrakt und generisch beschrieben und verarbeitet werden. Denn andernfalls müssen bei jedem Wechsel der Außenanlagentechnologie auch eine Veränderung der Sicherheitslogik und ein neuer kompletter Sicherheitsnachweis erfolgen. Daher ist die Sicherheitslogik durch einen „hardware abstraction layer" (HAL) von den end devices zu trennen. Die Sicherheitslogik kennt nur die für sie notwendigen Fähigkeiten und Stati der Anlagen. So ist es z. B. oberhalb des HAL in der Sicherheitslogik nur wichtig, ob und wie eine Außenanlage gerade befahrbar ist und nicht, ob es sich dabei um einen Bahnübergang oder eine Weiche handelt und wie diese technisch ausgestattet ist. Nur ihre Fähigkeiten müssen bekannt sein.

Auch die Kommunikation zu einem Object Controller muss auf der Basis von abstrahierten Steuerungsprotokollen erfolgen, die den einfachen Austausch von Object Controller und Außenanlage durch eine andere und isoliert zugelassene Technologie ermöglicht. Dazu werden hochwertige, kontextabhängige und profilbasierte Protokolle verwendet, mit denen einerseits ein situatives Fähigkeitsprofil verhandelt wird (ähnlich zu USB oder Bluetooth) und andererseits das spezifikationstreue Verhalten eines Endgerätes an der Schnittstelle vollständig überprüft werden kann. Erst innerhalb des Object Controllers werden hardwarespezifische Steuerungen für die Außenanlage generiert. Diese Architektur generiert eine größere Unabhängigkeit von Innen- und Außenanlage, sowohl für den Sicherheitsnachweis als auch für die Beschaffung und die Durchführung von Ersatzprojekten (Bild 7). Im Endergebnis ist ein „Plug & Rail" realisierbar, vorbehaltlich einiger nicht automatisierbarer Validierungen.

and generically. Otherwise, a change in the safety logic and a completely new safety certificate must be generated with every change of the outdoor equipment 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 abilities and statuses of the systems. As such, for example, it is only important in the safety logic above the HAL whether and how a 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 skills need to be known.

The communication to an object controller for a trackside asset must also be based on abstracted control protocols, which enable the easy replacement of an "object controller" and a "trackside asset" with another, insulated approved technology. High-quality, context-dependent and profile-based protocols are used to negotiate a situational capability profile (similar to USB or Bluetooth) and to fully verify the specification-compliant behaviour of the trackside asset at the interface. Hardware-specific controls for the outdoor system are only generated within the object controller. This architecture generates greater independence from indoor and outdoor systems, both for the safety certification and for the procurement and implementation of replacement projects (fig. 7). As a result, a "plug & rail" concept is feasible.

Another key role of the new HAL is sensor aggregation and automated actuator coordination (for example, all currently available DMI trackside / onboard concerning a movement authority for a train). Sensor aggregation means, for example, for the detection of a track occupancy which can be determined from many different sources of information depending on the equipment on the track section or the train. Purist approaches such as "Pure ETCS levels", which have only actually numbered some of the possible hardware constellations, do not represent an optimal solution and are unnecessary. The constantly evolving

Eine weitere wesentliche Rolle des neuen HAL liegt in der Sensorenaggregation und in der automatisierten Aktorenkoordination (z. B. aller gerade verfügbaren DMI und Signalisierungswege für einen Zug). Sensorenaggregation bedeutet z. B. für die Erkennung einer Gleisbelegung, dass diese durch viele verschiedene Informationsquellen ermittelt werden kann – je nach Ausstattung eines Gleisabschnitts oder eines Zuges. Puristische Ansätze wie z. B. „reine ETCS-Level", mit denen letztlich nur einige der möglichen Hardwarekonstellationen nummeriert werden, stellen keine optimale Lösung dar und sind unnötig. Wirtschaftlicher und leichter migrierbar ist der sich ständig weiterentwickelnde Mix aus unterschiedlichen Sensortypen (Bild 6), mit dem das Stellwerk umgehen muss. In Abstellbereichen bleiben Gleichstromkreise oder Achszähler eventuell länger bestehen, auf der Strecke werden sie aufgrund selbstlokalisierender Züge schneller überflüssig. Schon hinter dem ersten Zug, der sich selber präzise geometrisch lokalisieren kann (z. B. über ETCS Level 3), möchte man mit möglichst kurzer Zugfolgezeit fahren, auch wenn andere Züge noch durch Achszähler lokalisiert werden (Bild 8).

Eine wichtige Funktionalität für eine kostengünstige Migration zur ETCS-Führerstandsignalisierung ist die Fähigkeit des neuen Object Controllers, eine einzelne Außenanlage gleichzeitig an die alte und an die neue Innenanlage umschaltbar anzuschließen. Die Umschaltung ist fernsteuerbar und ermöglicht die industrielle Vorbereitung großer Netzsegmente inkl. Inbetriebnahme in einem Schritt, ohne dass hohe Kosten für zahlreiche temporäre Schnittstellen entstehen oder ein kostenaufwendiger Komplettersatz von Innen- und Außenanlagen notwendig wird.

mix of the different sensor types (fig. 6) which the interlocking has to deal with is more economical and easier to migrate. DC circuits or axle counters may last longer in parking areas, but on the line they will become more and more obsolete due to self-locating trains. It would be optimal to drive at the shortest possible distance behind the first train which can precisely locate itself geometrically (i. e. using ETCS Level 3), even if other trains are still localised using axle counters (fig. 8). Pure configurations lead to expensive migrations.

An important functionality for the 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 one-step commissioning, without incurring high costs for numerous temporary interfaces or necessitating a costly complete set of indoor and outdoor installations.

8 The ETCS interlocking as a prerequisite for asset reduction and cost optimisation

ETCS cab signalling eliminates outside signals. However, a favourable migration through specific interlocking technologies must be made possible, as this allows large-segment conversions, favourable project planning and the reuse of the existing trackside assets. Shunting signals may also be eliminated by cab signalling. This requires an interlocking which can integrate mobile cab signalling systems and alternative localisation systems into the security process.

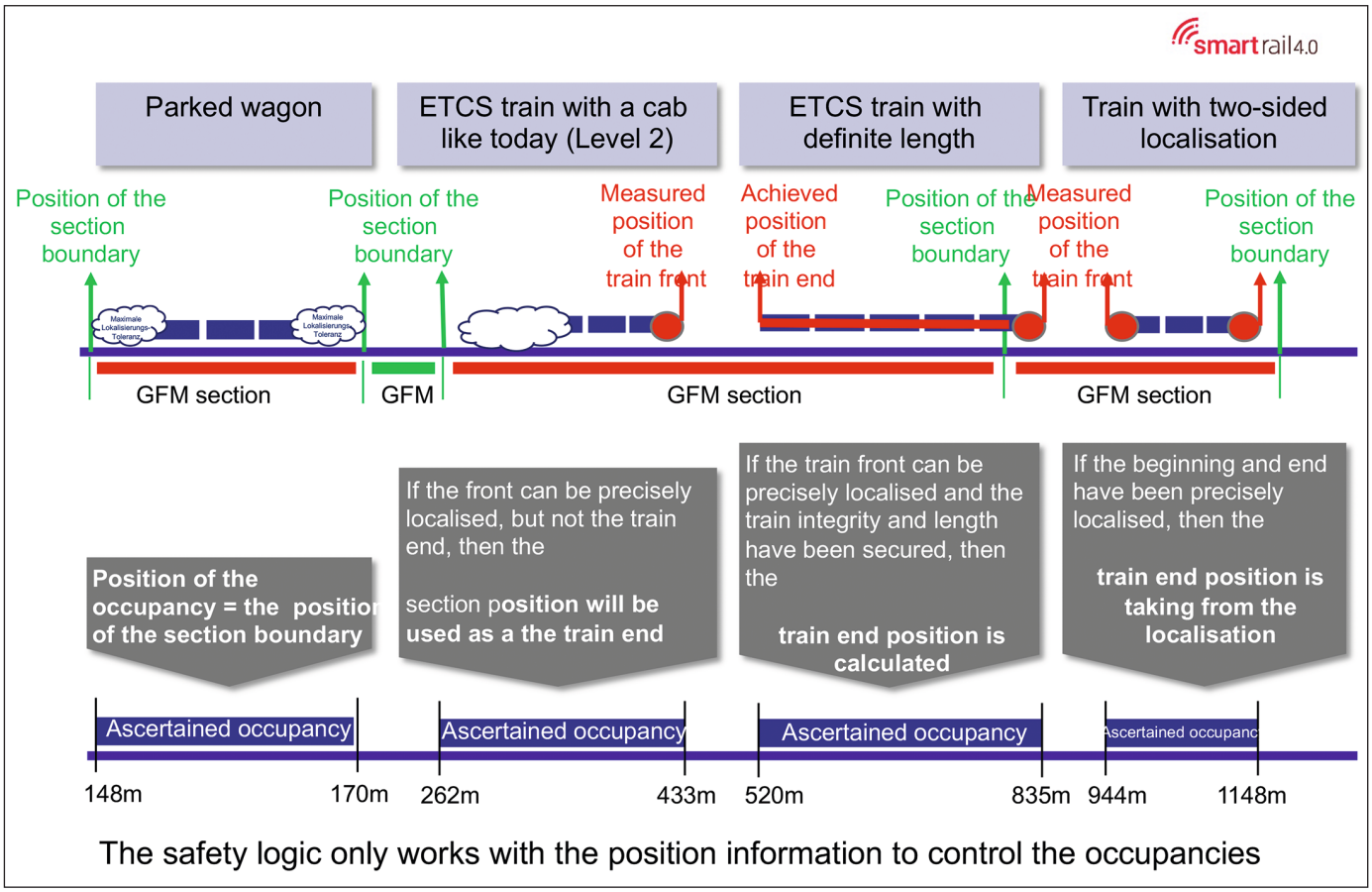


Bild 8: Nur eine Sicherheitslogik, die auf geometrischen Berechnungen basiert, kann den Mix der Sensoren voll ausnutzen, der in jeder Migration auftritt.
Fig. 8: Only a geometric safety logic can make the full use of the mix of fixed and mobile sensors, that exists in every migration.

8 Das ETCS-Stellwerk als Voraussetzung der Anlagenreduktion und Kostenoptimierung

Außensignale werden durch die ETCS-Führerstandsignalisierung eliminiert. Dafür muss jedoch eine günstige Migration durch spezifische Stellwerktechnologien ermöglicht werden, die die Umstellung in großen Segmenten, eine günstige Projektierung und die unveränderte Weiterverwendung der verbleibenden Außenanlagen ermöglicht.
Rangiersignale werden ebenfalls durch eine Führerstandsignalisierung eliminiert. Dafür ist ein Stellwerk erforderlich, das mobile Rangiersysteme und alternative Lokalisierungssysteme in den Sicherheitsprozess einbinden kann.
Heutige Gleisfreimeldesysteme und die wachsende Menge der Ortungsbalisen werden durch die Selbstlokalisierung des Zuges eliminiert, also durch sichere mobile Lokalisierung der geometrischen Gleisbelegung des Zuges inklusive Integritätsstatus. Dazu ist eine Stellwerklogik erforderlich, die mit geometrischen Belegungsinformationen und den verschiedenen degraded modes der kommenden mobilen Lokalisierungstechnologien in allen Kombinationen umgehen kann.

9 Status und nächste Schritte

Zurzeit laufen diverse Studien, second opinions und „proof of concepts" zum ETCS-Stellwerk, die bis Ende 2019 parallel zur Spezifikation und Ausschreibungsvorbereitung abgeschlossen werden. Die bisherigen Ergebnisse bestätigen die Machbarkeit, sodass das Programmteam davon ausgeht, dass das Konzept mit den beschriebenen Vorteilen realisierbar ist.

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

9 The status and the next steps

Various studies, second opinions and "proofs of concepts" are currently being prepared for the ETCS interlocking, which will be completed by the end of 2019 in parallel with the specification and tender preparation. The results to date have confirmed its feasibility, so the program team assumes that the concept can be realised with the described advantages. ■

LITERATUR | LITERATURE
[1] Publikationen zum ETCS-Stellwerk unter www.smartrail40.ch

AUTOREN | AUTHORS

Steffen Schmidt
Leadarchitekt smartrail 4.0 und
Leiter des Programms „ETCS Stellwerk"
SBB AG
Anschrift /*Address*: Hilfikerstrasse 3, CH-3014 Bern
E-Mail: steffen.schmidt@sbb.ch

David Grabowski
Projektleiter „ETCS Stellwerk Innenanlage" und
Leiter Sicherheitsmanagement smartrail 4.0
SBB AG
Anschrift /*Address*: Hilfikerstrasse 3, CH-3014 Bern
E-Mail: david.grabowski@sbb.ch