

Hin zu einem innovativen Eisenbahnbetrieb mit ETCS Hybrid Train Detection

Heading forwards to innovative railway operations with ETCS Hybrid Train Detection

Gregor Theeg | Craig McLellan | Heiko Saalbach | Frank Wend | Martin Hetzer | Lorenz Giese | Martin Haase

ETCS Level 2 – Hybrid Train Detection (ETCS HTD), früher auch bekannt als ETCS Hybrid Level 3, verfolgt das Ziel, die Streckenkapazität im Personen- und Güterverkehr zu erhöhen und dabei die streckenseitige Gleisfreimeldung zu reduzieren. Sowohl Züge mit als auch ohne Integritätsüberwachung können im Mischbetrieb auf den mit HTD ausgerüsteten Strecken fahren. Basierend auf dem aktuellen Stand der Standardisierung und mit Blick auf aktuelle Projekte haben Siemens Mobility GmbH und Informatik Consulting Systems GmbH (ICS) eine Sicherheitsstudie durchgeführt, um HTD-spezifische Gefährdungen zu identifizieren und zu quantifizieren und um spezielle Herausforderungen der unterschiedlichen Lösungsvarianten zu bewältigen. Dies beinhaltet insbesondere die Handhabung von Bestandsfahrzeugen und die Strategien zur Nachrüstung bestehender Strecken.

1 Zweck und Gegenstand von Hybrid Train Detection

Herkömmliche Zugortungssysteme sind zuverlässig; jedoch beeinträchtigen lange Gleisfreimeldeabschnitte die Streckenkapazität.

ETCS Level 2 – Hybrid Train Detection (ETCS HTD), in der Vergangenheit auch ETCS Hybrid Level 3 genannt, ist eine mögliche Umsetzung von ETCS Level 2 nach Baseline 4, die einen weiteren Schritt hin zur Erhöhung der Streckenkapazität im Personen- und Güterverkehr und Reduzierung der Streckenausrüstung ermöglicht. HDT-Systeme nutzen eine hybride Form aus konventioneller Gleisfreimeldung mittels Gleisstromkreisen und Achszählern einerseits und zugbasierter Zugschlusserkennung und Positionsmeldung andererseits. Um die Funktionalität der Zugerkenung zu erweitern, nutzt HTD die Positionsmeldungen der Fahrzeuggeräte, um daraus zu ermitteln, ob Gleisabschnitte besetzt sind oder freigemeldet werden können.

Die festen Blockabschnitte der streckenseitigen Zugerkenung (Trackside Train Detection – TTD) werden in virtuelle Unterabschnitte (Virtual Sub-Sections – VSS) unterteilt, siehe Bild 1. Unter Nutzung der bestehenden Gleisinfrastruktur ermöglicht dies den Zugbetrieb mit deutlich kürzerer Zugfolge, ohne dabei die Streckenausrüstung zu erhöhen. Zu diesem Zweck sendet die ETCS-Fahrzeugeinrichtung eine erweiterte Positionsmeldung an die ETCS-Streckenzentrale (Radio Block Centre – RBC). Basierend auf erhaltenen Informationen aus externen Quellen über Zuglänge und Zugintegrität wird die Confirmed Train Length zur Verfügung gestellt, welche die Zugintegrität beinhaltet [1]. Dies geht einher mit einer teilweisen Verlagerung von Verantwortung vom Infrastrukturbetreiber zum Fahrzeugbetreiber, da die Zugintegrität

ETCS Level 2 – Hybrid Train Detection (ETCS HTD), formerly known as ETCS Hybrid Level 3 will increase the line capacity for passenger and freight transport and reduce trackside equipment. Both new trains with integrity monitoring capabilities and older trains without can operate on HTD lines in mixed traffic. Siemens Mobility GmbH and Informatik Consulting Systems GmbH (ICS) have conducted a safety study based on the current state of standardisation and in light of the projects in the pipeline in order to identify any HTD-specific hazardous scenarios and quantify the hazard rates, as well as to reveal and eliminate any challenges from the specific solution variants. This particularly includes the handling of the existing vehicles and the retrofitting strategy.

1 The purpose and scope of Hybrid Train Detection

While reliable, traditional train detection systems do have their limitations and can constrain line capacity due to the length of the physical train detection sections.

ETCS Level 2 – Hybrid Train Detection (ETCS HTD), also previously called ETCS Hybrid Level 3, is one possible implementation of ETCS Level 2 (Baseline 4) that enables a further step towards increasing the line capacity for passenger and freight transport and reducing trackside equipment. It provides a hybrid form for the conventional trackside train detection performed by track circuits and axle counters on the one hand and train-based rear end detection and position reporting on the other. HTD will use the position report from the on-board equipment to evaluate whether the track sections are occupied or can be released in order to enhance the train detection functionality.

The fixed block sections of conventional trackside train detection (TTD) are further subdivided into virtual sub-sections (VSS); see fig. 1. This enables train operations with a significantly shorter headway without increasing the trackside equipment by using the existing infrastructure. The ETCS on-board equipment sends an extended position report to the Radio Block Centre (RBC) for this purpose. The Confirmed Train Length is provided based on the information received from external sources on the train's length and integrity, thereby indicating the train integrity confirmation [1]. This is therefore accompanied by the transfer of responsibility from the infrastructure manager to the railway undertaking, as the train integrity monitoring information no longer comes exclusively from the trackside equipment, but is also based on the on-board functions [6].

However, TTD systems implemented using axle counters or track circuits will continue to be used for trains that are not equipped with integrity monitoring, in fallback situations or to supervise critical

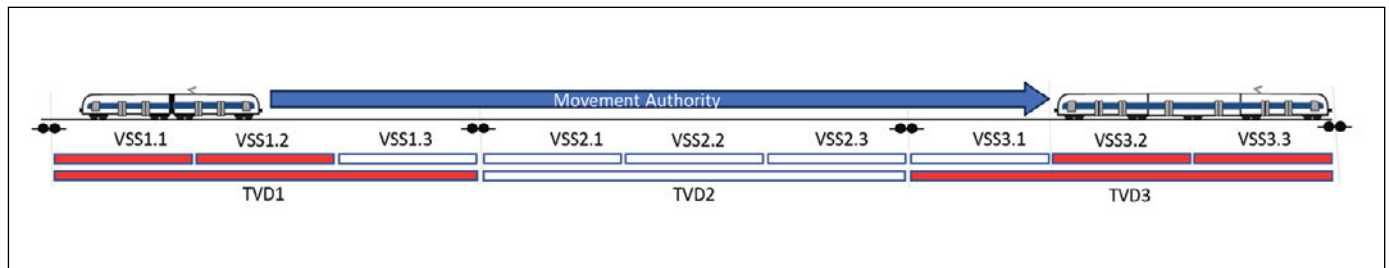


Bild 1: Grundprinzip von Hybrid Train Detection

Fig. 1: The basic principle behind Hybrid Train Detection

Quelle / Source: Siemens

ritätsinformation nicht mehr ausschließlich von der Infrastruktur kommt, sondern auch auf fahrzeugseitigen Funktionen basiert [6].

Dennoch werden TTD wie Achszähler und Gleisstromkreise auch weiterhin verwendet für nicht mit Zugintegritätsprüfung ausgestattete Züge, in der Rückfallebene oder um kritische Abschnitte wie Weichen, Nebengleise, Bahnübergänge, bewegliche Brücken und andere kritische Punkte zu überwachen.

Dies dient dazu:

- die streckenseitige Ausrüstung zu reduzieren, verglichen mit einer Vollausrüstung mit streckenseitiger Gleisfreimeldung
- die Leistungsfähigkeit zu erhöhen durch zusätzliche virtuelle Unterabschnitte
- den Betrieb mittels streckenseitiger Gleisfreimeldung aufrecht zu erhalten, wenn Zugposition und -integrität nicht gemeldet werden können.

2 Stand der Standardisierung (CCS TSI 2023)

Eine Aktualisierung der Control-Command and Signalling - Technical Specification for Interoperability (CCS-TSI), welche mehrere Change Requests (CRs) umsetzt, trat im September 2023 in Kraft. Mehrere dieser CRs wurden getrieben von dem steigenden Bedarf nach Lösungen wie HTD.

Die folgenden Abschnitte fassen kurz diejenigen CRs zusammen, die in der CCS TSI 2023 umgesetzt wurden und die für HTD-Anwendungen am bedeutsamsten sind.

2.1 Change Request 1342: Unpraktisches Nebeneinander der ETCS Level 2 und 3

CRs1342 wurde eröffnet wegen einiger Inkonsistenzen zwischen ETCS Level 2 und Level 3, wie sie in früheren Versionen der ETCS Systemanforderungsspezifikation (Subset-026) [1] definiert waren. Bei Betrachtung streckenseitiger Anwendungen wie HTD, die sowohl Züge mit als auch ohne Zugintegritätsprüfung bedienen können, war in den bestehenden Definitionen unklar, ob diese Strecken Level 2, Level 3 oder beiden zuzuordnen sind.

CRs1342 löste diese Zweideutigkeit letztendlich durch Löschung des Level 3 aus den ETCS-Spezifikationen bei gleichzeitiger Integration der Level-3-Funktionen in den Level 2. Das heißt, dass alle funkbasierten ETCS-Anwendungen als Level 2 eingeordnet werden, wobei es eine Option der streckenseitigen Implementierung ist, ob die Möglichkeit zur fahrzeugseitigen Zugintegritätsprüfung genutzt wird oder nicht.

Aus fahrzeugseitiger Sicht ist die Umsetzung der Zugintegritätsüberwachung (Train Integrity Monitoring System – TIMS) in Level 2 optional, aber der Infrastrukturbetreiber kann sie durch Festlegung entsprechender Streckenzugangskriterien im Infrastrukturregister (Register of Infrastructure – RINF) vorschreiben.

sections such as points, sidings, level crossings, movable bridges and other locations that are to be protected.

This approach aims to:

- reduce the trackside equipment compared with full equipment with TTD;
- improve performance by means of the virtual spacing of the new or existing track vacancy detection (TVD) sections;
- maintain operations with trackside equipment when the position and train integrity cannot be reported.

2 The state of the standardisation (CCS TSI 2023)

An update of the Control-Command and Signalling - Technical Specification for Interoperability (CCS-TSI) came into effect in September 2023 and implemented several change requests (CR) in the ETCS technical specifications. Several of these CR have been driven by the increasing demand for solutions such as HTD.

The following sections briefly summarise the CR implemented in CCS TSI 2023 that have the most relevance to HTD applications.

2.1 Change Request 1342: the impractical coexistence between ETCS Level 2 and Level 3

CR1342 was brought due to some inconsistencies in the definitions of ETCS Levels 2 and 3, as defined in previous versions of the ETCS System Requirements Specification (Subset-026) [1]. When considering trackside applications such as HTD, which can host trains both with and without integrity monitoring capabilities, it was not clear from the existing definitions whether such lines should be classed as Level 2, Level 3 or perhaps as a mixed level area.

CR1342 ultimately resolved these ambiguities by removing Level 3 from the ETCS specifications with the Level 3 functionality being incorporated into Level 2. This means that all radio-based ETCS applications will now be categorised as Level 2, whereby the trackside implementation has the option of using or not using the train integrity reports from the ETCS on-board equipment.

From the on-board point of view, the implementation of a train integrity monitoring system (TIMS) is optional in Level 2, but the infrastructure manager has the option of mandating its implementation by defining a line access condition in the Register of Infrastructure (RINF).

As a result of the removal of Level 3 from the ETCS specifications, the ERTMS Users Group has renamed the Hybrid Level 3 concept HDT.

2.2 Change Request 940: the minimum safe rear end position and position reporting ambiguities

CR940 provided a stronger basis for the deployment of interoperable HTD solutions by clarifying how the train integrity status is managed by the ETCS on-board equipment. The CR solution has estab-

Im Ergebnis der Streichung des Level 3 aus den ETCS-Spezifikationen benannte die ERTMS User Group das Hybrid Level 3 Konzept um in HDT.

2.2 Change Request 940: Zweideutigkeit der Minimum Safe Rear End Position und der Positionsmeldungen

CRs940 bietet eine stärkere Basis für die Entwicklung interoperabler HTD-Lösungen, indem klargestellt wurde, wie der Status der Zugintegrität seitens der ETCS-Fahrzeugeinrichtung zu verwalten ist. Die CRs-Lösung legt fest, dass die Zugintegritätsinformation, die an der Zugschnittstelle empfangen wird, drei Zustände einnehmen kann:

- Zugintegrität bestätigt
- Zugintegrität verloren gegangen
- Zugintegrität unbekannt.

Ein detailliertes Zustandsdiagramm ist in Subset-026 [1] definiert. Dieses beschreibt, wie die ETCS-Fahrzeugeinrichtung den Integritätsstatus an das RBC melden soll, basierend auf den von der Zugschnittstelle und anderen Informationsquellen erhaltenen Daten.

2.3 Change Request 1304: Fehlende Sicherheitsanforderungen für Level 3

Bevor im September 2023 die neue CCS TSI veröffentlicht wurde, enthielten die ETCS-Spezifikationen keine Sicherheitsanfor-

derungen, die die Zugintegritätsinformation, die an der Zugschnittstelle empfangen wird, drei Zustände einnehmen kann:

- Train integrity confirmed
- Train integrity lost
- Train integrity status unknown.

A detailed state machine is then defined in Subset-026 [1], describing how the ETCS on-board unit will report the integrity status information to the RBC, while considering the information received from the train interface, as well as any other criteria.

2.3 Change Request 1304: missing Level 3 safety requirements

Until the new CCS TSI came into force in September 2023, the ETCS specifications contained no safety requirements covering Level 3 (or what was known as Level 3 prior to CR1342). CR1304 was submitted to close this loophole and Subset-091 v4.0.0 [2] therefore now contains additional safety requirements that are relevant to HTD applications. They are detailed in Chapter 4.

3 New or enhanced trackside functions

HTD systems can integrate seamlessly into signalling systems, thereby providing essential data to control train movements and optimise railway operations. Fig. 2 illustrates the information exchange in an HTD system.

Trackside signals and/or boards and signs can be placed on the track to operate trains in a degraded mode or run trains that are not equipped for HTD. Hence, vehicles that are able to connect to the RBC, but are not equipped for HTD and vehicles that cannot connect to the RBC must be considered alongside vehicles that have been fitted for HTD operations. Timer functions have been introduced for these situations. They cause a fail-safe reaction on the affected parts of the track. The smart setting of the timers depending on the local circumstances can help optimise the train spacing and headway.

By implementing HTD, fixed block sections using TTD can be further divided into virtual subsections (VSS); see fig. 1. Given that the VSS statuses are not detected by any trackside equipment, trackside needs to implement VSS management that determines the VSS status using information from the RBC (based on the train's position reports) and interlocking. A virtual section can have four different states:

- Free – no train reported on the VSS and it is certain that the VSS is free.
- Occupied – an integer train is located on the VSS and it is certain that there is no other train behind in the same VSS.
- Ambiguous – a train is located on the VSS, but it is not certain that there is no other train behind in the same VSS.
- Unknown – no train is reported on the VSS, but it is not certain that the VSS is free.

Fig. 3 shows an example of how the train location is derived for a non-integer train. The position of the rear end can only be assumed since there is no positive confirmation of its location. Hence, the VSS where the train is located are ambiguous, and they change to unknown as they are left with the assumed rear end.

Fig. 4 shows an example of how the train location is derived for an integer train. The established rear end is derived from the estimated front end and the confirmed train length from the last position report with “integrity confirmed” as well as from the TTD. The functional safety requirements and associated risks related to safe vehicle location and track vacancy detection require a corresponding addition to the ERTMS/ETCS reference architecture

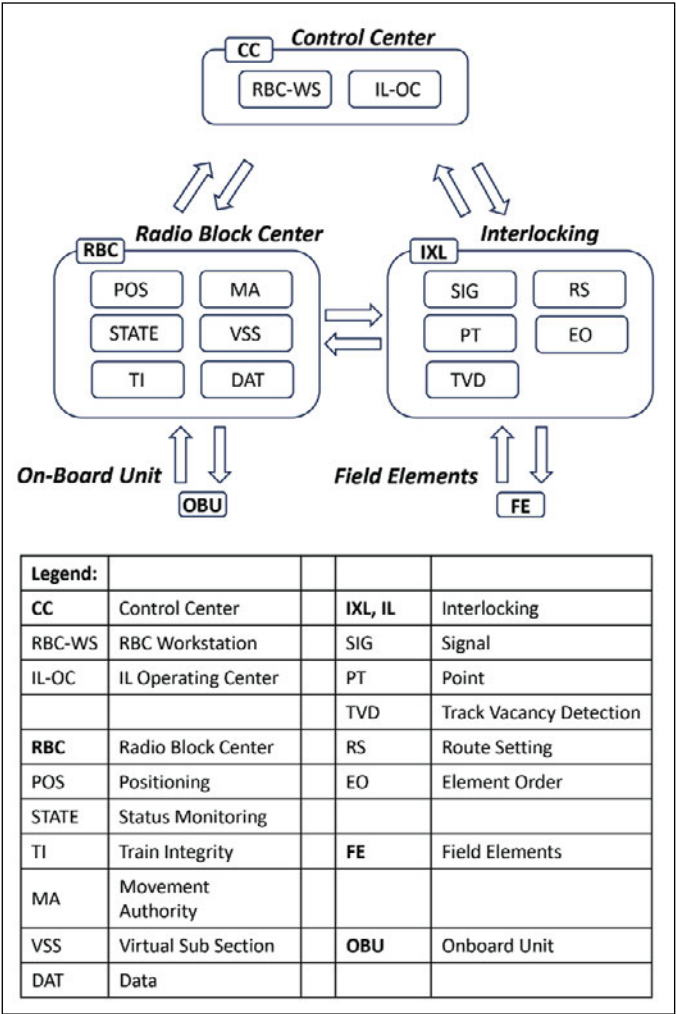


Bild 2: HTD-Informationsaustausch
Fig. 2: The HTD information exchange
Quelle / Source: Siemens

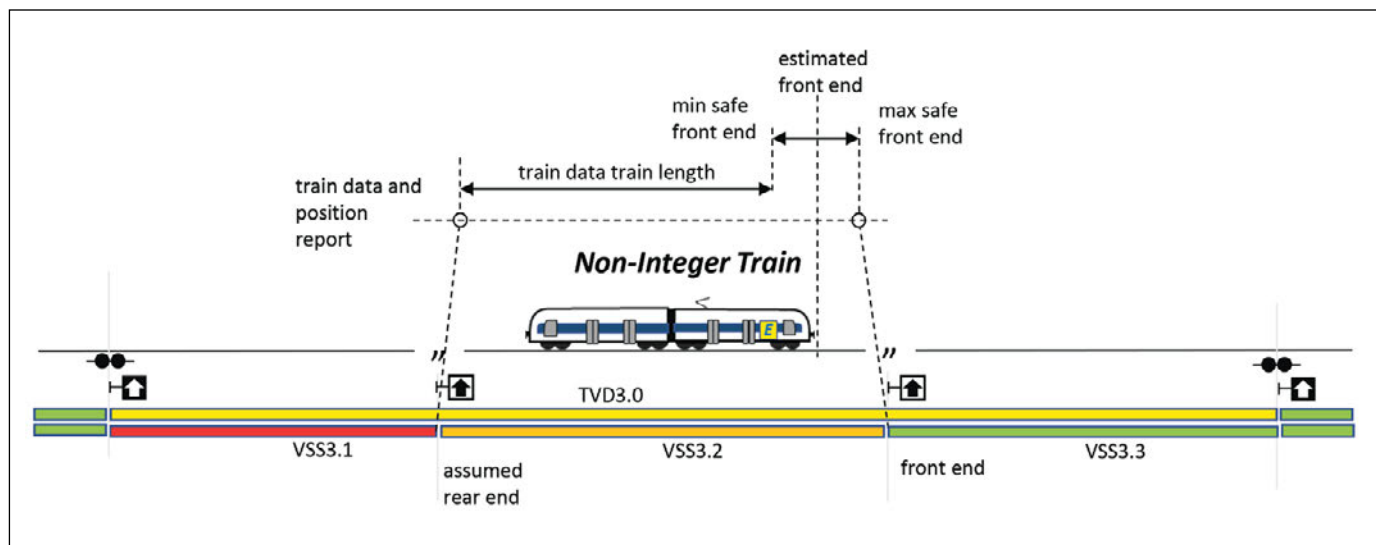


Bild 3: Zugortung für einen nicht integren Zug

Fig. 3: The train location for a non-integer train

Quelle / Source: [3]

derungen für Level 3 (oder was vor CRs1342 Level 3 genannt wurde). CRs1304 wurde aufgeworfen, um diese Lücke zu schließen, und im Ergebnis enthält Subset-091 v4.0.0 [2] jetzt zusätzliche Sicherheitsanforderungen, die für HTD-Anwendungen relevant sind. Diese sind in Kapitel 4 näher ausgeführt.

3 Neue und erweiterte streckenseitige Funktionen

HTD-Systeme können sich nahtlos in bestehende Systeme integrieren, indem sie notwendige Daten zur Steuerung von Zugfahrten zur Verfügung stellen und den Bahnbetrieb optimieren. Bild 2 zeigt den Informationsaustausch in HTD-Systemen.

Streckenseitige Signale und / oder Signaltafeln können weiterhin am Gleis aufgestellt werden für Züge, die nicht für HTD ausgerüstet sind, und als Rückfallebene. Daher müssen neben den Fahrzeugen, die für HTD ausgerüstet sind, sowohl solche Fahrzeuge berücksichtigt werden, die sich zwar mit dem RBC verbinden können, aber nicht für HTD ausgerüstet sind, als auch solche, die sich nicht mit dem RBC verbinden können. Für diese Situationen wurden Timer-Funktionen eingeführt, die eine Fail-Safe-Reaktion auf den betreffenden Streckenabschnitten einleiten. Eine ge-

(Subset-091 [2]). fig. 5 shows a graphical representation of the hazardous events within the ERTMS/ETCS reference architecture that are affected by the HTD functionality and that are assigned safety objectives in the form of tolerable hazard rates (THR).

4 The definition of safety targets

UNISIG Subset-091 Version 4.0.0 [2] defines two new safety targets related to HTD-specific functions: EXT_SR07 regarding the confirmed train length and EXT_SR08 regarding train integrity information:

a) EXT_SR08: Train integrity information shall be provided by external source with at least SIL2 quality.

This SIL2 safety requirement for the train integrity monitoring information provided to ETCS has been derived on the basis that an unsafe situation only arises when there has been a mechanical failure on the coupler i.e. a hazard only arises when there is a failure of the monitoring function AND a failure of the coupler. The statistics provided by the X2Rail-4 project, as cited in Subset-091 [2], indicate that unintended train separations occur with a frequency of $6.98E-5$ /h per freight train and $2.61E-6$ /h per passenger train [5]. A SIL2

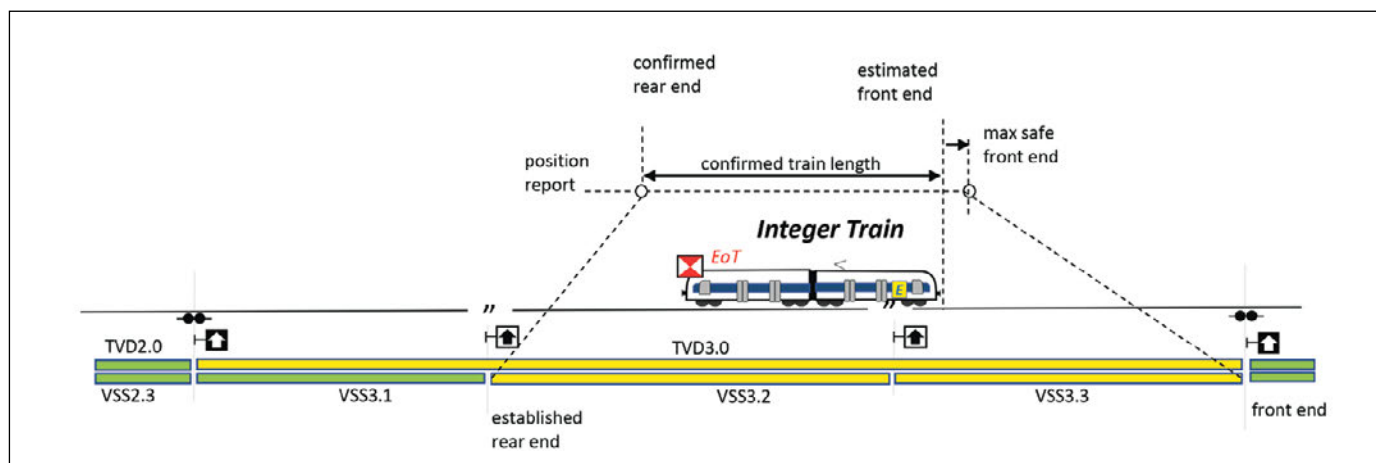


Bild 4: Zugortung für einen integren Zug

Fig. 4: The train location for an integer train

Quelle / Source: [3]

schickte Auswahl der Timer in Abhängigkeit von örtlichen Randbedingungen kann helfen, die Zugfolge zu optimieren.

Mit der Einführung von HTD können die festen Blockabschnitte mit TTD weiter unterteilt werden in virtuelle Unterabschnitte (VSS), siehe Bild 1. Da VSS nicht von der streckenseitigen Technik erkannt werden, muss die Streckenseite ein VSS-Management einrichten, das unter Nutzung von Daten des RBC (die wiederum auf den Zugpositionsmeldungen basieren) und des Stellwerks den Zustand der VSS-Abschnitte bestimmt. Ein virtueller Unterabschnitt kann vier unterschiedliche Zustände einnehmen:

- **Frei** – Es befindet sich sicher kein Zug in der VSS.
- **Besetzt** – Ein integrier Zug befindet sich in der VSS, und es ist sicher, dass sich kein weiterer Zug dahinter in derselben VSS befindet.
- **Mehrdeutig** – Ein Zug befindet sich in der VSS, aber es ist ungewiss, ob sich ein weiterer Zug dahinter in derselben VSS befindet.
- **Unbekannt** – Es ist kein Zug in der VSS bekannt, aber es ist auch nicht sicher, ob die VSS frei ist.

Bild 3 zeigt ein Beispiel, wie für einen nicht integren Zug die Zugortung bestimmt wird. Die Zugschlussposition kann nur vermutet werden, da es keine positive Bestätigung der Ortung gibt. Daher sind die VSS, wo sich der Zug befindet, nicht eindeutig und ändern sich in „unbekannt“, wenn das angenommene, hintere Ende den VSS verlässt.

Bild 4 zeigt ein Beispiel, wie die Zugortung für einen integren Zug bestimmt wird. Die Position des Established Rear End wird hergeleitet aus dem Estimated Front End und der Confirmed Train Length aus dem letzten Position Report mit bestätigter Integrität, wie auch aus den TTD.

Die funktionalen Sicherheitsanforderungen und damit zusammenhängenden Risiken in Bezug auf die sichere Zugortung und Gleisfreimeldung erfordern eine entsprechende Erweiterung der ERTMS/ETCS-Referenzarchitektur (Subset-091 [2]). Bild 5 zeigt eine grafische Darstellung der gefährlichen Ereignisse innerhalb der ERTMS/ETCS-Referenzarchitektur, die von der HTD-Funktion beeinflusst werden, und denen Sicherheitsziele in Form von tolerierbaren Gefährdungsraten (Tolerable Hazard Rates – THR) zugeordnet sind.

4 Definition der Sicherheitsziele

UNISIG Subset-091 Version 4.0.0 [2] definiert zwei neue Sicherheitsziele in Bezug auf HTD-spezifische Funktionen: EXT_SR07 zur bestätigten Zuglänge und EXT_SR08 zur Zugintegritätsinformation:

a) EXT_SR08: Die Zugintegritätsinformation soll von der externen Quelle mit mindestens SIL2-Qualität zur Verfügung gestellt werden. Diese SIL2-Anforderung für die Zugintegritätsüberwachung an das ETCS wurde hergeleitet aufgrund der Tatsache, dass ein unsicherer Zustand nur dann entstehen kann, wenn auch ein mechanischer Fehler in der Kupplung auftritt. Eine Gefährdung kann also nur entstehen, wenn gleichzeitig ein Fehler in der Überwachung UND ein Fehler der Kupplung vorliegen. Statistiken aus dem Projekt X2Rail-4, die in Subset-091 [2] zitiert sind, ergaben, dass unbeabsichtigte Zugtrennungen bei Güterzügen mit einer Rate von $6,98E-5$ /h und bei Personenzügen mit einer Rate von $2,61E-6$ /h auftreten [5]. Unter Nutzung des schlechteren Wertes ist ein SIL2-Sicherheitsziel für die Überwachungsfunktion gerechtfertigt.

b) EXT_SR07: Die Confirmed-Train-Length-Information, die im Position Report gesendet wurde, soll SIL4 entsprechen.

Gemäß Subset-026 [1] stellt die Confirmed Train Length den Abstand dar zwischen dem MIN Safe Rear End zu dem Zeitpunkt, als der Zug zum letzten Mal als integer gemeldet wurde, und dem

We create FRMCS.

Mission-critical communication solutions are our DNA. We drive regulatory work and define future communication standards.

Visit us at InnoTrans 2024
24-27 September
Berlin | Hall 4.1 | Booth 650

www.kontron.com/kttrdn

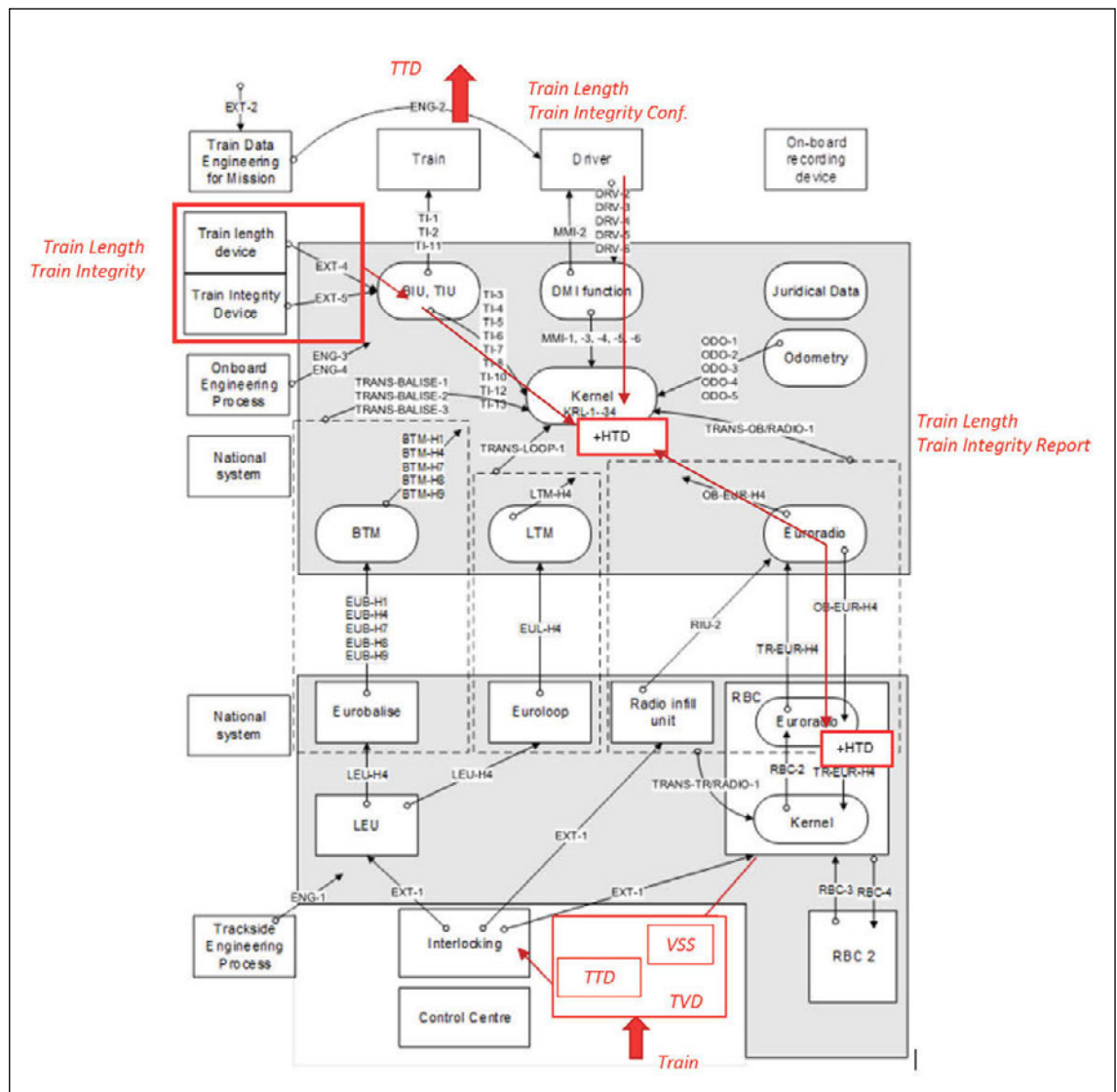
Kontron Transportation
Your trusted partner. Now. Tomorrow.



Bild 5: ERTMS / ETCS-Referenzarchitektur (Subset-091 v4.0.0 [2]) ergänzt um HTD-Funktionen

Fig. 5: The ERTMS / ETCS reference architecture (Subset-091 v4.0.0 [2]) amended by the HTD functionality

Quelle / Source: [2], ergänzt



Estimated Front End zu dem Zeitpunkt, wenn die Zugintegritätsinformation an das RBC gesendet wird, siehe Bild 6.

Im Gegensatz zum Zugintegritätsstatus, der nur im Fall eines Kupplungsfehlers relevant wird, wird die Confirmed Train Length immer dann von der Streckenseite zur Zugortung genutzt, wenn die Zugposition mit bestätigter Integrität gemeldet wird. Falls ein Fehler dazu führt, dass die Confirmed Train Length nicht die gesamte tatsächliche Länge des Zuges abdeckt, könnte die Streckenseite einen tatsächlich belegten Abschnitt als frei ansehen. Folglich kann ein Fehler in der Confirmed Train Length direkt zu einer Gefährdung führen, daher ist ein höheres Sicherheitsziel notwendig.

Eine HTD-Implementierung nutzt fahrzeugseitige Funktionen (insbesondere die Bestimmung der Zuglänge und die Zugintegritätsüberwachung), um Funktionen auszuführen, die vorher der streckenseitigen Gleisfreimeldung zugeordnet waren und die sich laut Bild 1 in Subset-091 [2] außerhalb der Harmonized Domain befinden. Daher kann ein Sicherheitsziel für „Ein VSS-Abschnitt wird als frei gemeldet, obwohl er tatsächlich besetzt ist“ weder Teil von ETCS_OB01 (0,67E-9 für ETCS Fahrzeugausrüstung ohne Übertragung) noch von ETCS_TR01 sein (0,67E-9 für ETCS Streckenausrüstung ohne Übertragung).

Unter Berücksichtigung der katastrophalen Konsequenzen eines möglichen Unfalls wurde aufgrund der Risikomatrix der EN 50126

safety target for the monitoring function can therefore be justified when using the more conservative value.

b) EXT_SR07: Confirmed train length sent in position report shall be of a quality corresponding SIL4.

According to Subset-026 [1], the Confirmed Train Length represents the distance between the min safe rear end at the time the train was last known to be integer and the estimated position of the train front at the time when the train integrity information is sent to the RBC, as illustrated in fig. 6.

In contrast to the train integrity status, which only becomes relevant when there has been a coupler failure, the Confirmed Train Length is used by the trackside to localise the train every time the train position is reported with confirmed integrity. If a failure results in the Confirmed Train Length that does not cover the full extent of the train, the trackside may consider the track to be clear when it is in fact physically occupied. Consequently, a higher safety target is required, given that a failure in the Confirmed Train Length information can directly result in a hazard.

An HTD trackside implementation relies on vehicle functions (in particular: the determination of the train length and train integrity supervision) to replace the functions of the trackside Train Detection Systems, which are classified as outside the harmonised domain (see fig. 1 in Subset-091) [2]. Therefore, a safety target for a “VSS sec-

eine eigene tolerierbare Gefährdungsrate von $1E-9$ für „sehr unwahrscheinlich“ festgelegt.

5 Methodik der Sicherheitsanalyse

Ein funktionsübergreifendes Team von Siemens an den Standorten Braunschweig, Berlin und Madrid mit Fachleuten aus den Bereichen ETCS, Bahnbetrieb und Sicherheit definierte die Benutzeranforderungsspezifikation, die Betriebsszenarien und die funktionalen Spezifikationen für ETCS HTD. Darauf aufbauend führte Informatik Consulting Systems GmbH (ICS) erstmals eine umfassende System-sicherheitsanalyse unter Einbeziehung sowohl der streckenseitigen als auch der fahrzeugseitigen Funktionen durch, um die Sicherheitsziele herzuleiten und klarzustellen.

Die europäischen Spezifikationen lassen noch viel Gestaltungsspielraum, was eine umfassende Analyse schwierig macht. Daher mussten Annahmen und Einschränkungen als Grundlage für die Analyse festgelegt werden, um den Umfang zu beschränken und dennoch für die wahrscheinlichen Umsetzungen anwendbar zu sein. Eine weitere Maßnahme, um den Umfang in sinnvoller Weise einzugrenzen, war, die Analyse auf solche Risiken zu fokussieren, die HDT-spezifisch sind, die also dadurch zusätzlich entstehen, dass HTD anstelle der klassischen Gleisfreimeldesysteme genutzt wird. Ziel war dabei, die Analyse anwendbar zu machen auf die vorgesehenen Migrationskonzepte von der reinen TTD-Ortung zu HTD.

Der erste Schritt der Analyse (Bild 7) diente dazu, Fehler zu identifizieren, die beim Betrieb in HTD auftreten können. Für eine Failure Mode and Effects Analysis (FMEA) wurden betriebliche Szenarien und Projektierungsrichtlinien [4] für HTD analysiert. Danach wurden alle identifizierten Fehler darauf bewertet, ob sie ein HTD-spezifisches Risiko generieren oder nicht.

Nach Identifizierung und Auswahl der relevanten Fehlerszenarien wurden diese als Gates in einer Fault Tree Analysis (FTA) verwendet, welche darauf abzielte, das gesamte HTD spezifische Risiko zu quantifizieren.

Das Top-Level-Ereignis repräsentiert die Wahrscheinlichkeit des HTD-spezifischen Risikos, dass die Zugererkennung gefährlich ausfällt, welches sich aus der Summe der Wahrscheinlichkeiten der Fehlerszenarien ergibt.

Die Fehlerszenarien wiederum setzen sich aus Basisereignissen zusammen, die zusammentreffen müssen, damit das Fehlerszenario eintritt. Die Basisereignisse bestehen aus den initialen Fehlerereignissen und dem Ausfall der mitigierenden Sicherheitsfunktionen. Die mitigierenden Funktionen wurden ausgewählt vor dem Hintergrund, dass die Analyse auf zu erwartende HTD-Implementierungen anwendbar sein soll. Sie beinhalten Sicherheitsfunktionen von ETCS (z.B. ein externes Gerät zur zusätzlichen Bestimmung der Zuglänge) wie auch Systeme nach dem Stand der Technik (z.B. Bremsen und Achszähler).

Die Analyse basierte auf Subset-091 Version 3.9.2. Zwischenzeitlich wurde der CRs 1304 in Version 4.0.0 umgesetzt, siehe Bild 7.

6 Ergebnis: Identifizierung der gefährlichen Szenarien

Der Fehlerbaum, der in der Sicherheitsanalyse erzeugt wurde, kann die Frage beantworten, ob und unter welchen Bedingungen das Sicherheitsziel erreicht wird, indem dieses mit dem TOP-Ereignis verglichen wird. Weiterhin können die Teilfehlerbäume analysiert werden, um spezielle gefährliche Szenarien genauer zu betrachten und festzustellen, wie kritisch diese sind.

Die Analyse identifizierte die folgenden gefährlichen Szenarien mit spezifischen HTD-Funktionen:

Sicher. Modular. Und für die digitale Schiene.

Unsere modulare Steuerungsplattform revolutioniert die Bahnindustrie und ermöglicht eine digitale Transformation. Von der Überwachung und Steuerung von Bahnübergängen bis hin zur elektrisch ortsgesteuerten Weiche (EOW) und dem EULYNX Object Controller bieten wir eine flexible Plattform, die sich Ihren individuellen Anforderungen anpassen lässt. Investieren Sie jetzt in die zukünftige Automatisierung der Bahn und profitieren Sie von innovativen, sicheren und digitalen Lösungen. Mit Pilz sicher und zuverlässig unterwegs in die digitale Zukunft!



Jetzt mehr erfahren!

PILZ
THE SPIRIT OF SAFETY

Pilz GmbH & Co. KG
Tel.: 0711 3409-0, info@pilz.de, www.pilz.de

InnoTrans

24.–27. September 2024

Halle 27, Stand 550

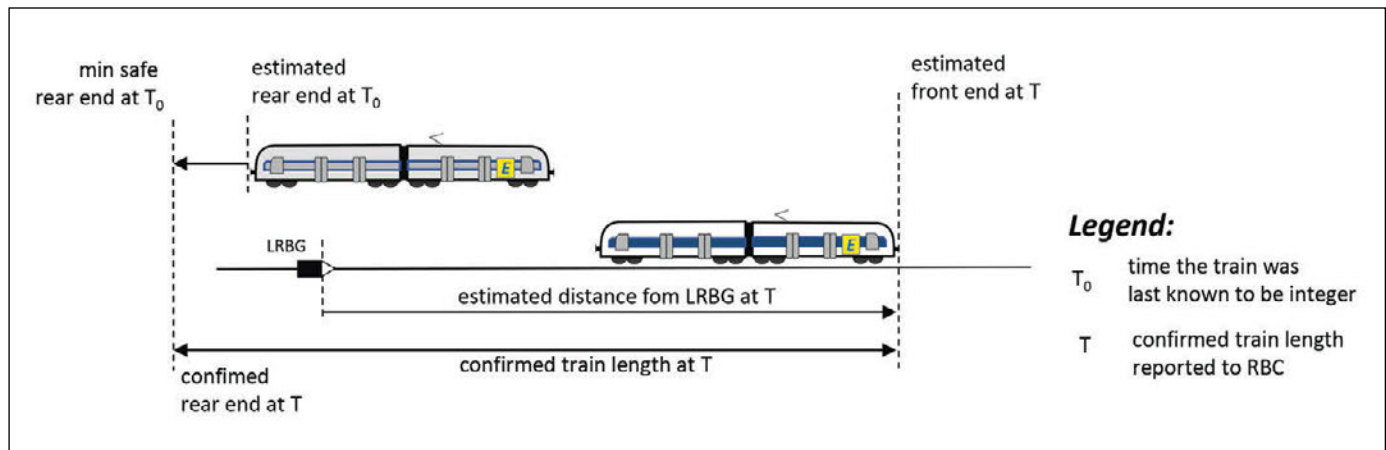


Bild 6: Die Confirmed Train Length informiert das RBC, wo sich das MIN safe rear end des Zuges befand, als der Zug zuletzt als integer gemeldet wurde.

Fig. 6: The Confirmed Train Length information informs the RBC where the minimum safe rear end of the train was located at the time when the train was last known to be integer. Quelle / Source: [1]

1. unerwartete und unerkannte Zugtrennung, die zur Kollision eines anderen Zuges mit dem zurückgebliebenen Zugteil führt
2. unerkanntes Zurücklassen eines Zugteils bei einer beabsichtigten Zugteilung (Flügelbetrieb)
3. falsche Eingabe der Zuglänge beim Start, was zur zu frühen Freigabe des Abschnitts hinter dem Zug führt
4. Schattenzug: Ein zweiter, nicht verbundener Zug versteckt sich hinter einem verbundenen Zug in der Startphase.

Nicht nur eine zu kurze Bestimmung der Zuglänge (d. h. der Zug ist tatsächlich länger als ermittelt wurde) kann gefährlich sein (Szenario 3), sondern im Zusammenhang mit dem Schattenzug-Szenario (Szenario 4) auch eine zu lange Bestimmung der Zuglänge:

- Szenario 3 erfordert die Umsetzung des CRs1304 für eine sicherere Bestimmung der Zuglänge entweder durch streckenseitige Maßnahmen (z. B. Achszähler an bestimmten Punkten) oder durch eine unabhängige zweite fahrzeugseitige Informationsquelle für die Bestimmung der Zuglänge (siehe Kapitel 7). Die Projektierungsrichtlinien [4] geben Hinweise, welche Bereiche mit streckenseitiger Gleisfreimeldung ausgerüstet werden sollten.
- Zu Szenario 4 sind in der spezifischen Anwendung Betrachtungen unter Einbeziehung der Gleislagepläne, Signallagepläne, Betriebsregeln und Zuggarnituren notwendig, um das Risiko von Schattenzug-Szenarien zu bewerten und zu minimieren oder auszuschließen.

Die anderen Szenarien 1 und 2 sind bereits durch Befolgen der aktuellen ETCS TSI hinreichend unwahrscheinlich.

7 Technische Umsetzung für Vollbahnanwendungen

Um den hohen Sicherheitsanforderungen des Subset-091 [2] an eine Berechnung und Übermittlung der Train Integrity Information zu genügen, sind fahrzeugseitig unterschiedliche Architekturvarianten angedacht. Insbesondere die in hoher Qualität (SIL4) geforderte Ermittlung der Confirmed Train Length hat dabei einen entscheidenden Einfluss auf die Randbedingungen der Umsetzungsstrategie. So geht die reale Zuglänge auf der Grundlage der ETCS Train Data gemäß CRs940 (siehe auch Abschnitt 2) in die Berechnung mit ein.

Abgesehen vom European Vital Computer (EVC) als Quelle eines statisch vorkonfigurierten/validierten Wertes kann eine SIL4-

tion is reported as being free even though it is physically occupied" is part neither of ETCS_OB01 (0.67E-9 for ETCS on-board without transmission) nor ETCS_TR01 (0.67E-9 for ETCS trackside without transmission).

A tolerable hazard rate of 1E-9 has been defined ("highly improbable") for the specific HDT functions based on the risk matrix from EN 50126 and considering the catastrophic consequences of a possible accident.

5 The methodology of the HTD safety analysis

A cross-functional team from Siemens in Braunschweig, Berlin and Madrid, including key experts in ETCS, train operation and safety, has defined the ETCS HTD user requirement specification, operating modes and functional specifications. For the first time, a comprehensive system safety analysis, including both trackside and onboard functions, has been conducted by the Informatik Consulting Systems GmbH (ICS) in order to derive and clarify the safety targets.

The European specifications still leave a lot of design space open, which makes a comprehensive analysis difficult. A set of assumptions/limitations has been introduced as the basis of the analysis with the intent of limiting its scope and still applying to any likely HTD implementations. The analysis aims to derive and analyse only HTD specific risks (risks that are introduced or exacerbated using HTD instead of "classical" train detection systems) as another way of meaningfully limiting the scope. The goal was to make the analysis feasible and applicable to common concepts on how to migrate to HTD from pure trackside TTD systems.

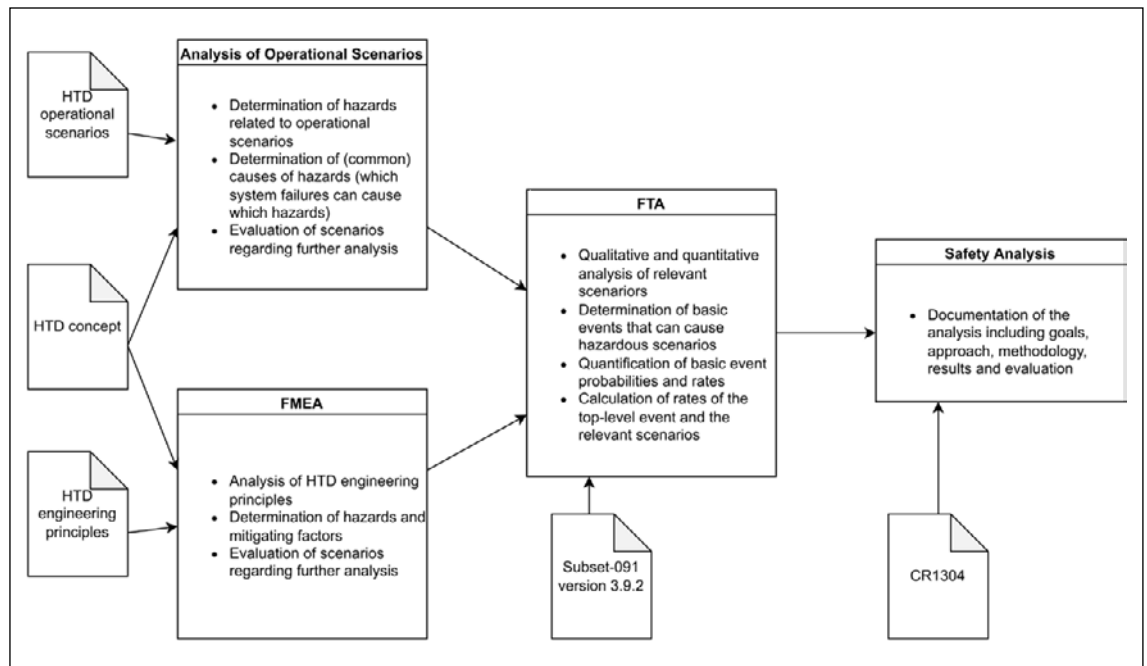
The first step of the analysis (fig. 7) was aimed at identifying any failures that can occur during operations in HTD. Operating scenarios in the HTD context and the HTD Engineering Guidelines [4] were analysed using a Failure Mode and Effects Analysis (FMEA). After completing this step, all the identified failures were evaluated to see whether they fitted the aforementioned criteria of causing an HTD-specific risk or not.

After identifying and choosing the relevant failure scenarios, they were used as gates in a Fault Tree Analysis (FTA), which aimed to quantify the total HTD-specific risk. The top-level event, which represents the HTD-specific risk for train detection to fail critically, is calculated as the sum of all the failure scenario probabilities.

Bild 7: Informationsfluss in der Analyse

Fig. 7: The information flow of the analysis

Quelle / Source: ICS GmbH



Qualität im Hinblick auf eine betrieblich erwünschte dynamische Quelle (z. B. im Kontext des Anwendungsfalles Kuppeln / Entkuppeln) initial nicht angenommen werden. Dies gilt insbesondere für eine gemäß Subset-091 [2] legitimierte externe Quelle wie die Fahrzeugsteuerung. Dafür rückt neben einer reinen ETCS-Lösung, die beispielsweise eine fahrzeugübergreifende EVC-EVC-Kommunikation nutzt, eine den Randbedingungen des Subset-091 [2], EXT_SR07 genügende Lösung in den Fokus. Diese sieht einen sicheren Vergleich von funktional unabhängig erzeugten, sicheren Inputs aus unterschiedlichen Quellen vor. Dafür bietet sich eine Ermittlung und Bereitstellung der Confirmed Train Length in SIL4-Qualität durch den EVC an, die dann auf dem sicheren Vergleich von unterschiedlichen Werten für die Zuglängen basiert.

The probability of a scenario is determined by the basic events that have to coincide for the scenario to occur. The basic events consist of initial failure events and the failure of any mitigating safety functions.

The mitigating safety functions were chosen while keeping in mind that the analysis should be applicable to common, possible HTD implementations. These include the safety functions required by ETCS (e.g. an external device that determines the train length) and common state-of-the-art systems (e.g. brakes and axle counters).

The probability for the basic events was based on version 3.9.2 of Subset-091 and the SIL for state-of-the-art technologies. CR 1304 has been implemented in version 4.0.0 in the meantime (fig. 7).



InnoTrans 2024
24-27 SEP 2024
THE FUTURE OF MOBILITY



»Entdecken Sie die nächste Generation.«

Vorbeikommen und eine bahnbrechende Innovation entdecken.

Halle 25 | Stand 525

MESSE BERLIN GMBH
EXPOCENTER CITY | MESSEDAMM 22, 14055 BERLIN

esa-grimma.de

Diese werden auf unabhängigen Datenpfaden erzeugt und übermittelt, z. B. Zugsteuerung über ETCS TIU und ETCS-Zugdateneingabeverfahren über ETCS Fahrzeugeinrichtung (EVC, Driver Machine Interface – DMI), wie in Bild 9 dargestellt.

Für das Zugdateneingabeverfahren gemäß Subset-026 [1] ist dabei eine spezifizierte Eingabe, Bestätigung und Validierung der am DMI eingegebenen Zugdaten durch den Triebfahrzeugführer (Tf) vorgesehen. Dabei gilt es sicherzustellen, dass sowohl für die optionale Verwendung von Vorschlagswerten am DMI als auch für die durch den Tf genutzten Eingangsinformationen die erforderliche Unabhängigkeit zu den im ETCS TIU Datenpfad genutzten sicheren Inputs vorliegt. Bei erfolgreichem Vergleich der unabhängig ermittelten und übertragenen Zuglängen sowie Ermittlung und Bereitstellung der Confirmed Train Length durch den EVC sind die fahrzeugseitigen Randbedingungen an einen ETCS Level 2 HTD erfüllt.

Schlägt der sichere Vergleich der unabhängig ermittelten und übertragenen Zuglängen im EVC fehl, so wird der Tf darüber informiert und kann die Eingabe wiederholen. Die Anzahl der möglichen Wiederholungen richtet sich an den Randbedingungen der betrieblichen Risikoanalyse des Betreibers aus und führt bei Überschreitung der erlaubten Fehlversuche zu einer Anzeige des unabhängig erzeugten und übermittelten Wertes der Fahrzeugsteuerung. Die Validierung dieses Wertes durch den Tf führt dabei in jedem Fall zu einem Übergang in den ETCS Level 2. Die fahrzeugseitigen Randbedingungen an einen ETCS Level 2 HTD sind in diesem Fall nicht erfüllt.

8 Zusammenfassung

HTD wurde spezifiziert, um streckenseitige Gleisfreimeldung mit fahrzeugseitiger Zuglängenbestimmung und -integritätsprüfung zu kombinieren. Es ermöglicht die Reduzierung der Streckenausrüstung und erhöht die Effizienz des Betriebs auf der Strecke.

6 The results: identified hazardous scenarios

The fault tree constructed during the safety analysis can answer the question as to whether the safety target has been met by comparing it with the top-level event. Furthermore, the sub-trees can be analysed to look at specific hazardous scenarios and to figure out how critical they are.

The analysis identified the following hazardous scenarios with specific HTD functions:

1. An unintended and undetected train split leading to a collision between another train and the train part that has been left behind.
2. An undetected train part left behind after joining and splitting.
3. The incorrect initial entry of the train length, leading to the early release of the track sections behind the train.
4. A shadow train: a second, unconnected train hides behind the connected train in the start-up phase.

Not only can the overly short indication of a train's length (the train is actually longer than the indicated train length) be dangerous (Scenario 3), but so too can an overly long indication of the train's length within the context of the shadow train scenario (Scenario 4):

- Scenario 3 requires the implementation of CR1304 for a safer definition of the train length either using trackside solutions (e.g. axle counters) or an additional independent, on-board source of train length information (see Chapter 7). Engineering Guideline [4] gives hints as to which areas should be supervised by trackside train detection.
- In order to mitigate Scenario 4, considerations based on the local track layout, signalling layout, operating rules and train sets must be made in the specific application in order to evaluate and minimise or exclude the risk of any shadow train scenarios.

The other Scenarios 1 and 2 were found to be sufficiently mitigated hazards following the current ETCS TSI.

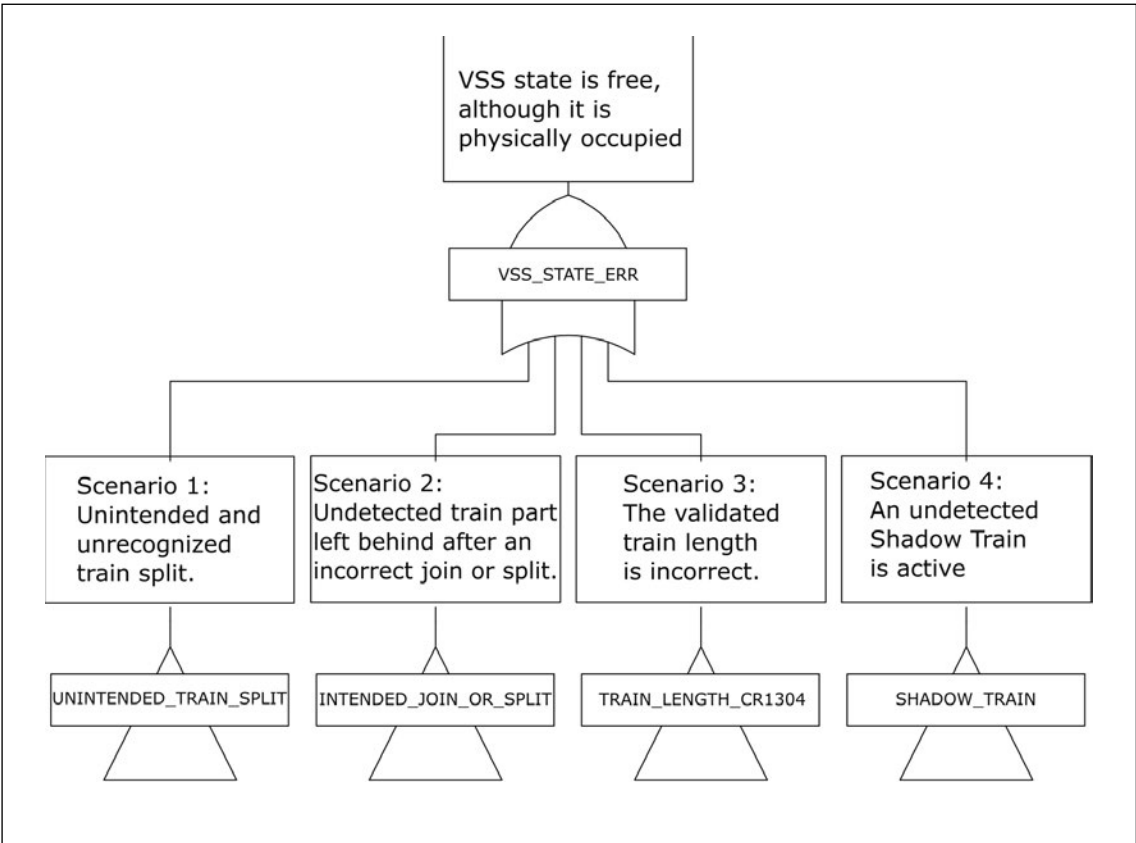


Bild 8: TOP-Fehlerbaum
Fig. 8: The TOP fault tree
Quelle / Source: ICS GmbH

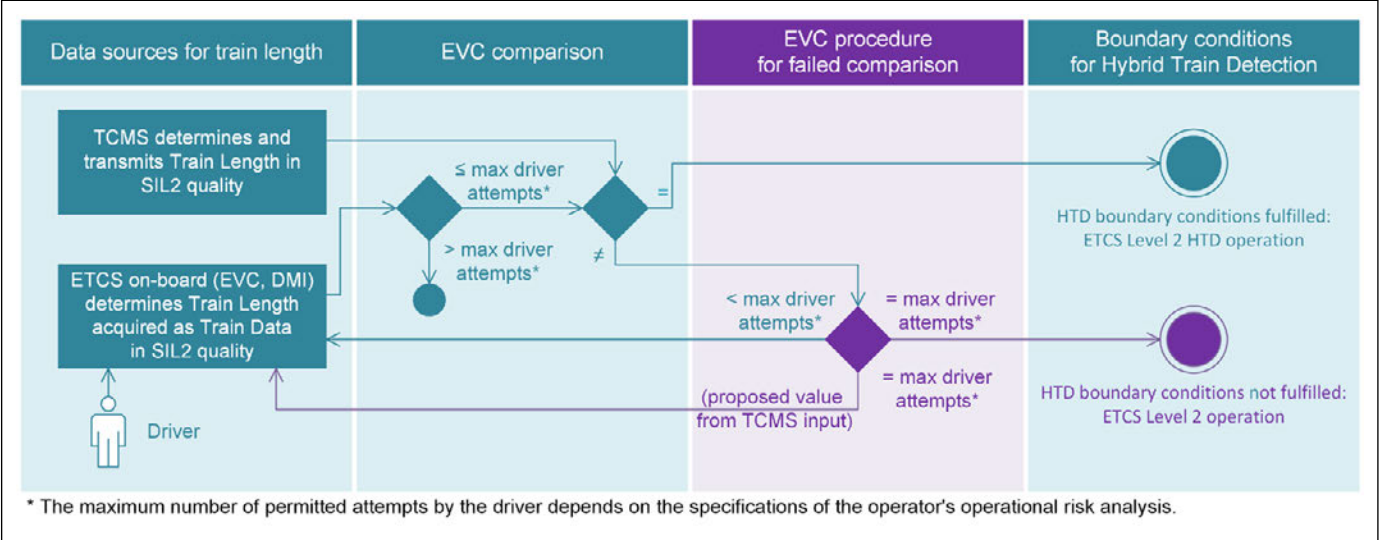


Bild 9: Randbedingungen für Hybrid Train Detection am Beispiel der Zuglänge

Fig. 9: The boundary conditions for Hybrid Train Detection using the example of train length

Quelle / Source: Siemens

Eine Analyse wurde durchgeführt und zeigt, dass ausreichende Betriebssicherheit unter HTD möglich ist. Vier wesentliche gefährliche Szenarien wurden identifiziert:

- unbeabsichtigte Zugtrennung
- Zurücklassen eines Zugteils beim Flügelbetrieb
- falsche Eingabe der Zuglänge
- Schattenzug hinter einem verbundenen Zug.

Um diese Gefährdungen zu beherrschen, sind zusätzliche fahrzeugsbasierte Maßnahmen zur sicheren Bestimmung der Zuglänge in Entwicklung und Umsetzung. Einerseits gibt es einen Bedarf nach projektspezifischen Maßnahmen zur Reduzierung des Risikos von Schattenzügen. Herkömmliche TTD sollte weiterhin verwendet werden, um bestimmte Gefährdungen zu beherrschen, wie dies in den Projektierungsrichtlinien [4] empfohlen wird. Außerdem schlagen diese Richtlinien Werte für Timer-Funktionen vor, um bestimmte Gefährdungen zu beherrschen.

7 The technical implementation for mainline applications

Different architecture variants are being considered on the vehicle side in order to meet the high safety requirements of Subset-091 [2] for the calculation and transmission of train integrity information (see section 4). The determination of the Confirmed Train Length required at a high quality (SIL4) has a particularly decisive influence on the boundary conditions for the implementation strategy. The real train length is included in the calculation based on the ETCS Train Data in accordance with CR940 (see section 2). Aside from the European Vital Computer (EVC) as the source of a statically preconfigured/validated value, no SIL4 quality with regard to an operationally desired dynamic source (e.g. within the context of a coupling/uncoupling use case) can initially be assumed. This particularly applies to an external source legitimised in accordance with Subset-091 [2] such as the train control and monitoring sys-

Sichere Digitalisierungslösungen für die Mobilität!

Bahnbetriebliche IP-Netze

Cybersecurity für Bahn & ÖPNV

Übertragungsnetz-lösungen

Digitalisierung durch sichere Vernetzung

Lassen Sie uns sprechen!

24.-27. September 2024

InnoTrans



Halle 4.1 | Stand 440

Wir stellen die Weichen auf Zukunft!

telent
service • commitment • value
www.telent.de

Autoren-Belegexemplar, Herr Theeg, Siemens Mobility GmbH. Weitergabe an Dritte urheberrechtlich untersagt.

Die Analyse basierte auf der zum Zeitpunkt neuesten ETCS Baseline 3 und vorgeschlagenen CRs. Die neue Baseline 4 setzt einige dieser CRs um. HTD kann als eine Umsetzung von ETCS Level 2 in Baseline 4 angesehen werden.

Diese Analyse bildet eine Basis für erste Anwendungsprojekte mit HTD, die derzeit in Umsetzung sind. ■

LITERATUR | LITERATURE

- [1] ERTMS/ETCS Subset-026: System Requirements Specification, v4.0.0
- [2] ERTMS/ETCS Subset-091: Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, v3.9.2 & v4.0.0
- [3] Principles ERTMS/ETCS Hybrid Train Detection; Ref 16E042, Version 1F; 2022-12-20
- [4] 80. ERTMS/ETCS Hybrid Train Detection Engineering; Ref 21E087, Version -3; 2022-12-09
- [5] X2Rail-4 Deliverable D6.1 "Results of feasibility studies and laboratory tests for candidate technologies selection and adaptation of existing solutions", 2020-10-12
- [6] Hetzer, M.; Kriener, J.; Unger, R.; Voß, J.H.: Bringing ETCS Level 3 into operation from an onboard perspective, SIGNAL+DRAHT 07-08/2022, p. 29-36

AUTOREN | AUTHORS

Dr. Gregor Theeg

RAMS Manager Mainline
Siemens Mobility GmbH
Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig
E-Mail: gregor.theeg@siemens.com

Craig McLellan

Key Expert ERTMS Principles
Siemens Mobility GmbH
Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig
E-Mail: craig.mclellan@siemens.com

Heiko Saalbach

RAMS Manager Mainline
Siemens Mobility GmbH
Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig
E-Mail: heiko.saalbach@siemens.com

Dr. Frank Wend

RAMS Manager Mainline (retired / im Ruhestand)
Siemens Mobility GmbH
E-Mail: frank.wend@freenet.de

Martin Hetzer

RAMS Manager ATP On-board
Siemens Mobility GmbH
Anschrift / Address: Kieffholzstraße 44, D-12435 Berlin
E-Mail: martin.hetzer@siemens.com

Lorenz Giese

RAM and functional Safety Engineer
Informatik Consulting Systems GmbH
Anschrift / Address: Kreuzstraße 12, D-04103 Leipzig
E-Mail: lorenz.giese@ics-gmbh.de

Martin Haase

RAM and functional Safety Engineer
Informatik Consulting Systems GmbH
Anschrift / Address: Kreuzstraße 12, D-04103 Leipzig
E-Mail: martin.haase@ics-gmbh.de

tem (TCMS). Therefore, the focus is on a solution that meets the boundary conditions of Subset-091 [2], EXT_SR07 in addition to a pure ETCS solution that uses, for example, EVC-EVC communication across vehicles. This provides for a safe comparison of the functionally independently generated, safe inputs from different sources. This can be achieved by the EVC determining and providing the Confirmed Train Length based on a safe comparison of the train length values. These are generated and transmitted on different, independent data paths, e.g. TCMS via ETCS TIU and the ETCS train data entry procedure via ETCS on-board equipment (EVC, Driver Machine Interface – DMI) as shown in fig. 9.

The input, confirmation and validation of the train data entered on the DMI by the train driver is specified for the train data entry procedure in accordance with Subset-026 [1]. It must be ensured that the required independence from the safe inputs used in the ETCS TIU data path exists both for the optional use of any default values on the DMI and for the input information used by the train driver.

If the independently determined and transmitted train lengths are successfully compared and the Confirmed Train Length is determined and provided by the EVC, the on-board boundary conditions for ETCS Level 2 HTD are fulfilled.

If the safe comparison of the independently determined and transmitted train lengths in the EVC fails, the driver is informed and can repeat the entry. The maximum number of permitted attempts is based on the boundary conditions for the operator's operating risk analysis and leads to the display of an independently generated value transmitted from the train control and monitoring system (TCMS) if the permitted number of failed attempts is exceeded. The validation of this value by the train driver always leads to a transition to ETCS Level 2. However, the on-board boundary conditions for ETCS Level 2 HTD are not met in this case.

8 Conclusion

HTD has been specified as a means of combining trackside train detection with on-board equipment that reports a train's position and integrity. It allows for a decreased need for trackside equipment and increases the efficiency of operations on the tracks.

An analysis has been conducted that shows that sufficient operating safety is achievable under HTD. Four main hazards have been identified:

- unintended train splits;
- leaving behind train parts during planned joining and splitting;
- the incorrect entry of the train length information;
- a shadow train behind a connected train.

In order to control all these hazards, additional train-based measures for the safe determination of the train length are under development and implementation. On the other hand, there is also a need for project-specific measures to minimise any shadow train risks. Conventional TTD should still be used to avoid certain hazards as recommended by the HTD Engineering Guidelines [4]. Furthermore, these Guidelines suggest specific parameters for the timer functions that mitigate some of the hazards.

The analysis was based on the latest ETCS Baseline (Baseline 3) and the proposed CR. The new Baseline 4 incorporates some of these CR. HTD can be considered an implementation of ETCS Level 2 in ETCS Baseline 4.

This analysis forms a basis for the first implementation projects with HTD that are currently in progress. ■