Ausrüstung von Fahrzeugen zur Realisierung des ETCS Level 3-Betriebs

Bringing ETCS Level 3 into operation from an onboard perspective

Martin Hetzer | Jael Kriener | Remo Unger | Jan Henrik Voß

Mit der geplanten Einführung von European Train Control System Level 3 (ETCS L3) hat Siemens Mobility die geltenden Spezifikationen, Analyseergebnisse europäischer Arbeitsgruppen und diskutierter Lösungsansätze zu einer ganzheitlichen Perspektive für die Ausrüstung von Fahrzeugen im Kontext eines ETCS L3-Betriebs zusammengefasst. Durch Anwendung einer strikten Nutzerperspektive wurden die technischen Auswirkungen auf die Fahrzeugausrüstung für die Überwachung der Zugvollständigkeit (Train Integrity) abgeleitet. Außerdem weist der Beitrag auf eine nicht eindeutige Regelung im entsprechenden Lösungsvorschlag (CR940) der Europäischen Eisenbahnagentur (ERA) hin, die ihren Ursprung in einer noch fehlenden harmonisierten Risikoanalyse für die sichere Zuglängenermittlung („Safe Train Length") hat.

1 Einführung

Die Frage, wie man ungewollte Zugtrennungen erkennen und melden kann, d. h. die Zugvollständigkeitsüberwachung realisiert, ist so alt wie die Eisenbahn selbst [1]. Ein liegengebliebener Waggon stellt ein enormes Risiko für nachfolgende Züge dar, wenn er nicht rechtzeitig erkannt wird. Dieses Thema hat maßgeblich an Bedeutung gewonnen, da der seit langem geplante ETCS L3 vor der Einführung steht. Im Kontext der Anwendung finden dabei eine Verlagerung von Funktionalitäten von der Strecke zum Fahrzeug sowie von Verantwortlichkeiten von Infrastruktur-Managern hin zu den Bahnbetreibern statt. So werden beispielsweise Eingangsinformationen für die Zugvollständigkeitsüberwachung nicht mehr ausschließlich von der Streckenausrüstung (z. B. Achszählern), sondern auch von der Fahrzeugausrüstung erzeugt.

Zwar wurden in den vergangenen zehn Jahren mehrere technische Prototypen für die Zugvollständigkeitsüberwachung entwickelt [2, 3], aber auf der Bereichsebene sind die Diskussionen im Hinblick auf die relevanten ETCS-Anforderungen und die erforderlichen Sicherheitsziele noch nicht abgeschlossen. Nach unserem Verständnis ist dies zum Teil auf einen fehlenden Konsens über die Aufteilung der Verantwortlichkeit zwischen den technischen Teilsystemen zurückzuführen, d. h. zwischen Zugleittechnik, ETCS-Fahrzeugausrüstung und dem zuständigen Zugbetreiber [3].

Zur Klärung der Aufteilung von Verantwortlichkeit auf der Fahrzeugseite gründete Siemens Mobility Ende 2019 eine Arbeitsgruppe, um die verschiedenen Erwartungen zu einer ganzheitlichen Perspektive zusammenzufassen. Hierfür werden die Fähigkeiten, aber auch die limitierenden Eigenschaften aller beteiligten fahrzeugseitigen Teilsysteme und Akteure gegenübergestellt und bewertet. Der Beitrag gibt eine Übersicht zur fahrzeugseitigen Aufteilung der Funk-

With the advent of European Train Control System Level 3 (ETCS L3), Siemens Mobility has condensed the diverse set of related specifications, European working group analyses and solution proposals into a holistic onboard perspective on ETCS L3 operations. The technical implications for the train integrity device have been derived by employing a strict user perspective. Furthermore, this article hints at an ambiguity in the corresponding European railway Agency (ERA) solution proposal (CR940) which is rooted in the existing lack of a harmonised risk analysis for determining "safe train length".

1 Introduction

The question of how to detect and report unintended train separations, i.e. train integrity monitoring, is as old as the railway system [1], since a stranded wagon poses an enormous risk to any following trains, if not detected in time. This topic has recently gained momentum, as the long envisioned ETCS L3 is finally on the brink of introduction. In ETCS L3, a substantial responsibility shift will take place from the infrastructure managers to the railway undertakings, since the train integrity monitoring inputs will no longer be generated by trackside equipment (e.g. thee axle counters), but will rely on onboard information.

While several technical prototypes for monitoring train integrity have been developed in the last decade [2,3], sector-level discussions regarding the relevant ETCS requirements and the necessary safety targets are still ongoing. In our understanding, this is partly rooted in the lack of consensus as to the allocation of responsibility between the technical subsystems, i.e. the train control management system, the onboard ETCS equipment and the acting train operator [3].

At the end of 2019, Siemens Mobility started a working group to condense the diverse expectations into a holistic view that balances the capabilities, but also the limitations from all the onboard subsystems and actors in order to shed some light on the allocation of responsibility to the onboard equipment. As such, this article provides an overview of the functional breakdown of the train integrity functionality and takes up the status of the harmonisation of the related safety requirements. Train integrity use cases are then operationalised and used to derive further user requirements. Building on this, the technical implications are subsequently outlined and discussed.

2 Train integrity and ETCS L3

With the publication of the TSI CCS 2022 for ETCS L3 operations, the principles of Hybrid ERTMS / ETCS L3 according to

tionen zur Zugvollständigkeitsüberwachung (Train Integrity) und greift den Stand der Harmonisierung der zugehörigen Sicherheitsanforderungen auf. Darüber hinaus werden spezifische betriebliche Anwendungsfälle analysiert und zur Ableitung weiterer Anwenderanforderungen verwendet. Hierauf aufbauend werden technische Implikationen skizziert und erörtert.

2 Train Integrity und ETCS L3

Mit der Veröffentlichung der TSI CCS 2022 werden für den ETCS L3-Betrieb die Prinzipien des Hybrid-ERTMS/ETCS L3 gemäß [4] angewandt. Dabei kommen feste virtuelle Blöcke zur Abstandregelung von Zügen zum Einsatz, die mit einer Zugvollständigkeitseinrichtung ausgestattet sind. Für die sichere Trennung von Zügen ohne Zugvollständigkeitseinrichtung sowie für die Behandlung von Störungen wird auf eine gegenüber konventionellen ETCS L2-Strecken reduzierte Anzahl streckenseitiger Gleisfreimeldeeinrichtungen zurückgegriffen. Es sei darauf hingewiesen, dass für einen reinen ETCS L3-Betrieb in Zukunft nur noch eine fahrzeugseitige Zugvollständigkeitseinrichtung verwendet wird, um die streckenseitigen Gleisfreimeldeeinrichtungen vollständig zu ersetzen. Dies wird zu erheblichen Einsparungen auf der Infrastrukturseite führen, da eine streckenseitige Gleisfreimeldung, z. B. mit Achszählern oder Gleisstromkreisen, nur noch punktuell zum Einsatz kommt [5].

Gemäß den ERTMS/ETCS-Spezifikationen [6] – erweitert durch CR940 – deckt die Train-Integrity-Funktionalität für die Berechnung der „Train Integrity Information" zwei hinreichend unabhängige Funktionen zur Bestimmung des „Train Integrity Status" und der „Safe Train Length" ab.

Der „Train Integrity Status" ist ein notwendiger Input für die Berechnung der „Safe Train Length". Nach dem aktuellen Stand der Standardisierung kann dieser aus zwei möglichen Quellen stammen und an den European Vital Computer (EVC) übermittelt werden:

- von einem externen Gerät (z. B. der Zugsteuerung) oder
- vom Triebfahrzeugführer (Tf), der die Zugvollständigkeit über das Driver Machine Interface (ETCS DMI) bestätigt.

Die Berechnung der „Safe Train Length" durch den EVC – nicht zu verwechseln mit der aus den ETCS Train Data sicher ermittelten tatsächlichen Zuglänge – berücksichtigt die folgenden Werte:

- die aktuelle Position der Zugspitze,
- die vom Zug zurückgelegte Strecke zum Zeitpunkt der Bestätigung des „Train Integrity Status" und
- die aus den ETCS Train Data sicher ermittelte tatsächliche Zuglänge.

Auf Basis des aktuellen Stands der Standardisierung können die ETCS Train Data aus den folgenden zulässigen Quellen stammen:

- von einem externen Gerät (z. B. der Zugsteuerung),
- im EVC gespeicherte vorkonfigurierte / validierte Werte oder
- vom Tf, der die tatsächliche Zuglänge über das ETCS DMI eingibt und bestätigt.

Die „Train Integrity Information" wird mit dem Position Report des Zuges an das Radio Block Center (RBC) übermittelt. Diese wird nach der streckenseitigen Auswertung in der Movement Authority (MA) des Folgezuges verwendet.

3 Gefährdungsidentifikation und Sicherheitsanforderungen

Die funktionalen Sicherheitsanforderungen und zugehörigen Gefährdungen im Zusammenhang mit der Train-Integrity-Funktionalität wurden von Shift2Rail (X2Rail-4 WP6, WP7) untersucht. Basierend auf den in der CENELEC-Sicherheitsnorm EN50126 [7] und der europäischen Verordnung über gemeinsame Sicherheitsverfahren zur Beurteilung von Risiken EU 402/2013 [8] und EU 2015/1136 [9] skiz-

[4] have been applied to use fixed virtual blocks in order to separate the trains that have been fitted with a train integrity device. The limited installation of trackside train detection is used to join and split trains without a train integrity device, as well as to handle any degraded situations. It should be noted that only a train integrity device will be used for pure ETCS L3 operations in the future in order to completely replace the track vacancy detection systems. This will lead to considerable savings on the infrastructure side, as trackside train detection, e.g. using axle counters or track circuits, will only be used selectively [5].

In accordance with the existing ERTMS / ETCS specifications [6] – extended by CR940 – train integrity functionality for the calculation of "train integrity information" covers two sufficiently independent functions for determining the "train integrity status" and "safe train length".

The "train integrity status" is a required input for the calculation of the "safe train length". According to the current state of standardisation, this may come from two possible sources and be transmitted to the European Vital Computer (EVC):

- confirmed by an external device (e.g. the train control system) or
- entered by the train driver using the Driver Machine Interface (DMI).

The calculation of the "safe train length" by the EVC – which must not be confused with the real (physical) train length securely determined from the ETCS train data – considers the following values:

- the train's current front end,
- the route travelled behind the train at the time when the "train integrity status" was confirmed and
- the real train length securely determined from the ETCS train data.

According to the current state of standardisation, ETCS train data can originate from the following permitted sources:

- an external device (e.g. the train control system),
- the pre-configured / validated values stored in the EVC, or
- from the driver entering and confirming the real train length via the DMI.

The "train integrity information" is transmitted to the Radio Block Center (RBC) with the Train Position Report. This is used once the following train's Movement Authority (MA) has been evaluated trackside.

3 Hazard identification and safety requirements

The functional safety requirements and related hazards allocated to the train integrity functionality have been analysed by Shift-2Rail (X2Rail-4 WP6, WP7). Explicit risk estimation has been chosen as the risk acceptance criteria (RAC) to determine the tolerable hazard rate (THR) on the basis of the safety principles outlined by the CENELEC EN50126 safety standard [7] and the EU 402/2013 [8] and EU 2015/1136 [9] European Regulation on Common Safety Methods for Risk Assessment. However, the considered severity class is "catastrophic" for both functions. Thus, the THR of 1E-9 /h is allocated to the top hazards known as "incorrect 'train integrity status' information is leading to an accident" and "incorrect 'safe train length' information is leading to an accident".

An explicit risk assessment has been performed on the basis of the field data provided by a European railway undertaking in order to determine the "train integrity status". The tolerable hazard rate value was apportioned to two contributing functions, i.e. the

zierten Sicherheitsprinzipien wurde eine explizite Risikoabschätzung als Risikoakzeptanzkriterium (RAC) zur Bestimmung der zulässigen Gefährdungsrate (THR) gewählt. Für beide Funktionen ist der betrachtete Schweregrad „katastrophal". Daher wird den Gefährdungen „Fehlerhafte ‚Train Integrity Status'-Information führt zu Unfall" und „Fehlerhafte ‚Safe Train Length'-Information führt zu Unfall" generisch eine THR von 1E-9 /h zugeordnet (Bild 1).

Für die Ableitung von Sicherheitsanforderungen an die Bestimmung des „Train Integrity Status" wurde eine explizite Risikoabschätzung auf der Grundlage von Felddaten europäischer Bahnbetreiber durchgeführt. Der Wert für die zulässige Gefährdungsrate wurde auf die zwei beteiligten Funktionen aufgeteilt, d. h. Zugkopplung und Überwachung der Zugvollständigkeit durch die Zugvollständigkeitseinrichtung. Das Ergebnis ist ein Sicherheits-Integritätslevel von SIL2.

Wenn die einem qualitativen SIL2 zugrundeliegende quantitative Sicherheitsanforderung auf die für die Ermittlung des „Train Integrity Status" gemäß UCR940 spezifizierten Informationsquellen abgebildet wird (siehe auch Abschnitt 2), kann davon ausgegangen werden, dass eine Umsetzung auf der Grundlage des aktuellen Stands der Entwicklung der Sicherheitsanforderung genügt. Dies gilt sowohl für den von einem externen Gerät (z. B. der Zugsteuerung) ermittelten „Train Integrity Status" als auch für einen vom Tf am ETCS DMI bestätigten Wert.

Für die Ableitung von Sicherheitsanforderungen an die Bestimmung der „Safe Train Length" gibt es bisher keine europäisch harmonisierte Risikoanalyse. Es bleibt daher notwendig, ein SIL4 unter Einbeziehung aller (funktional) relevanten Systemkomponenten nachzuweisen.

Wenn die einem qualitativen SIL4 zugrundeliegende quantitative Sicherheitsanforderung auf die für die Ermittlung der „Safe Train Length" gemäß UCR940 spezifizierten Informationsquellen abgebildet wird (siehe auch Abschnitt 2), kann sowohl für die durch den EVC bestimmte Position der Zugspitze als auch den durch den EVC bestimmten Fahrweg hinter dem Zug von einer zur Sicherheitsanforderung konformen Umsetzung auf Basis des aktuellen Stands der Entwicklung ausgegangen werden.

Anders ist die Ausgangslage bei den derzeit zulässigen Quellen der tatsächlichen Zuglänge auf der Grundlage der ETCS Train Data gemäß CR940 (siehe auch Abschnitt 2). Abgesehen vom EVC als Quelle eines statisch vorkonfigurierten / validierten Wertes kann eine SIL4-Güte im Hinblick auf eine betrieblich erwünschte dynamische Quelle (z. B. im Kontext des Anwendungsfalles Kuppeln / Entkuppeln) nicht angenommen werden. Dies gilt sowohl für ein externes Gerät (z. B. die Zugsteuerung) als auch für die Eingabe durch den Tf. Hier müssen produktspezifische Maßnahmen definiert werden, die im Kontext der Anwendung zu argumentieren sind.

In diesem Zusammenhang wurde auch eine Anpassung der CR940 zur Erweiterung der Anforderungen an mögliche Quellen einer dynamisch ermittelten Zuglänge vorgeschlagen. Dies schließt die Entlastung des Tf bei Argumentation der Sicherheitsfunktion mit ein.

4 Zugbetrieb und Anwenderanforderungen

Um ein besseres Verständnis der Nutzung der Train-Integrity-Funktionalität in verschiedenen Betriebsszenarien aus der Fahrzeugperspektive zu erlangen, wurde eine ganzheitliche Analyse erstellt. Die Zielsetzung war die Ableitung weiterer Anforderungen aus der erwarteten Nutzerinteraktion mit dem zukünftigen System im Betrieb. Zunächst wurden für die Train-Integrity-Funktionalität relevante Anwendungsfälle bestimmt und mit einem Bahnbetreiber besprochen, um notwendige Erkenntnisse aus dem Betrieb zu gewinnen.

train coupling and the train integrity monitoring by the train integrity device. However, the result was a safety integrity level of SIL2.

If the quantitative safety requirement underlying a qualitative SIL2 is mapped to the information sources specified for determining the "train integrity status" in accordance with CR940 (see also section 2), the implementation can be assumed to conform to the safety requirement based on the current state of development. This applies both to the "train integrity status" determined by an external device (e.g. the train control system) and to a "train integrity status" confirmed by the driver at the ETCS DMI.

On the other hand, there is no harmonised risk analysis for determining a "safe train length". It must therefore be possible to demonstrate SIL4 with the inclusion of all the (functionally) relevant system components.

If the quantitative safety requirement underlying a qualitative SIL4 is mapped to the information sources specified for determining the "safe train length" according to CR940 (see also section 2), it can be assumed that the determination of both the current front end of the train and the route travelled behind the train has been performed by the EVC and therefore implemented in conformity with the safety requirement based on the current state of development.

The situation is different for the currently permitted sources of the real train length based on the ETCS train data according to CR940 (see also section 2). Regardless of the EVC as the source of the statically pre-configured / validated value, a SIL4 quality cannot be assumed regarding an operationally desired dynamic source (e.g. within the context of the coupling / uncoupling use case). This applies to both the external device (e.g. the train

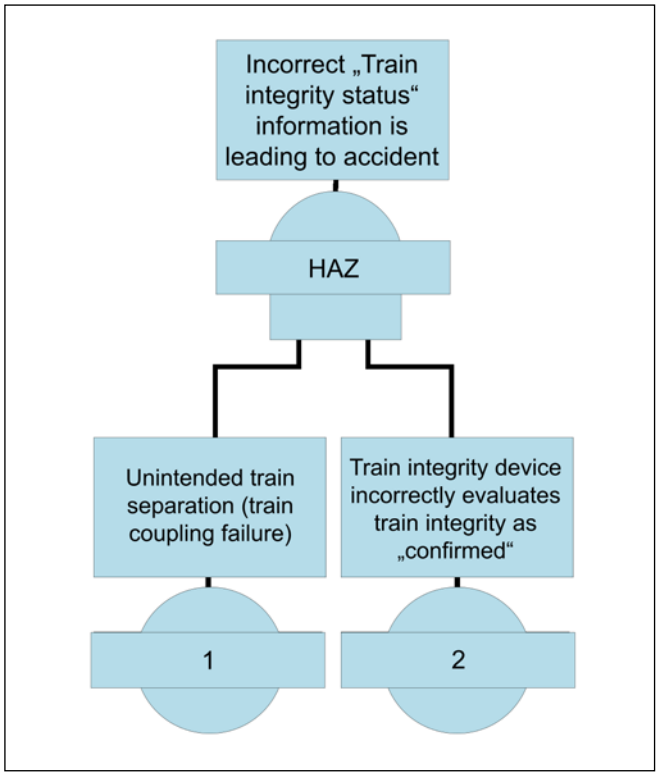

Bild 1: Fehlerbaum „Fehlerhafte ‚Train Integrity Status'-Information führt zu Unfall"
Fig. 1: The "incorrect 'train integrity status' information is leading to an accident" fault tree
Quelle / *Source*: Siemens Mobility GmbH

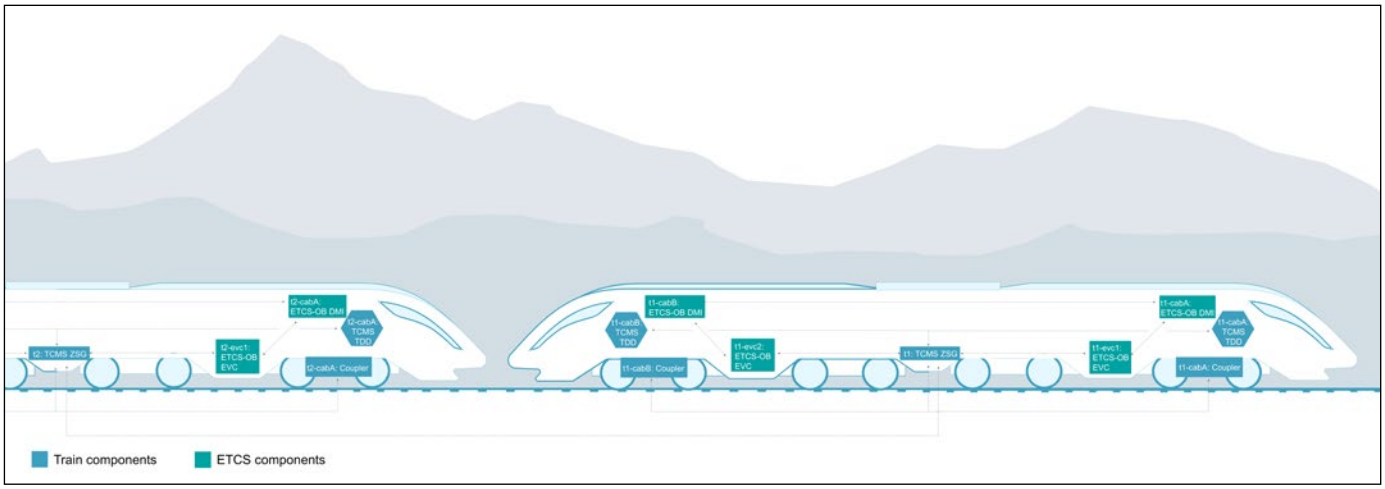

Bild 2: Zugarchitektur
Fig. 2: The train architecture

Quelle / *Source*: Siemens Mobility GmbH

Im Detail wurden die Anwendungsfälle als Ablaufdiagramme modelliert, um den internen Informationsfluss und die Interaktion an bestimmten Schnittstellen wie ETCS DMI, dem Technik- und Diagnosedisplay (TDD) des Train Control and Management Systems (TCMS) oder der Luftschnittstelle zwischen EVC und RBC zu verdeutlichen.
Die Grundlage für die Modellierung bildeten eine generische Zugarchitektur-Spezifikation, die Lösung für CR940 und die Spezifikationen für ETCS Baseline 3 Release 2. Eine zusätzliche Komplexität ergab sich aus der teilweise uneindeutigen und unbeständigen Spezifikationslage sowie den laufenden Diskussionen im Hinblick auf den L3-Betrieb (siehe auch Abschnitt 3).
Der Schwerpunkt wurde auf einen Zug in Mehrfachtraktion, bestehend aus zwei Fahrzeugen, gelegt. Jede Zugeinheit nutzt eine Train-Integrity-Architektur basierend auf zwei EVC, einer TCMS-Einheit mit direktem Zugriff auf den aktuellen Kuppelstatus und zwei Display-Einheiten pro Führerstand, ETCS DMI und TCMS TDD (Bild 2).
Basierend auf dieser Zugarchitektur wurden die Anwendungsfälle unter Verwendung von Ablaufdiagrammen illustriert, indem eine Lebenslinie für jede relevante Komponente des Fahrzeugs erzeugt wurde. Um das ganzheitliche Bild zur Train-Integrity-Funktionalität zu erhalten, wurde die Illustration um die streckenseitige RBC-Komponente sowie den Tf erweitert.
Die untersuchten Anwendungsfälle sind: Start-up aus dem ausgeschalteten Zustand, Start of Mission (SoM), Übergang zu L3, Kuppeln und Entkuppeln der Fahrzeuge sowie Fortsetzen des Betriebs nach dem Ausschalten, unzeitige Zugtrennung oder Kommunikationsfehler. Außerdem wurde nach Betrieb in Level 0, 1 oder NTC und Betrieb in Level 2 oder 3 unterschieden.
Anhand des Anwendungsfalls „Start of Mission im Level 2 oder 3" wird der Modellierungsansatz beispielhaft skizziert. Der Betriebsbeginn ist als Fortsetzung des Anwendungsfalls „Start-up aus dem ausgeschalteten Zustand" zu verstehen. Nach abgeschlossener Zugtaufe und Bestätigung der Zugkonfiguration wird der „Train Integrity Status" von der TCMS-Einheit an den EVC übermittelt. Außerdem müssen verschiedene Quellen für die Zuglänge unterschieden werden, sodass unterschiedlich restriktive Sicherheitsanforderungen für die Information berücksichtigt werden können.
Nach erfolgreichem Kommunikationsaufbau, wie in Subset-026, Abschnitt 5 spezifiziert, wird ein erster Position Report an das RBC gesendet. Wegen der ausstehenden Berechnung der „Safe Train Length" besteht der Position Report aus dem „Train Integrity Status" im Zustand „no integrity information" gemäß CR940.

control system) and the driver's input. Product-specific measures, which must be argued within the context of the application, must be derived here.
Within this context, however, an adaptation of the CR940 to extend the requirements to possible sources of a dynamic train length determination have also been suggested. This includes relieving the driver when arguing the safety function.

4 Train operations and user requirements

A holistic analysis has been established in order to gain a deeper understanding of the use of train integrity in different operating scenarios from a vehicle perspective. The goal was to derive further requirements from the expected user interaction with the future system under operation.
As a first step, train integrity relevant use cases were determined and discussed with a railway undertaking in order to gain valuable insight from operations. The use cases were modelled in detail as sequence diagrams in order to make the internal information flow and interaction explicit at specific interfaces, such as ETCS DMI, the Train Control and Management System (TCMS) Technical and Diagnostic Display (TDD) or the air gap between EVC and RBC.
The modelling basis was a generic train architecture specification, the solution for CR940 and the set of specifications for ETCS baseline 3 release 2. Further complexity existed due to the ambiguous and volatile set of specifications and ongoing discussions regarding L3 operations (see also section 3).
The focus was on a multi-traction train consisting of two trainsets. Each trainset uses a train integrity architecture based on two EVC, one TCMS unit with direct access to the current coupling status and two display units per cab, ETCS DMI and TCMS TDD.
The use cases were illustrated on the basis of the train architecture using sequence diagrams by creating a lifeline for each relevant vehicle component. The illustration was extended to include an RBC component and the driver so as to gain a holistic picture of the train integrity.
The analysed use cases are start-up from no power, start of mission, the transition to L3, joining and splitting trainsets and the continuation of operations after powering down, untimely train separation or a communication error. Furthermore, a distinc-

Im nachfolgenden Zugdaten-Eingabeverfahren kann der Tf die vom TCMS gelieferte Zuglänge bestätigen oder ändern. Wird die Zuglänge vom Tf geändert, so wird der „Train Integrity Status" auf „no integrity information" gemäß CR940 gesetzt. Der intern behandelte „Train Integrity Status" des TCMS bleibt jedoch unverändert. Optional ist die Ausgabe einer Diagnosemeldung an den Tf möglich, die diesen über den neuen Stand des „Train Integrity Status" informiert. In diesem Fall wird der „Train Integrity Status" erst wieder gültig, nachdem das Zugdaten-Eingabeverfahren wiederholt wurde.
Ändert der Tf die Zuglänge nicht, so kann der EVC auf eine tatsächliche Zuglänge mit hoher Güte zurückgreifen. Sind alle weiteren erforderlichen Werte am EVC verfügbar, so kann basierend darauf nun auch die „Safe Train Length" berechnet werden.
Die ETCS Train Data – einschließlich der vom Tf während des Zugdaten-Eingabeverfahrens geänderten und validierten Zuglänge – und der Position Report werden anschließend an das RBC gesendet. Gemäß CR940 enthält der Position Report an das RBC den „Train Integrity Status" im Zustand „no integrity information".
Anschließend quittiert das RBC die ETCS Train Data, der Tf wählt „Start", und eine MA-Anforderung einschließlich eines Position Reports wird an das RBC gesendet. An diesem Punkt kann der Position Report den „Train Integrity Status" im Zustand „bestätigt durch externes Gerät" und eine berechnete „Safe Train Length" enthalten.
Anschließend sendet das RBC eine MA, und der EVC schaltet in die gewünschte Betriebsart um (Bild 3).
Ein Ergebnis der Untersuchung der Betriebsszenarien war, dass der EVC, der nicht der führende EVC ist und daher in den Sleeping-Modus geschaltet wurde, weder für die Ermittlung des „Train Integrity Status" noch für die Berechnung der „Safe Train Length" relevant ist. Daher wurden die Illustrationen entsprechend angepasst und der Sleeping-EVC abstrahiert, um die Komplexität zu reduzieren und Fehlinterpretationen zu vermeiden.
Des Weiteren zeigen die Modelle gewisse Uneindeutigkeiten in der Spezifikation auf. Betreiber erwarten, dass die ETCS-Fahrzeugeinrichtung nach dem SoM-Verfahren für den L3-Betrieb bereit ist. Hierzu muss es möglich sein, die tatsächliche Zuglänge mit hoher Güte zu ermitteln. Angesichts des Fehlens einer harmonisierten Risikoanalyse wird es jedoch weiterhin zur Diskussion stehen, auf welchem spezifischen Sicherheitsziel die Ermittlung der tatsächlichen Zuglänge basieren muss. Bis dahin ist das restriktivste Sicherheitsziel anzunehmen, weshalb der Tf keinen Beitrag zur Argumentation einer Sicherheitsfunktion zur Berechnung der „Safe Train Length" leisten sollte.

5 Technische Auswirkungen

Wie zuvor erwähnt, erfordert ETCS L3, auch als hybrider L3-Betrieb, dass neue Informationen – „Train Integrity Status" und „Safe Train Length" – von der ETCS-Fahrzeugausrüstung zur ETCS-Streckenausrüstung übertragen werden. Daher müssen durch die ETCS-Fahrzeugausrüstung neue Funktionalitäten implementiert werden, um diese neuen Informationen zu generieren. Darüber hinaus stellen diese neuen Funktionalitäten eine neue Stufe der Verantwortlichkeit für die ETCS-Fahrzeugausrüstung dar und sind mit neuen Herausforderungen verbunden.
Die Train-Integrity-Funktionalität bringt zwei grundlegend neue Aspekte mit sich:

1. Nach dem aktuellen Stand der Entwicklung besteht die Hauptverantwortung der ETCS-Fahrzeugausrüstung in der Überwachung des Standortes und der Geschwindigkeit des Zuges. Vor allem soll dieser vor dem Ende einer MA sicher zum Stillstand kommen. Mit der Einführung des ETCS L3 und Bereitstellung von Zugvoll-

tion was made between operations in Levels 0, 1 or NTC and operations in Levels 2 or 3.
The modelling approach has been outlined taking the "start of mission in Level 2 or 3" use case as an example. St–rt of mission needs to be read as a continuation of the "start-up from no power" use case. After the train inauguration and confirmation of the train configuration, the "train integrity status" is transmitted from the TCMS unit to the EVC. Furthermore, the different sources of the actual train length must be distinguished in order to consider the different restrictive safety requirements pertaining to this information.
The first position report is sent to the RBC once a successful session has been established, as specified in Subset-026, section 5. Due to the pending calculation of the "safe train length", the position report consists of the "train integrity status" in the "no integrity information" state according to CR940.
The driver is able to confirm or change the train length provided by the TCMS in the following train data entry procedure. The "train integrity status" is set to "no integrity information" according to CR940 when the train length is changed by the driver. However, the "train integrity status" internally handled by TCMS remains unchanged. Optionally, the output of a diagnostic message to the driver informing him of the new "train integrity status" is also conceivable. In this case, however, the "train integrity status" will only become valid again after the train data entry procedure has been repeated.
If the driver does not change the train length, the EVC can calculate the actual train length at a high quality. Moreover, the EVC is also able to calculate a "safe train length" at this point, if the parameters necessary for the "safe train length" calculation are already available to the EVC.
The ETCS train data – including the train length modified and validated by the driver during the train data entry procedure – and the position report are then sent to the RBC.
According to CR940, the Position Report sent to the RBC will contain the "train integrity status" in the "no integrity information" state.
The RBC subsequently acknowledges the ETCS train data, the driver selects "start" and an MA request, including a position report, is sent to the RBC. At this point the position report may include the "train integrity status" in the "confirmed by external device" state and a calculated "safe train length".
The RBC then sends an MA and the EVC switches to the desired mode.
The first finding from the investigation of the operating scenarios was that the EVC that is not the leading EVC and is therefore switched to sleep mode is not relevant for either determining the "train integrity status" or calculating the "safe train length". Hence, the illustrations were adapted and the sleeping EVC were abstracted in order to reduce the complexity and prevent any false interpretations.
Secondly, the models highlight an important ambiguity within the specification. Operators expect the ETCS onboard system to be ready for L3 operations after the SoM procedure. As such, it must be possible to determine the real train length at a high quality. However, in the absence of a harmonised risk analysis, there will still be a discussion about which specific safety target the determination of the real train length is based on. Until then, the most restrictive safety target must be assumed. What is clear, however, is that the driver should not have to make a safety contribution insofar as such a high safety target is linked to the determination of the "safe train length".

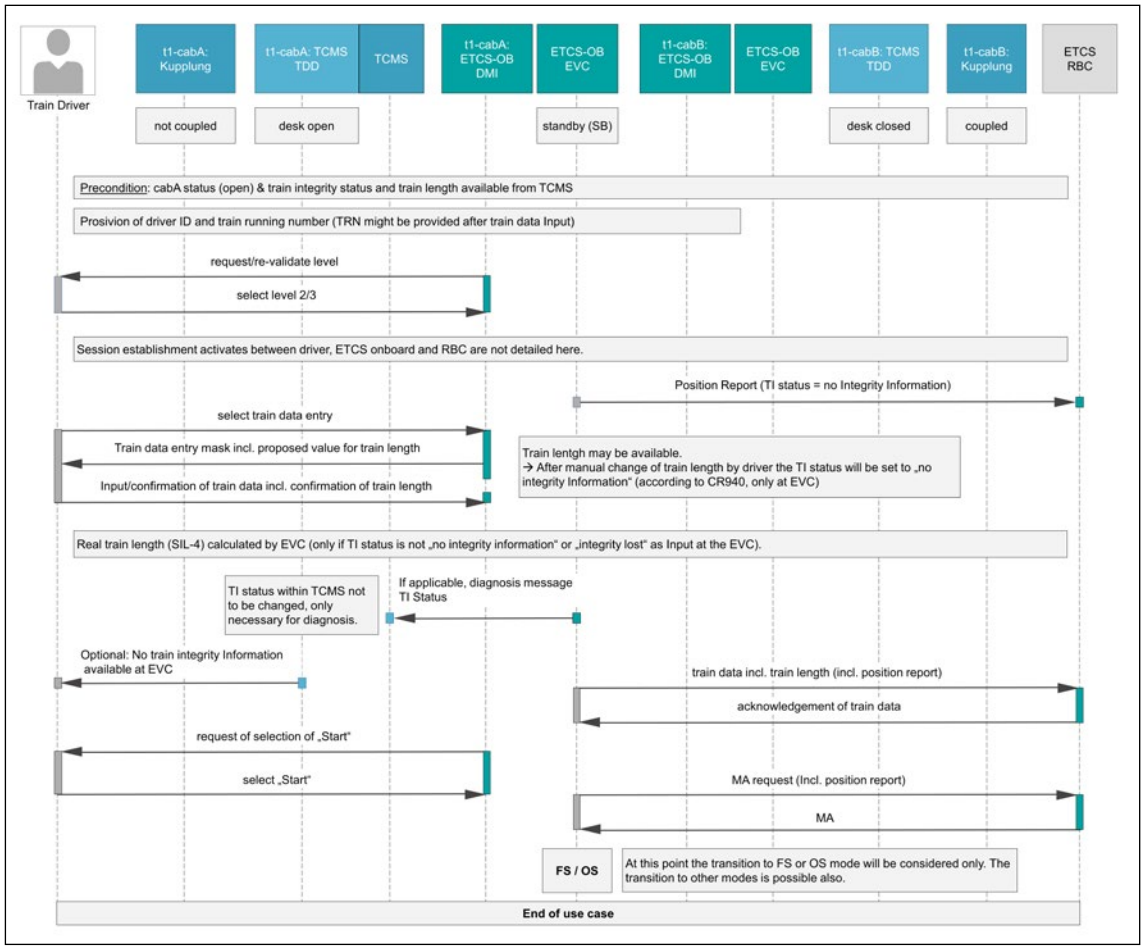

Bild 3: Anwendungsfall Start of Mission Level 2 oder 3
Fig. 3: The Level 2 or 3 start of mission use case Quelle / *Source*: Siemens Mobility GmbH

ständigkeitsinformationen durch das Fahrzeug selbst schützt die ETCS-Fahrzeugausrüstung nicht nur den Zug, in dem es installiert ist, sondern vor allem auch nachfolgende Züge auf der Strecke. Daher spielt eine einzelne ETCS-Fahrzeugausrüstung zukünftig eine andere Rolle im Kontext des Systems Bahn. Eine solch grundlegende Änderung der Randbedingungen hat natürlich Auswirkungen auf die Analyse und Ableitung von Anforderungen, insbesondere von nicht-funktionalen Anforderungen.

2. Derzeit kann jede ETCS-Fahrzeugausrüstung in einem einzelnen Fahrzeug als „Insel" angesehen werden. Der Zug wird nicht als funktionale Einheit ausgelegt. Die ETCS-Fahrzeugausrüstung erhält alle relevanten Informationen zur Umsetzung der Zugsicherungsfunktionalität vom Tf (über das Zugdaten-Eingabeverfahren) und vom TCMS (über Signale wie Cab Status, Sleeping angefordert usw.). Wie wir gesehen haben, ist dies möglicherweise nun nicht mehr ausreichend.

Die technische Lösung für diese neue erforderliche Funktionalität richtet sich stark an den hierfür festgelegten Anforderungen, einschließlich geltender Sicherheitsanforderungen, aus. Als allgemeine Faustregel gilt dabei, dass jede komplexe Information bis SIL2 durch das TCMS generiert und über die entsprechende Schnittstelle zur ETCS-Fahrzeugausrüstung übertragen werden kann. Jede komplexe Information, für die eine höhere Güte als SIL2 erforderlich ist, muss von der ETCS-Fahrzeugausrüstung selbst generiert werden.

Für die Train-Integrity-Information kann derzeit SIL2 für den „Train Integrity Status" angenommen werden, während für die „Safe Train Length" jedoch eine restriktivere (höhere) Sicherheitsanforderung angesetzt werden muss. Dies bedeutet in technischer Hinsicht, dass der „Train Integrity Status" vom TCMS ermittelt und über die zuge-

5 The technical implications

As outlined above, ETCS L3, even as hybrid L3 operations, requires new information – the "train integrity status" and "safe train length" – to be transmitted from the onboard ETCS system to the trackside ETCS. Hence new functionalities must be implemented in the ETCS onboard system in order to generate this new information. Moreover, this new set of functionalities represents a higher level of responsibility for the onboard ETCS system and comes with a new set of challenges.

There are two fundamentally new aspects to the train integrity functionality:

1. As the current state of the art, the primary responsibility of the onboard ETCS unit is to protect the equipped train by supervising its location and speed. And most importantly to make sure that it will come to a stop before the end of the MA. When providing train integrity information, the onboard ETCS system not only protects the train on which it is installed, but crucially also any train following on the track. Thus, a single onboard ETCS unit currently plays a different role in the entire railway system than that expected in the future. Such a fundamental change to the basic approach obviously has its implications for the analysis and derivation of the requirements, especially the non-functional ones.
2. Each onboard ETCS unit within a single trainset can currently be seen as an "island". The onboard ETCS system acquires all the relevant information to play its train protection role from the driver (via the data entry procedure) and

hörigen Schnittstellen an die ETCS-Fahrzeugausrüstung übertragen werden kann. Davon wird aktuell in der Spezifikation der Schnittstelle ausgegangen, in der diese Information als Eingabe vom TCMS zur ETCS-Fahrzeugausrüstung definiert ist und durch Mechanismen nach dem aktuellen Stand der Technik übertragen werden kann (siehe die aktuellen Entwürfe von Subset-034 und Subset-119).
Ganz anders ist die Situation für die „Safe Train Length", für die derzeit Sicherheitsanforderungen in der Größenordnung von SIL4 nötig sein könnten. Die Schnittstelle zwischen TCMS und ETCS-Fahrzeugausrüstung unterstützt derzeit nicht die Übermittlung von komplexen numerischen Daten dieser Güte. Dies bedeutet, dass die tatsächliche Fahrzeuglänge, die zur Berechnung der „Safe Train Length" erforderlich ist, durch die ETCS-Fahrzeugausrüstung selbst bestimmt werden muss.
Wenn der laufende Analyse- und Standardisierungsprozess zu einer Anforderung für die technische Ermittlung der tatsächlichen Zuglänge mit der Güte SIL4 führt, so wird dies mit den technischen Lösungen auf Basis des aktuellen Stands der Entwicklung in Hochgeschwindigkeits- und Regionalzügen nicht ohne Weiteres erfüllbar sein. In diesem Fall kann eine einzelne ETCS-Fahrzeugausrüstung nicht länger als "Insel" betrachtet werden. Die einzelnen ETCS-Fahrzeugausrüstungen müssen zu einem vereinten fahrzeugseitigen ETCS-Teilsystem vernetzt werden, das die Eigenschaften des gesamten (dynamisch konfigurierten) Zuges, den es sichert, kennt. Hiermit sind neue Herausforderungen verknüpft, einschließlich der Definition neuer Schnittstellen zu den ETCS-Fahrzeugausrüstungen sowie neuer Sicherheitsprotokolle, die eine solch hohe Güte gewährleisten können.
Die beschriebenen Aufgaben sind nicht unlösbar – ähnliche Probleme wurden bereits in verwandten Bereichen gelöst, z. B. im Nahverkehrssektor. Ihre Lösung, insofern erforderlich, wird für die ETCS-Fahrzeugausrüstung einen erheblichen Entwicklungsschub bedeuten.

6 Fazit

Die Einführung von ETCS L3 birgt Potenziale für Kosteneinsparungen und Kapazitätserweiterungen und verlagert im Kontext der Überwachung der Zugvollständigkeit (Train Integrity) essenzielle Funktionalitäten von der Strecke zum Fahrzeug sowie Verantwortlichkeiten von Infrastruktur-Managern hin zu den Bahnbetreibern. Um dies erfolgreich tun zu können, ist es äußerst wichtig, dass die neue fahrzeugseitige Train-Integrity-Funktionalität ihr volles Potenzial entfalten kann. Von entscheidender Bedeutung ist dabei, dass geltende Spezifikationen zu einem guten, harmonisierten Verständnis aller beteiligten Stakeholder führen; insbesondere bei Behörden, Betreibern und Herstellern.
Durch die Operationalisierung relevanter Anwendungsfälle hat sich die hier vorgestellte Analyse als effektiv erwiesen, um Ablauf, Timing und Qualität der technisch ermittelten sowie der durch den Tf eingegebenen Informationen darzustellen, die zur fahrzeugseitigen Berechnung der Train-Integrity-Informationen erforderlich sind. Dies ermöglichte allen Mitwirkenden, ihre erwartete Rolle zu hinterfragen und zur detaillierten Spezifikation der Train-Integrity-Funktionalität sowie der notwendigen Ausrüstung von Fahrzeugen im Kontext eines ETCS L3-Betriebs beizutragen.
Die Analyse hat gezeigt, dass die Standardisierung Fortschritte macht; jedoch bestehen weiterhin einige Unklarheiten, die ihre Ursache u. a. in der weiterhin fehlenden Harmonisierung einer Risikoanalyse für die sichere Zuglängenermittlung („Safe Train Length") haben. Die Festlegung europäisch harmonisierter Sicherheitsziele hat ggf. maßgebliche Implikationen auf die fahr-

from the TCMS (via signals such as Cab Status, Sleeping Requested, etc.). As we have seen, this may no longer be sufficient.
The technical solution to such a new required functionality depends strongly on the requirements, including the safety requirements, determined for it. As a general rule of thumb, any complex information up to SIL2 can be determined by the TCMS and transmitted via the interface to the onboard ETCS system; any complex information that is required at a quality greater than SIL2 has to be determined by the onboard ETCS system.
With regard to the train integrity information, SIL2 can currently be assumed for the "train integrity status", but the more restrictive safety requirements of SIL4 have to be assumed for the "safe train length". This means that the "train integrity status" can be technically determined by the TCMS and transmitted to each ETCS onboard unit via their interface; this is currently assumed in the interface specification, where this information has been defined as an input from TCMS to the onboard ETCS and can be transmitted by the state of the art mechanisms (see Subset-034 & Subset-119 in the current draft versions).
The situation is quite different for the "safe train length" where safety requirements at the order of SIL4 might currently be necessary. The interface between the TCMS and the onboard ETCS system does not currently support the transmission of complex numeric data of this quality. This means that the real train length, which is required for calculating the "safe train length", has to be determined at such a high quality in the onboard ETCS system.
If the ongoing analysis and standardisation process results in a requirement for the technical determination of a real train length at SIL4 quality, this will not be readily solvable using the technical solutions that are the state of the art in high-speed and regional trains.
In this case, each ETCS onboard unit will no longer be able to be an isolated island on the train. The single onboard units will have to be connected to form a unified onboard ETCS system that has knowledge of the properties of the entire (dynamically configured) train it is protecting. This comes with a set of challenges, including new interfaces to the ETCS onboard units to be defined and new safety protocols to reach this high level of quality. These challenges are not insurmountable, as similar problems have been solved in related domains (e.g. mass transit trains), but such a solution for the ETCS onboard system, if required, will represent a considerable advance over and above the current state of the art.

6 Conclusion

The introduction of L3 ETCS promises both cost reductions and potential capacity increases and as such it shifts the responsibility for generating the train separation functionality inputs from the trackside to the train. In order to achieve this, it is of utmost importance that the new onboard train integrity functionality can reach its full potential and hence it is crucial that the train integrity specification is well understood, justified and aligned among all the stakeholders from the regulatory, operations and supply sides.
By operationalising the relevant use cases, the analysis at hand has proven to be an effective way of visualising the sequence, timing and quality of both the technical and train driver inputs which are needed to calculate train integrity onboard. This enables ETCS external contributors to question their expected role and contribute to the train integrity specification. As a result, a holistic view of train integrity has been created.

zeugseitige Train-Integrity-Architektur und die Argumentation der Zugvollständigkeitsüberwachung als solche. ■

This analysis has shown that standardisation is progressing, albeit that a few ambiguities rooted in the ongoing lack of a harmonised risk analysis for safe train length determination remain. The definition of a European harmonised safety target has significant implications for onboard train integrity architecture and train integrity supervision as such. ■

LITERATUR | LITERATURE

[1] Mitchell, I.: Train Integrity liegt in der Verantwortung des Bahnbetreibers, SIGNAL+DRAHT (101), 6/2009, S. 38-39
[2] Srb, S.; Kampik, V.: Technische Möglichkeiten der sicheren Feststellung der Zugvollständigkeit – Anwendbarkeit in modernen Zugsteuerungs- und -sicherungssystemen, SIGNAL+DRAHT (114), 1+2/2022, S. 22-30
[3] Seiffert, R.: Train Integrity, Realisierung von ETCS L3, SIGNAL+DRAHT (102), 9/2020, S. 49-50
[4] Hybrid ERTMS/ETCS L3, 16E042, Version 1E, 03/02/2022
[5] Eckert, A.; Brinkmann, F.; Scheier, B.: Kostenvergleich einer innovativen Zugvollständigkeitskontrolle, SIGNAL+ DRAHT (112), 12/2020, S. 52-58
[6] ERTMS/ETCS System Requirements Specification, 3.6.0, 13/05/2016
[7] EN50126-1:2017 Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS Prozess
[8] Durchführungsverordnung (EU) Nr. 402/2013 der Kommission vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009, 30.04.2013
[9] Durchführungsverordnung (EU) 2015/1136 der Kommission vom 13. Juli 2015 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken, 13.07.2015

AUTOREN | AUTHORS

Martin Hetzer
RAMSS Manager ATP-Fahrzeugausrüstung
E-Mail: martin.hetzer@siemens.com

Dr. Jael Kriener
Systemarchitekt ETCS-Fahrzeugausrüstung
E-Mail: jael.kriener@siemens.com

Remo Unger
System Manager ETCS-Fahrzeugausrüstung
E-Mail: remo.unger@siemens.com

Dr. Jan Henrik Voß
Program Manager Software-Applikationen für ETCS-Fahrzeugausrüstung
E-Mail: janhenrik.voss@siemens.com

Alle Autoren / *all authors*:
Siemens Mobility GmbH
Anschrift / *Address*: Kiefholzstraße 44, D-12435 Berlin