Verslag over het verzoek om informatie inzake ERTMS Cold Movement Detection en de ERTMS Train Integrity Monitor

Voor extern gebruik

Datum 1 juni 2015

Inhoud

Samenvatting

Op 11 april 2014 heeft het kabinet een voorkeursbeslissing genomen voor de uitrol van ERTMS Level 2 op de drukste corridors van het spoorwegnetwerk. Op dit moment bevindt het ERTMS-programma zich in de planuitwerkingsfase. In deze fase worden onder meer de specificaties voor diverse onderdelen opgesteld.

Wat de uitrol betreft, is er voor een aantal functies tot nu toe nog geen operationele ervaring opgedaan in de bestaande ERTMS-implementaties in Nederland. Tot die functies behoren de Cold Movement Detection (CMD) en de Train Integrity Monitor (TIM). De specificaties van deze functies vallen deels buiten het toepassingsgebied van de ERTMS-specificaties van de EU zoals neergelegd in de TSI CCS. Daarom zijn binnen het kader van het ERTMS-programma aanvullende specificaties opgesteld en is er een aantal vragen aan de UNISIG-partijen gesteld om te evalueren of de betreffende vereisten geschikt zijn voor het beoogde doel. Zeven van de acht aangeschreven bedrijven hebben een antwoord gegeven.

Het besluit of (één van) deze functies wordt geïmplementeerd is nog niet genomen, evenals de keuze over welke baseline. Dit verzoek om informatie dient als nadere beschouwing van deze functies te worden bezien..

In hun reactie geven de UNISIG-partijen aan dat zij werken aan oplossingen voor CMD aangezien deze functie deel uitmaakt van de ERTMS-specificaties van baseline 3. De uitdagingen bij het voldoen aan de voorgeschreven specificaties liggen vooral op het gebied van de stroomvoorziening en de vraag of er vaste of variabele instelwaarden ten aanzien van toegestane beweging zijn toegestaan. Diverse bedrijven hebben opgemerkt dat een aantal specificaties (betrouwbaarheid en veiligheid) op treinniveau ingesteld zouden moeten worden en niet op subsysteemniveau.

Alle UNISIG-partijen die gereageerd hebben gaven aan dat zij bezig zijn met het uitwerken van een of meer oplossingen voor de TIM. De grootste uitdagingen worden verwacht bij het verstrekken van de informatie over de treinlengte op basis van SIL 4 in combinatie met de eis dat dit voor alle denkbare combinaties van treinsamenstellingen mogelijk moet zijn. Aan de eis met betrekking tot de informatie over treinintegriteit is daarentegen redelijk eenvoudig te voldoen. De specificaties op subsysteemniveau (deel B) beperken de mogelijkheden voor de toeleveringssector om oplossingen te ontwikkelen die in meer Europese landen ingevoerd kunnen worden.

De verkregen antwoorden en opmerkingen worden gebruikt om de specificaties voor CMD en de TIM te verbeteren. De verstuurde specificaties zijn in dit verslag opgenomen en zijn dus nog aan verandering onderhevig.

1 Inleiding en vragen

Op 11 april 2014 heeft het kabinet een voorkeursbeslissing genomen voor de uitrol van ERTMS Level 2 in de drukste corridors van het spoorwegnetwerk. De Engelse versie van die beslissing is hier[1] te vinden. Op dit moment bevindt het Programma ERTMS zich in de planuitwerkingsfase, de fase waarin ook het systeemontwerp plaatsvindt. In die planuitwerkingfase worden onder meer de specificaties voor diverse onderdelen opgesteld

Wat de uitrol betreft, is er voor een aantal functies tot nu toe nog geen operationele ervaring opgedaan in de bestaande ERTMS-implementaties in Nederland. Tot die functies behoren onder meer de Cold Movement Detection (CMD) en de Train Integrity Monitor (TIM).

Het besluit of (één van) deze functies wordt geïmplementeerd is nog niet genomen, evenals de keuze over welke baseline. Dit verzoek om informatie dient als nadere beschouwing van deze functies te worden bezien..

De specificaties van deze functies vallen deels buiten de ERTMS-specificaties van de EU zoals neergelegd in de huidige TSI CCS. Dat betekent dat er aanvullende specificaties opgesteld kunnen worden. Die specificaties zijn in het kader van het Programma ERTMS in Nederland opgesteld. Daarbij is een aantal vragen aan systeemleveranciers van ERTMS gesteld om te evalueren of de betreffende specificaties geschikt zijn voor het beoogde doel.

Dit verslag bevat openbare informatie over dit verzoek om informatie, evenals een geanonimiseerde samenvatting van de ontvangen gegevens.

1.1 Procedureverloop van het verzoek om informatie

Op 12 januari 2015 zijn twee documenten met vragen en specificaties inzake CMD en de TIM per e-mail aan alle leden van UNISIG gestuurd. De opgestuurde specificaties zijn in dit document opgenomen (hoofdstuk 3 en 4). De specificaties zijn in de Engelse taal geschreven.

UNISIG is een industrieel consortium dat is opgericht om de technische specificaties voor het ERTMS/ETCS te ontwikkelen. Als Associated Member van UNIFE, een erkende stakeholder, levert UNISIG een actieve bijdrage aan de activiteiten van het Europees Spoorwegebureau (European Railway Agency- ERA) op het gebied van de technische specificaties voor het ERTMS/ETCS (bron: www.ertms.net).

Er zijn op dit moment acht marktpartijen lid van UNISIG, te weten: Alstom, AnsalsoSTS, AZD Praha, Bombardier, CAF; Mermec Group, Siemens en Thales.

Op 13 februari 2015 hadden zeven van de acht leden een reactie gestuurd. Op diezelfde dag heeft er een bijeenkomst met een van die leden plaatsgevonden. De tijdens die bijeenkomst verstrekte informatie is verwerkt in de geanonimiseerde samenvatting in hoofdstuk 2.

[1] https://www.rijksoverheid.nl/documenten/rapporten/2014/04/11/railmap-ertms-versie-3-0-nota-alternatieven

1.2 CMD en de TIM: een inleiding

CMD is nuttig bij het opstarten van treinen vanuit de 'No Power'-modus. Een cold movement detector controleert of een trein verplaatst is terwijl het ERTMS EVC zich in de No Power-modus bevond. Hierdoor weet de ERTMS EVC of de laatst gemeten positie nog steeds valide is.

De CMD-functionaliteit is nader gespecificeerd in de ERTMS-specificaties. Deze kunnen echter nog nader gedetailleerd worden voor de geplande operatie. Dat is de reden dat in het kader van het Programma ERTMS in Nederland een nadere specificatie van de CMD is geïnitieerd. Die specificaties zijn van een functioneel niveau en zijn in overeenstemming met de ERTMS-specificaties van de EU (om precies te zijn: de SRS (subset 26)).

De TIM is een functie die nodig is voor toepassing van ERTMS Level 3, zowel met als zonder baan gebonden treindetectie. Level 3 is gebaseerd op het vrijgeven van bezette infrastructuur op basis van positiemeldingen van de trein (en dus niet via baan gebonden detectiesysteem). Het kan hierbij zowel om een virtuele sectie als een 'bewegend blok' gaan.

Aangezien Nederland heeft besloten om ERTMS Level 2 in te voeren, wordt binnen het Programma ERTMS nagedacht of treinen met de TIM uitgerust kunnen worden om in de toekomst aan de vereisten van ERTMS Level 3 te kunnen voldoen.

De TIM-functionaliteit is nader gespecificeerd in de ERTMS-specificaties. Deze kunnen echter nog nader gedetailleerd worden voor de geplande toepassing in Nederland. Dat is de reden dat in het kader van het Programma ERTMS in Nederland de specificatie van de TIM is geïnitieerd. Die specificaties zijn van een functioneel niveau en zijn in overeenstemming met de bestaande basisfuncties in de ERTMS-specificaties van de EU (voornamelijk de SRS (subset 26)).

1.3 Vragen omtrent Cold Movement Detection

De volgende vragen omtrent CMD zijn aan de UNISIG-leden gesteld tegen de achtergrond van de doelstelling van de CMD.

Doel van de CMD is het valideren van de aan boord opgeslagen informatie bij het verlaten van de No Power-modus wanneer er zich geen 'koude beweging' heeft voorgedaan (zie ERTMS-subset 26, 4.11).

Vragen omtrent CMD:

1. Wat zijn uw mogelijkheden om de gespecificeerde CMD-functies beschikbaar te stellen?
2. Over welke oplossingen beschikt u? Geef indien mogelijk ook de bijbehorende technische specificaties.
3. Acht u deze specificaties toereikend om de doelstelling te realiseren? Zo nee, welke suggesties heeft u om de specificaties te verbeteren? (ontbreken er bijv. specificaties of zijn bepaalde functies te ruim of juist onvoldoende gespecificeerd?)
4. Wat moet er nog gebeuren om uw oplossing in nieuwe of te moderniseren treinen te implementeren? (bijv. ontwikkeling, technische constructie, testen bouwen, onderhoud e.d.)
5. Wanneer verwacht u deze functie beschikbaar te hebben?
6. Heeft u nog andere suggesties in verband met de implementatie van de CMD-functies in materieel?

1.4 Vragen omtrent de Train Integrity Monitor

De specificaties van de TIM zijn opgesplitst in een deel A en een deel B. Deel A heeft betrekking op de functionele specificaties gebaseerd op "treinniveau". Deel B betreft een mogelijke technische specificatie voor de TIM als een aparte module in een trein.

Deel A en deel B hebben de volgende doelstellingen:

- Deel A: uitrusten van ERTMS-treinen met een TIM-functionaliteit die kan functioneren met infrastructuur op ERTMS-niveau 3;
- Deel B: beschikbaarheid van een Train Integrity-module met gestandaardiseerde functies en interfaces.

Met betrekking tot deel A en deel B zijn de volgende vragen gesteld:

Vragen omtrent TIM deel A:

1. Wat zijn uw mogelijkheden om de gespecificeerde TIM-functies beschikbaar te stellen?
2. Over welke oplossingen beschikt u? Geef indien mogelijk ook de bijbehorende technische specificaties.
3. Acht u deze specificaties toereikend om de doelstelling te realiseren? Zo nee, welke suggesties heeft u om de specificaties te verbeteren? (ontbreken er bijv. specificaties of zijn bepaalde functies te ruim of juist onvoldoende gespecificeerd?)

4. Wat moet er nog gebeuren om uw oplossing in nieuwe of te moderniseren treinen te implementeren[2]? (bijv. ontwikkeling, technische constructie, testen bouwen, onderhoud e.d.)
5. Wanneer verwacht u deze functie beschikbaar te hebben?
6. Heeft u nog andere suggesties in verband met de implementatie van de TIM-functies in materieel?

Vragen omtrent TIM deel B:

1. Acht u deze specificaties toereikend om de doelstelling te realiseren? Zo nee, welke suggesties heeft u om de specificaties te verbeteren? (ontbreken er bijv. specificaties of zijn bepaalde functies te ruim of juist onvoldoende gespecificeerd?)
2. Wat zijn de voor- en de nadelen van dit specificatiepakket? (bijv. extra ontwikkeling, de vereisten zijn onverenigbaar met bestaande oplossingen e.d.)

[2] Gemoderniseerde treinen zijn onder meer passagiers treinen die nu operationeel zijn.

2 Ontvangen antwoorden naar aanleiding van de vragen

Zeven van de acht UNISIG-leden hebben de gestelde vragen beantwoord. Hierna worden die antwoorden geanonimiseerd en samengevat weergegeven.

2.1 Cold Movement Detection

Voor de CMD worden er al verschillende oplossingen ontwikkeld, tevens is er een aantal oplossingen reeds op de markt beschikbaar. Deze oplossingen sluiten echter niet volledig aan bij de specificaties die bij het verzoek om informatie waren gevoegd. Over de volgende onderwerpen zijn opmerkingen ontvangen:

- onderhoudsinterval;
- functioneringsperiode van de CMD;
- spreidingswaarde van de toegestane beweging;
- Kans op een gevaarlijke gebeurtenis;
- Kans op een niet-gevaarlijke gebeurtenis.

Wat het onderhoudsinterval betreft, was een aantal bedrijven van mening dat het interval van de CMD afgestemd zou moeten worden op het onderhoudsinterval van de totale ERTMS-unit aan boord (OBU - On-Board Unit). Niettemin kunnen aanvullende eisen waardevol zijn, maar deze dienen dan wel in lijn te zijn met de onderhoudsperioden van de totale ERTMS OBU.

De minimale periode voor het functioneren van de CMD is vastgelegd in ERTMS-subset 026 en is bepaald op 72 uur. In de specificaties is de voorgeschreven periode zeven dagen. De reden hiervoor is dat sommige treinstellen gedurende een langere periode stil kunnen staan, bijv. bij feestdagen in combinatie met een weekend. Een aantal leden heeft opgemerkt dat bepaalde vereisten weliswaar nuttig kunnen zijn voor de exploitanten, maar dat zij op technisch vlak ook problemen met zich mee kunnen brengen, met name voor de stroomvoorziening van de CMD (via de trein of een speciale accu).

In de specificaties is de spreiding van de acceptabele toegestane beweging onder de noemer “niet verplaatst” bepaald op 0,1 tot 10 meter. De bovengrens is gekozen met het oog op lange goederentreinen en de doorgaans toegepaste remsystemen op basis van luchtdruk terwijl zij 's nachts stilstaan. Het is mogelijk dat er zich aan beide uiteinden van de trein locomotieven bevinden, waardoor de trein bij het ontkoppelen van de remmen automatisch een paar meter in een bepaalde richting kan bewegen. Een toegestane bovengrens van 10 meter is in dit verband behoorlijk hoog.

Enkele leden gaven aan dat de spreiding te ruim is en tot technische problemen leidt. Hun aanbeveling was om de ondergrens te gebruiken om de accuratie van de CMD te definiëren en dat die 0,1 meter niet noodzakelijk is voor een veilig functioneren van de CMD. De bovengrens van 10 meter werd als te hoog beschouwd. Volgens een aantal leden zou de bovengrens van de spreiding overeen moeten komen met de maximale lengte die waarborgt dat er geen balise-groep over het hoofd is gezien bij de melding “geen beweging gedetecteerd”.

Volgens verschillende UNISIG leden zijn aanvullende eisen aan de kans op veiligheid kritische gebeurtenissen niet nodig aangezien de CMD-functie onderdeel is van de totale THR portionering van de SIL-4 eisen van de complete OBU. Met andere woorden: de vereisten in verband met gevaarlijke gebeurtenissen worden gedefinieerd in het kader van het totale ERTMS-systeem waar de CMD deel van uitmaakt. Het toevoegen van vereisten voor gevaarlijke gebeurtenissen als gevolg van de CMD heeft alleen een meerwaarde indien de risico's van het gebruik van de CMD meer beperkt moeten worden dan de andere risico's die door het totale systeem worden veroorzaakt.

De kans op een niet-gevaarlijke gebeurtenis is van invloed op het aantal keren dat een beweging wordt gemeten wanneer dit niet het geval is. Sommige bedrijven verwijzen naar de beschikbaarheidsvereisten op het 'aan-boord-niveau' (treinniveau) en geven aan dat deze voldoende zouden moeten zijn voor de vereisten van de CMD.

Daarnaast heeft een aantal bedrijven erop gewezen dat de specificaties voor een specifieke ERTMS-functie niet mogen afwijken van de specificatie van het ERA. Een paar bedrijven hebben vraagtekens geplaatst bij een aantal vereisten in de specificatie.

Er zijn geen opmerkingen ontvangen over eventuele ontbrekende specificaties in de vereisten.

2.2 Train Integrity Monitor

Alle UNISIG-leden die gereageerd hebben, zijn bezig met de ontwikkeling van TIM-apparatuur. Er zijn op dit moment echter nog geen TIM-voorzieningen beschikbaar die aan de gevraagde specificaties voldoen.

Een aantal van de leden heeft erop gewezen dat de TIM-specificaties op Europees niveau nog niet compleet zijn. Er zijn op dit moment drie CR's bekend in het kader van het CCM-proces dat door het ERA wordt georganiseerd (CR940, 941, 149). Naast deze CR's moeten alle aanvullende specificaties in overeenstemming zijn met de specificaties zoals beschreven in ERTMS-subset 026 en met andere ERTMS-specificaties.

Uit de reacties van de zeven UNISIG-leden komen verschillende oplossingen naar voren om aan de vereisten te voldoen. De communicatie tussen treinstellen is verplicht en kan via transmissielijnen maar ook via GSM-R plaatsvinden. In een aantal metrosystemen wordt dit al als zodanig toegepast.

Het lastige gedeelte van de TIM is niet zozeer de treinintegriteit, maar de automatische (SIL-4) informatie over de lengte van de trein. Aangezien de kans dat een trein niet compleet is, vrij klein is (bijv. $1*10^{-5}$), moet de onveilige faalkans van de Train Integrity Monitor zodanig zijn dat die kans teruggebracht wordt tot $1*10^{-9}$. Een strengere specificatie dan SIL-4 is niet nodig aangezien de TIM deel uitmaakt van de OBU die in zijn geheel moet voldoen aan de vereiste van SIL-4.
De TIM zou de treinlengte eveneens moeten bepalen op basis van het SIL-4-niveau. Sommige leden merken op dat het moeilijk is om hieraan te voldoen, mede gezien de eis dat dit bij alle mogelijke treinsamenstellingen moet kunnen gebeuren. Er is voorgesteld om het aantal mogelijke treinsamenstellingen te beperken tot de treinsamenstellingen (van dezelfde treinstellen) die ook daadwerkelijk operationeel

zijn. Er worden geen problemen voorzien voor het bepalen van een veilige treinlengte van treinstellen op zich. Een van de aangevoerde argumenten in dit verband is dat dit deel van de informatie van de trein hardware afkomstig moet zijn en niet van de TIM zelf.

Wat het te moderniseren materieel betreft, bestaat de mogelijkheid dat het huidige materieel wel over informatie omtrent de integriteit en de lengte van de trein beschikt, maar waarschijnlijk niet op basis van het SIL-4-niveau. Wellicht dat het nodig is om extra communicatie/draden te installeren om aan de veiligheidsvereisten te voldoen. Dat is afhankelijk van het specifieke materieel en voor sommige treinen waarschijnlijk moeilijk in praktijk te brengen.

Bij goederentreinen kan de stroomvoorziening aan het eind van de trein een probleem vormen. Er zijn oplossingen denkbaar om de treinintegriteit te controleren (door het detecteren van de luchtdruk in de remmen), maar niet om de lengte van de trein vast te stellen. Bedrijven geven aan dat het moeilijk zal worden om de SIL-4-informatie over de lengte van de trein te bepalen.

Een aantal bedrijven heeft voorstellen gedaan voor eisen die beter op treinniveau dan op TIM-niveau gespecificeerd kunnen worden. Het betreft eisen op het gebied van betrouwbaarheid, veiligheid en vertragingstijd. Daarnaast dient het functioneren van het treinsysteem bepaald worden op basis van de vereisten met betrekking tot de beschikbaarheid en responstijden van de apparatuur in de trein. Wanneer de responstijd van de RBC aan de trein 5 seconden bedraagt, is het met het oog op het functioneren van het treinsysteem niet noodzakelijk om hogere eisten te stellen aan de informatie van de TIM. Sommige UNISIG-leden wijzen erop dat een aantal van de huidige vereisten in de specificatie tot dubbele hardware kan leiden.

Met betrekking tot deel B (vereisten op subsysteemniveau) hebben verschillende leden opgemerkt dat deze specificaties de mogelijkheden voor de toeleveringssector beperken om oplossingen te ontwikkelen die in meerdere Europese landen ingevoerd kunnen worden. Wanneer een oplossing in meerdere landen geïmplementeerd kan worden, brengt dat zowel voor de betreffende landen als voor de toeleveringssector voordelen met zich mee.

3 Specifications Cold Movement Detector

The objective of the CMD is have ERTMS equipped trains with Cold Movement Detection functionality in order to have the on board stored information valid when exiting NoPower-mode and no cold movement occurred (see subset 26, 4.11).

Id	Type	Requirement	Rationale
1	requirement	The ETCS equipment shall include the Cold Movement Detection (CMD) function in accordance with subset 26; 3.15.8, 4.4.4, 4.5.2, 4.11 etc.	The Cold Movement Detection function in the train is applicable. This is a requirement as the CMD is optional.
2	definition	The distance D_CMD_allowed_movement is defined as: the maximum displacement of the train which is accepted by the CMD as “no movement”.	Definition of the allowed displacement within “no movement”. A small displacement is needed to have an acceptable availability of the CMD function. Small movements due to for example coupling or wind need to be accepted as “no movement”.
3	requirement	The value of D_CMD_allowed_movement shall be set as a train-parameter.	The variable is to be treated as a train parameter as fixed train data.
4	requirement	The value of D_CMD_allowed_movement shall be in the range of 0.1 to 10 m.	The variable has a limited range. The amount of bits and step size for this variable is to be defined. Logarithmic scaling is acceptable.
5	definition	the hazardous event CMD_WRONG_1 is defined as: The transition condition (subset 26; 4.11) is “no cold movement occurred” while the train movement has been more than D_CMD_allowed_movement	Definition of safety hazard 1. This hazard is defined for the transition condition (subset 26; 4.11). The hazard consists of the failure of the CMD function AND the occurrence of a train movement.
6	requirement	The failure rate for the hazardous event CMD_WRONG_1 shall be less than $0,1*10^{-9}$/h	Requirement to safety hazard 1. We have chosen for 1/10 SIL4 because this failure is directly in the chain of the train positioning report and contributes to a faulty MA. We have no quantitative argumentation for this requirement.
7	definition	the event CMD_WRONG_2 is defined as: The transition condition (subset 26; 4.11) is “cold movement detected or information not available” while the train movement has been less than D_CMD_allowed_movement	Definition of availability fault 2: performance/capacity
8	requirement	The failure rate for the event CMD_WRONG_2 shall be less than $1*10^{-6}$/h	Requirement to availability fault 2: same level of the OBU.
9	requirement	The supplier shall specify the interface of the CMD as part of the TIU.	The specifications of the CMD at the TIU level shall be written by the supplier.
10	requirement	The suppliers interface specification of the CMD shall be free of use for the customer.	If the supplier writes specifications at the TIU level these shall be available and free for use for the customer.
11	requirement	The CMD function shall be available for at least 7 days after the ETCS system goes into “no power”.	Requirement for battery life time if relevant.
12	requirement	The maintenance interval for the CMD function shall be at least 10 years	Requirement for maintenance.

4 Specifications for ERTMS Train Integrity Module

This document describes the requirements for the Train Integrity Function and its supporting TIM device in rolling stock.

This document consists of two parts: part A describes the Train Integrity Function and its requirements at train level and interfacing with the RBC. Part B describes an assumed architecture in which a TIM device communicates via a Train Interface Unit (TIU) with the ETCS-On Board Unit.

4.1 Part A: Requirements on train level

The requirements in this chapter are at train level. The objective of part A is to have ERTMS equipped trains that can run in ETCS level 3.

Id	Type	Requirement	Rationale
TL_1	information	The ETCS on-board equipment shall report train integrity information (L_TRAININT and Q_LENGTH) to the RBC according to ss026, 3.6.5.2 (v3.4.0) in every position report (packet 0 and packet 1).	The train-integrity function at the interface train-track is applicable.
TL_2	requirement	Paragraph 3.6.5.2 in subset 26 is also valid for level 2.	This requirement solves CR940, problem 4. Note: this is no new requirement: in 3.6.5.1.2-g is stated that train integrity has to be part of the positioning report (so also in Level 2). 3.6.5.2 explains the content of Q_LENGTH and L_TRAININT.
TL_3	requirement	L_TRAININT and Q_LENGTH shall be valid for all possible train compositions.	It has to be checked if the supplier can find solutions for all possible train sets, particularly those train sets not delivered by the supplier. The (existing) automatic couplings can be used however shall physically remain unchanged. Coupling between trains without and with TIM function shall be possible.
TL_4	requirement	In Q_LENGTH the status information “Train integrity information confirmed by integrity monitoring device” shall be implemented.	The TIM function is part of the on-board unit. At this level no statements about the TIM’s sub-systems and architecture in the ETCS OBU.
TL_5	requirement	The Q_LENGTH status information “Train integrity information confirmed by integrity monitoring device” shall be determined automatically (without drivers actions).	The Q_LENGTH status information shall be determined automatically, without actions from the driver needed.
TL_6	information	In Q_LENGTH the status information “Train integrity information confirmed (entered) by driver” may be implemented.	The supplier may implement also the TIM function with a button for the driver.
TL_7	requirement	If both status information “Train integrity information confirmed (entered) by driver” and “Train integrity information confirmed by integrity monitoring device” are available, the latter shall be presented in Q_LENGTH.	The automated TIM function prevails over the TIM function with a button for the driver. A train with Q_LENGTH is “Train integrity information confirmed (entered) by driver” is treated by ProRail as not-integer.

Id	Type	Requirement	Rationale
TL_8	definition	L_TRAININT is defined as Safe Train Length, related to the position of the minimum safe rear end at the moment of Train Integrity confirmation, according to figure 15 in subset 26 (v3.4.0), 3.6.5.	L_TRAININT is defined as the “Safe Train Length at T” according to figure 15 in subset 26 (v3.3.0), 3.6.5.
TL_9	definition	The time delay in the train integrity determination is defined as (T-T_0)s. See subset 26, 3.6.5.2., figure 15. The maximum time delay for determining train integrity is defined as Tresponse.	Definition of time delay of train integrity detection. Note: at the moment T_0 train integrity may not have been detected for T_0.
TL_10	Requirement	Tresponse shall be less than 2s.	Requirement to time delay for response. This is a performance requirement.
TL_11	Constraint concerning the train	It is assumed that the driving direction of the “minimum safe rear end of the train” is the same as the driving direction of the train, i.e. If the driving direction has not been changed AND train integrity was confirmed for a certain time ago, the actual minimum safe location of the rear end of the train, will never be in rear of the minimum safe location of the rear end of the train at the time the integrity was confirmed for.	Roll back protection is considered to be taken care of in the train. If the driving direction of the train changes (E.g. reversed in Post Trip) the driving direction of the safe rear end changes as well. Without this assumption the train cannot report a safe train length.
TL_12	requirement	The unsafe failure rate, i.e. the probability that in the report to the RBC • the reported Q_LENGTH is “train integrity confirmed by integrity monitoring device” AND • the reported train length L_TRAININT is less than safe train length, shall be less than $0,1*10^{-9}$/h	Requirement to the safety hazard. We have chosen for 1/10 SIL4 because this failure is directly in the chain of train detection and contributes to a faulty MA. We have no quantitative argumentation for this requirement. If the train is broken and reported as integer, then it is only unsafe if the minimum safe rear end position of the train based on L_TRAININT is beyond the actual position of the trains safe rear end. As L_TRAININT is defined as the distance between the estimated train front end, and the minimum safe rear end, the train length is increased with L_DOUBTOVER.
TL_13	requirement	In case the ETCS on-board is not able to report the train integrity with the required safety level, then the on-board shall report “No train integrity information available”	The safe state shall be reported if insufficient information is available.
TL_14	requirement	If it is detected that the train is broken, then the ETCS on-board shall report this to the RBC using Q_LENGTH is “train integrity lost”, within a train dependent response time (Tresponse).	In this situation the maximum distance between the train front end and the train rear end cannot be communicated to the RBC.

Id	Type	Requirement	Rationale
TL_15	requirement	The availability failure rate that the on-board reports “train integrity confirmed by driver” while all units (*) in the train are fitted with the a train integrity function and the actual status is “Train integrity information confirmed by integrity monitoring device” shall be less than 10^{-6}/h (*) a unit can be a locomotive, multiple unit or steering car.	Not reporting the correct integrity affects availability.
TL_16	requirement	The availability failure rate that the on-board reports “no train integrity information” for a period longer that Tresponse while all units (*) in the train are fitted with the a train integrity function (excluding the situations in TL_22 and TL_23) shall be less than 10^{-6}/h (*) a unit can be a locomotive, multiple unit or steering car.	Not reporting the correct integrity affects availability. Regarding CR940 problem 3 it is not clear if the L_TRAININT shall grow or the onboard reports temporally no integrity information available until the integrity is confirmed. This requirement allows both implementations until the CR is clarified.
TL_17	requirement	The reliability failure rate, when the information "train integrity lost” is reported while the train is not broken, shall be less than 10^{-6}/h.	If the train integrity lost is reported while it is not the case this affects reliability.
TL_18	requirement	The reliability failure rate when the train is broken longer than a time Tresponse, but the information “train integrity lost” is not included in the position reports to the RBC. shall be less than 10^{-6}/h.	Not giving the information “train integrity is lost” while the train is broken is not a safety failure for the level 3 operation if the conditions given in requirement TL_12 are fulfilled, i.e. the L_TRAININT is still correct.
TL_19	requirement	If the Q_LENGTH status information is “Train integrity information confirmed by integrity monitoring device” the L_TRAIN parameter of the train data shall be set automatically (without actions by the driver) according to the actual train length. In this case the driver has no possibility to change the L_TRAIN parameter manually.	If TIM function is available the train length (L_TRAIN) shall be set automatically to reduce the risk of data entry errors in determining the safe train length see TL_8. Note: L_TRAIN is the static train length while L_TRAININT is the dynamic safe train length.
TL_20	Requirement	The unsafe failure rate, i.e. the probability that the L_TRAIN is shorter than the actual train length shall be less than $0{,}1*10^{-9}$/h	Requirement to the safety hazard. We have chosen for 1/10 SIL4 because this failure is directly in the chain of train detection and contributes to a faulty MA. We have no quantitative argumentation for this requirement. It is unsafe if the minimum safe rear end position of the train based on L_TRAININT which is based on L_TRAIN is beyond the actual position of the trains rear end.
TL_21	Requirement	The reliability failure rate, i.e. the probability that the L_TRAIN is longer than the actual train length + 10 m shall be less than 10^{-6}/h.	Reporting a longer train length than the real train length the performance. The 10 m is applicable for passengers trains.

Id	Type	Requirement	Rationale
TL_22	Requirement	When the actual train length has changed the L_TRAIN parameter of the train data shall be set and sent to the RBC according to the actual train length. The train shall report “no integrity information available” as long as the acknowledgment from RBC on the train data is not received.	While the acknowledgement has not been received, this is the safe state because the train could have been split. The RBC shall be informed on the changed train length. This is related to the problems in CR940. The acknowledgement is message 8. RBC shall confirm the new L_TRAIN to be sure that the new information has reached the RBC.
TL_23	requirement	The driver shall be able to manually override the Q_LENGTH status information to “No train integrity information available”. In this integrity override status the real integrity status of the train is to be treated as “No train integrity information available”.	In case of a defect or coupling with non-TIM compatible rolling stock the TIM function shall be switched off (override). Both the Q_LENGTH status and the real integrity status of the train become “No train integrity information available”.
TL_24	requirement	The manual override of the Q_LENGTH status information to “No train integrity information available” shall be performed with a switch.	The switching off of the TIM function shall be implemented with a switch.
TL_25	requirement	The status information Q_LENGTH shall be shown to the driver. This can be implemented in several ways, for example: • on request of the driver on another DMI than the harmonized ETCS DMI • on a lamp • for each change of status as a message on the harmonized ETCS DMI, etc.	The driver needs to be able to check the integrity status. The harmonized DMI does not support this.

4.2 Part B: Requirements on sub-system level

Part A describes the requirements at the interface between the train and the RBC (1) train-track interface in figure 2). The internal requirement specifications in the RBC are not in the scope of this document. The internal requirement specifications in the train (2) to 5) in figure 2) are detailed in part B of this document.

These requirements are composed from a railway undertaking viewpoint.

The objective of part B is to have a Train Integrity Module available with standardized functions and interfaces..

The architecture is given in figure 1.

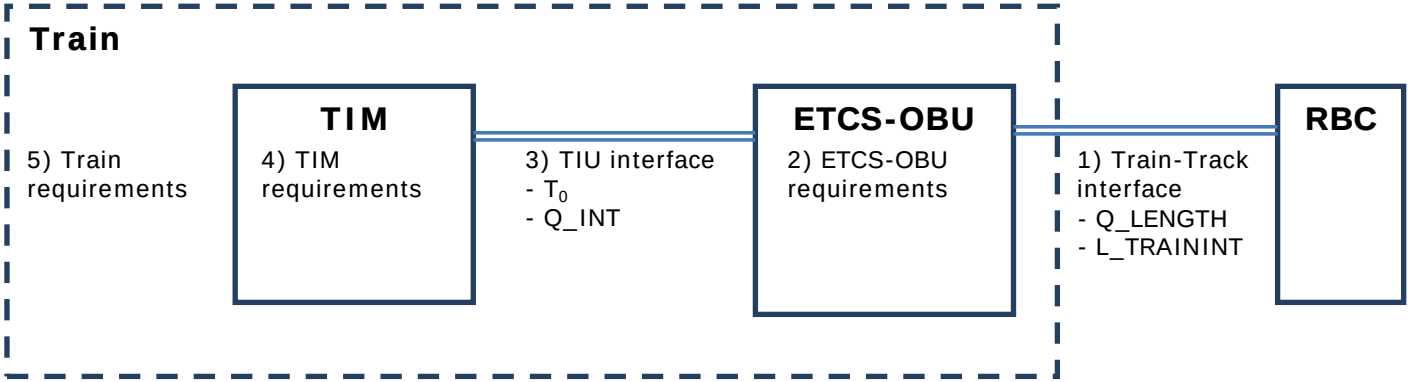

Figure 1. Architecture for TIM function and device

The requirements in this chapter are at sub-system level. Table 3 shows the reference-ids for the requirements related to figure 1.

reference	***Description***
Train-x	5) Train requirements
TIM-x	4) TIM requirements
TIU-x	3) TIU interface requirements
ETCS-x	4) ETCS-OBU requirements

Table 1.

General requirements per module/interface

- Train: the probability of losing integrity shall be defined as a constraint to the train (and the process handling the train)
- Train Integrity Monitoring device: this module determines if the train was not broken with a certain (train dependent) delay and communicates this information to the ETCS system
- Interface ETCS-TIM device (part of the TIU): includes “train integrity is confirmed for a specific moment in time”, and the time for which , or “train integrity cannot be confirmed”, or “train is broken”, or “failed” and time synchronization between TIM and ETCS on-board
- ETCS: Calculate L_TRAININT if information from the TIM device is received, taking the delay time into account.

Requirements at sub-system level

Id	Type	Requirement	Rationale
Train-1	Constraint	The probability of losing integrity shall be less than 10^{-5}/h	The current frequency is around 10^{-6}/h
TIM-1	Requirement	The TIM module shall synchronize its internal clock with the ETCS on-board internal clock, with a tolerance < 10ms.	10ms is the required resolution of the ETCS train borne clock (T_TRAIN)
TIM-2	Requirement	In case the train is not broken, the TIM device shall report to the ETCS on-board the time (T_0) for which the integrity of the train is confirmed. This time (T_0) will have a delay (Tdelay) relative to the moment the message is sent to the ETCS on-board.	If only the status “integrity confirmed” or “integrity not confirmed” is reported, then the ETCS on-board has to assume the worst case delay time, which can be long, depending on the train type and TIM solution.
TIM-3	Requirement	In case the train is broken, the TIM device shall report to the ETCS on-board “Train integrity lost”	
TIM-4	Requirement	If the TIM device cannot determine if the train is broken due to failure of the device, then the TIM device shall report “fail state” to the ETCS on-board	
TIM-5	Requirement	If the TIM device cannot determine if the train is broken due to another reason (e.g. due to missing information) then the TIM device shall report “No train integrity information available” to the ETCS on-board	
TIM-6	Requirement	The unsafe failure rate of the TIM device, i.e. the probability that • the TIM device reports “train integrity confirmed” for a certain time (T_0) while the train was broken at that time, shall be less than 10^{-5}/h	The total failure rate including the probability that a train breaks will become: P_trainbreaks * (FR_TIM + FR_ETCS-OBU) = 10^{-5} * (10^{-5} + 10^{-9}) Where: • P_trainbreaks: probability the train breaks • FR_TIM: failure rate of the TIM device • FR_ETCS-OBU: failure rate of the ETCS on-board.
TIM-7	Requirement	The delay (Tdelay) shall always be less than a rolling stock dependent time “Tdelay_max”	The delay time of the TIM device
TIM-8	Requirement	For train sets Tdelay_max shall be less than 1s.	For train sets the train integrity can actively be monitored. For other train types (hauled passenger of freight), the delay could be much longer. The ETCS equipment shall be useable in all train types.

Id	Type	Requirement	Rationale
TIM-9	Requirement	The availability failure rate of the TIM device, i.e. the probability that • "TIM device faulty" is reported to the ETCS on-board OR • "no information available" is given to the ETCS on-board shall be less than 10^{-6}/h	The TIM device is the module which can cause unavailability of the TIM function if ETCS (including on-board) is operational, so the complete failure rate may be assigned to the TIM device.
TIM-10	Requirement	The reliability failure rate of the TIM device, i.e. the probability that • "train broken" is reported to the ETCS on-board, while the train is not broken, shall be less than 10^{-6}/h	The TIM device is the module which can cause unavailability of the TIM function if ETCS (including on-board) is operational, so the complete failure rate may be assigned to the TIM device.
TIM-11	Requirement	The reliability failure rate of the TIM device, i.e. the probability that • "integrity is confirmed" is reported to the ETCS on-board while the train has been broken longer than a time Tdelay_max ago shall be less than 10^{-3}/h	As the total failure rate (train broken, i.e. 10^{-5}, and not reported 10^{-3}) becomes 10^{-8}/h, it can be neglected in the total reliability failure rate.
TIM-12	Requirement	The TIM device shall report the integrity status and the related time stamp T_0 at least once per second to the ETCS on-board.	
TIM-13	requirement	The maintenance interval for the TIM device shall be at least 10 years	Requirement for maintenance.
TIU-1	Requirement	The TIU shall provide a protocol for time synchronization between TIM device and ETCS on-board shall be available	
TIU-2	Requirement	The TIU shall provide a variable Q_INT to indicate the following four states from the TIM device to the ETCS on-board: • Train Integrity is confirmed • Train is broken • TIM device faulty • No information available	
TIU-3	Requirement	The TIU shall provide a variable to communicate the time (T_0) for which the integrity is confirmed (if so).	
TIU-4	requirement	The suppliers interface specification of the TIM at the TIU shall be free of use for the customer.	The specifications at the TIU level shall be available and free for use for the customer.
ETCS-1	Requirement	If • a message confirming the train integrity is received from the TIM device then, the ETCS on-board shall determine the "confirmed safe minimum rear end location" of the train at the time (T_0). The ETCS on-board shall store the least restrictive (i.e. farthest) determined "confirmed safe minimum rear end location", thus overwrite the stored value only if the new value is less restrictive.	

Id	Type	Requirement	Rationale
ETCS-2	Requirement	If • a stored value for the “safe minimum rear end location” is available then, when composing a train position report, the ETCS on-board shall calculate the distance between the reported estimated front end of the train and the minimum rear end location of the train at time (T_0). The distance shall as “L_TRAININT” be included in the position report (thus Q_LENGTH “Train integrity confirmed by integrity monitoring device”)	
ETCS-3	Requirement	If • the information “train broken” is received from the TIM device then, when composing a train position report, the ETCS on-board shall include “train integrity lost” for Q_LENGTH in the position report, until: Other information is received from the TIM device or the driver confirms train integrity.	
ETCS-4	Requirement	If • no valid information confirming train integrity from a TIM device is available AND • the driver has confirmed the integrity of the train after the last report “train is broken” was received from the TIM device, and after the last position report was sent to the RBC then, when composing a train position report, the ETCS on-board shall include “Train integrity confirmed by driver” for Q_LENGTH in the position report (once).	
ETCS-5	Requirement	If • no valid information confirming train integrity from a TIM device is available AND • the driver has <u>not</u> confirmed the integrity of the train after the last report “train is broken” was received from the TIM device, and after the last position report was sent to the RBC then, when composing a train position report, the ETCS on-board shall include “No train integrity information available” for Q_LENGTH in the position report.	