Report on the Request for Information on ERTMS Cold Movement Detection and ERTMS Train Integrity Monitor

For external use

Date: **1 June 2015**

Content

Management Summary

On 11 April 2014, the Dutch Government made a Preference Decision regarding the rollout of ERTMS Level 2 on the busiest corridors of the railway network. Currently, the ERTMS program is in the Plan Elaboration Phase, which also includes system design. Among other activities, the specifications for various components will be established during this Elaboration Phase.

With regards to the rollout, for a number of functions no operational experience has been gained as of yet in the existing Dutch ERTMS implementations. These functions include Cold Movement Detection (CMD) and the Train Integrity Monitor (TIM). The specifications for these functions partly fall outside the scope of the EU ERTMS specifications as laid down in the CCS TSI. For this reason, additional specifications have been drawn up within the framework of the ERTMS Programme, and UNISIG members have been asked to answer several questions to establish whether these requirements meet the intended objectives. Seven of the eight companies that were contacted have answered the questions.

The decision of (one of) these functions are implemented is not yet taken, even if the choice is implemented over the baseline. This Request for Information should be seen as a further consideration of these functions, regardless of whether they will eventually be implemented or not.

In their reaction, the UNISIG members indicate that they are working on solutions for CMD since this is part of the ERTMS specifications of baseline 3. The main challenges in fulfilling the established specifications relate to power supply and to the question whether fixed or variable settings for the range of allowed movement are to be allowed. Several companies have stated that some of the specifications (reliability and safety) should be set at train level, instead of at subsystem level.

All the UNISIG members who responded stated that they are working on the elaboration of one or multiple solutions for TIM. The greatest difficulties are expected to occur in providing the information on train length based on SIL 4, in combination with the requirement that this should be done for all possible train compositions. By contrast, the requirement relating to information on train integrity will be relatively easy to fulfil. The specifications at subsystem level (Part B) limit the possibilities for the supplying industry to find solutions which can be implemented in multiple European countries.

The answers and comments received will be used to improve the specifications for CMD and TIM.

1 Introduction and questions

On 11 April 2014, the Dutch Government made a Preference Decision regarding the rollout of ERTMS Level 2 on the busiest corridors of the railway network. The English version of this decision can be found here.[1] Currently, the ERTMS program is in the Plan Elaboration Phase, which also includes system design. Among other activities, the specifications for various components will be established during this Elaboration Phase.

With regard to the rollout, for a number of functions no operational experience has been gained as of yet in the existing Dutch ERTMS implementations. These functions include Cold Movement Detection (CMD) and the Train Integrity Monitor (TIM).

The decision of (one of) these functions are implemented is not yet taken, even if the choice is implemented over the baseline. This Request for Information should be seen as a further consideration of these functions, regardless of whether they will eventually be implemented or not.

The specifications for these functions partly fall outside the scope of the EU ERTMS specifications as laid down in the CCS TSI. This means that additional specifications can be drawn up within the framework of the ERTMS Programme in the Netherlands. In this context, ERTMS system suppliers have been asked to answer a number of questions to establish whether these specifications meet the intended objectives.

This report contains public information on this Request for Information and gives an anonymized summary of the information received.

1.1 Procedure of the Request for Information

On the 12 January 2015, two documents with questions and specifications for CMD and TIM were sent by email to all the members of UNISIG. The specifications for CMD and TIM which were sent are included in this document (chapter 3 and 4).

UNISIG is an industrial consortium which was created to develop the ERTMS/ETCS technical specifications. As an Associated Member of UNIFE, a recognised stakeholder, UNISIG actively contributes to the activities of the European Railway Agency in the field of ERTMS/ETCS technical specifications (source: www.ertms.net).

At present, there are eight market players involved in UNISIG: Alstom, AnsaldoSTS, AZD Praha, Bombardier, CAF, Mermec Group, Siemens and Thales.

By 13 February 2015, seven out of eight members had sent a response. On the same day, a meeting was held with one of these members. The information received during this meeting has been included in the anonymized summary in chapter 2.

[1] http://www.government.nl/documents-and-publications/reports/2014/04/01/railway-map-ertms-version-3-0-memorandum-on-alternatives.html

1.2 Introduction to CMD and TIM

CMD facilitates the start-up of trains from 'No Power' mode. A Cold Movement Detector checks whether a train was moved while the ERTMS EVC was in 'No Power' mode. In this way, the ERTMS EVC is able to ascertain whether the last measured position is still valid.

The CMD functionality is specified in the ERTMS specifications. However, these specifications may be worked out in more detail for the purpose of the planned operation. To this end, a further specification of CMD has been initiated in the framework of the ERTMS Programme in the Netherlands. The specifications are set at a functional level and are fully in line with the EU ERTMS specifications (to be more specific: the SRS (subset 26)).

The TIM function is needed for the operation implementation of ERTMS Level 3, both with or without track-side train detection. Level 3 is based on the principle of releasing occupied infrastructure in response to position reports from the train (and therefore not on a track-side train detection system). This may be based either on a virtual section or on a 'moving block'.

Since it has been decided in the Netherlands to implement ERTMS Level 2, the ERTMS programme is considering whether trains can be equipped with TIM to be able to meet the requirements for ERTMS Level 3 in the future.

The TIM functionality is specified in the ERTMS specifications. However, these specifications may be finalised for the purpose of their implementation in the Netherlands. To this end, a further specification of TIM has been initiated in the framework of the ERTMS Programme in the Netherlands. The specifications are set at a functional level and are fully in line with the existing basic functions in the EU ERTMS specifications (mainly the SRS (subset 26)).

1.3 Questions regarding Cold Movement Detection

UNISIG members were asked the following questions relating to CMD, with reference to the objective of CMD.

The objective of CMD is to validate the information stored on board when exiting No Power mode when no cold movement has occurred (see ERTMS subset 26, 4.11).

Questions relating to CMD:

1. What are the possibilities for providing the CMD functions as specified?
2. What solutions do you have available? Please provide relevant technical specifications if possible.
3. Do you consider these specifications to be sufficient in order to achieve the objective? If not, what suggestions do you have to improve the specifications? (e.g. missing specifications, under or over-specified functions).
4. What steps must be taken to implement your solution in new or retrofitted trains? (e.g. development, engineering, testing, building, maintenance etc.)
5. By when do you expect to have this function available?
6. Do you have any other suggestions related to the implementation of the CMD functions in rolling stock?

1.4 Questions regarding Train Integrity Monitor

The specifications for TIM consist of two parts, A and B. Part A deals with the functional specifications based on 'train level'. Part B consist of a possible technical specification for TIM as a separate module in a train.

The objectives of parts A and B are:

- Part A: to have ERTMS trains equipped with TIM functionality that can run on ETCS Level 3 infrastructure;
- Part B: to have a Train Integrity Module available with standardised functions and interfaces.

The following questions were asked for part A and part B.

Questions TIM part A:

1. What possibilities do you see for providing the TIM functions as specified?
2. What solutions do you have available? Please provide relevant technical specifications if possible.
3. Do you consider these specifications to be sufficient in order to achieve the objective? If not, what suggestions do you have to improve the specifications? (e.g. missing specifications, under or over-specified functions).
4. What steps must be taken to implement your solution in new or retrofitted trains?[2] (e.g. development, engineering, testing, building, maintenance etc.)
5. By when do you expect to have this function available?
6. Do you have any other suggestions related to the implementation of the TIM functions in rolling stock?

Questions TIM part B:

[2] Retrofitted trains are currently operating trains.

1. Do you consider these specifications to be sufficient in order to achieve the objective? If not, what suggestions do you have to improve the specifications? (e.g. missing specifications, under or over-specified functions).
2. What are the pros and cons of this package of specifications? (e.g. additional development, requirements conflicting with existing solutions etc.)

2 Received answers to the questions

Seven out of eight UNISIG members responded to the questions asked. The answers received are presented in anonymized and summarized text below.

2.1 Cold Movement Detection

For CMD several solutions are already being developed, and some solutions are already available on the market. These solutions do not entirely match the specifications which were given in the Request for Information, however. Comments were received on the following topics:

- maintenance interval;
- period of functioning of CMD;
- range of allowed movement;
- failure rate for hazardous events;
- failure rate for non-hazardous events.

Several companies remarked that, with regards to the maintenance interval, the interval of the CMD should be aligned with the maintenance interval of the whole ERTMS On-Board Unit (OBU). Nevertheless, additional requirements can be valuable, but these should then also be in line with the maintenance intervals of the ERTMS OBU as a whole.

The minimum period for the functioning of CMD is stated in ERTMS subset 026 and is set for 72 hours. In the specifications, this period set at seven days. The reason for this is that some trainsets will stand still over a longer period of time, for instance when holidays are combined with a weekend. Several members noted that certain requirements may be useful for the operating companies but might also cause technical complexity, especially with regards to the CMD power supply (via the train or a special battery).

In the specifications, the range of allowed movement for what is accepted as 'not moved' is set to be between 0.1 and 10 m. The upper value has been chosen because of long freight trains and the air-pressure braking systems which are usually applied while standing still overnight. It is possible that there are locomotives at both ends of the train, such that the train might automatically move a few metres in one direction when releasing the brakes. To account for this, the upper limit of 10 m is quite high.

Several members indicated that the range is too wide and that it causes technical complexity. They recommended using the lower limit in defining the accuracy of the CMD, and considered that 0.1 m is not necessary for a safe operation. The upper limit of 10 m was found to be too high. According to several members, the upper limit of the range should match the maximum length that would make it possible to guarantee that no balise group is missed for the notification 'no movement occurred'.

According to several UNISIG members additional requirements in relation to the failure rate for hazardous events are not necessary, since the CMD function is part

of the THR allocation approach of SIL4 requirements relating to the OBU as a whole. In order words, the requirements relating to hazardous events are defined in the framework of the ERTMS system as a whole, of which CMD is a part. Adding requirements for hazardous events connected with CMD is only valuable if the risks caused by CMD are to be minimized more than other risks which are caused by the system as a whole.

The failure rate for non-hazardous events affects the number of times a movement is measured when none has taken place. The requirement in the specification is $1*10^{-6}$/h. Some companies refer to the availability requirements at the on-board level (train level), and suggest that these should be adequate for the requirements of CMD.

Furthermore, several companies pointed out that the specifications for a specific ERTMS function may not deviate from the ERA specifications. A few companies have raised questions about some of the requirements in the specification.

No comments on specifications missing from the requirements were received.

2.2 Train Integrity Monitor

All the UNISIG members who responded are developing TIM devices. However, at present there are no TIM devices available which fit the requested specifications.

Several members pointed out that the specifications for TIM have not been completed yet at the European Level. At the moment, three CRs are known in the framework of the CCM process organised by the ERA (CR940, 941, 149). Besides these CRs, all additional specifications must be in line with the specifications described in ERTMS Subset 026 and other ERTMS specifications.

Several solutions to meet the requirements were proposed in the responses of the seven UNISIG members. Communication between trainsets is mandatory and can be done by bus as well as by GSM-R. This is already applied in some metro systems.

The difficult aspect of TIM is not so much train integrity, but rather the automatic (SIL-4) train length information. Since the chance of a train not being complete is rather small (e.g. $1*10^{-5}$), the train integrity monitor should have a failure rate such that this chance is reduced to $1*10^{-9}$. A specification stricter than SIL-4 is not required, since TIM is part of the OBU which must meet the standards of SIL-4 as a whole. TIM should also determine train length based on the SIL-4 level. Several members remarked that this requirement is difficult to meet, also considering the requirement that this must be possible for all train compositions. Suggestions were made to restrict the number of possible train compositions to those compositions (of the same trainsets) that are actually in use. No problems were foreseen with regard to determining a safe train length for train sets themselves. One of the arguments made was that this information should be provided by the train hardware and not by TIM.

For rolling stock that is to be retrofitted, it is possible that current rolling stock does have information on train integrity and train length, but probably not based on SIL-4 level. Redundancy can be necessary in order to meet the safety requirements. This will depend on the rolling stock in question and may be difficult to achieve for certain trains.

For freight trains, power supply is difficult to establish at the end of the train. Solutions are thinkable for monitoring train integrity (by detecting air pressure in the brakes), but not for establishing train length. Companies indicate that SIL-4 information on train length will be hard to establish.

Several companies suggested a number of requirements which can be better specified at train level rather than at TIM level. These are requirements relating to reliability, safety and delay time. In addition, train system performance should be determined based on the requirements relating to availability and response times of the equipment on the train. When the response time from RBC to the train is 5 s, there is no need to set higher requirements for information from TIM with regard to train system performance. A number of UNISIG members point out that some of the current requirements in the specification might lead to redundancy in hardware.

Regarding part B (requirements on subsystem level), several members noted that these specifications limit the possibilities for the supplying industry to develop solutions which can be implemented in multiple European countries. Implementing a solution in multiple countries brings benefits for both the countries involved and for the supplying industry.

3 Specifications Cold Movement Detection

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.

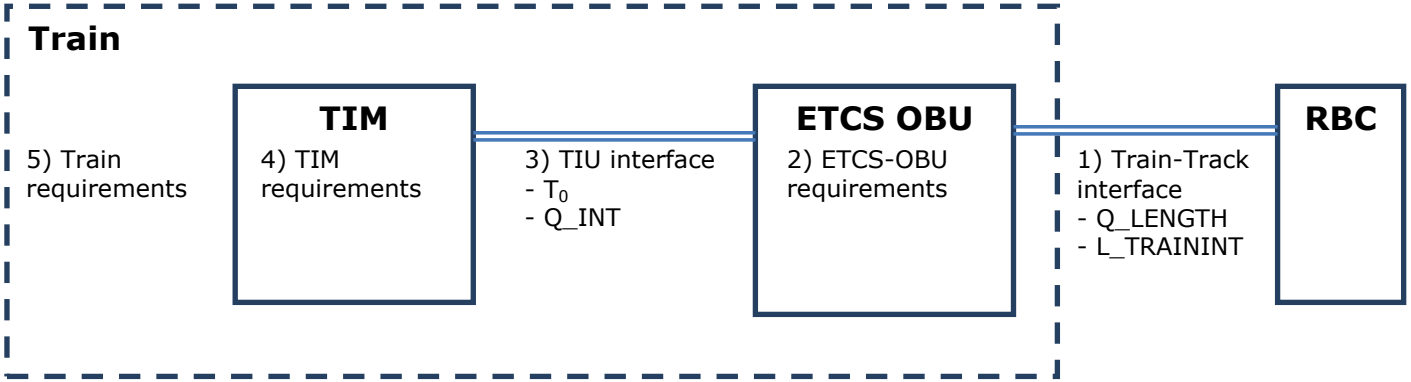

Figure 1. Architecture for TIM function and device

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 not 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.	