

## D4.2 Safety requirements

---

for the development of an STM ATB

Colophon	
Document ID	D4.2
Version	7.0
Revision	441250
Author	JW
Reviewed	441250 ,STMA-69558
Approved	441250 ,STMA-69575
Archive	SID-ERTMS-1000423
Date:	November 15 2019

## Authorisation

---

Compiled by: JW Signature/E-sign: 441250 ,STMA-69536	Date: November 15 2019
Reviewed by: BV Signature/E-sign: 441250 ,STMA-69558	Date: November 15 2019
Approved by: WD Signature/E-sign: 441250 ,STMA-69575	Date: November 18 2019


## CONTENT

1	References	5
2	Preface	5
3	Assumptions	7
4	Communication via Profibus	7
4.1	Detected losing one telegram at the profibus	7
4.2	Undetected losing telegrams at the Profibus	9
4.2.1	Safety levels of connections	10
4.2.2	Not detecting the loss of one telegram	11
4.2.2.1	DMI telegrams	11
4.2.2.2	STM controller telegrams	11
4.2.3	Not detecting the loss of multiple telegrams	12
4.2.3.1	Odometer	12
4.2.4	Undetected corrupting a telegram	13
4.2.4.1	DMI telegrams	13
4.2.4.2	STM controller telegrams	14
4.2.4.3	TIU	15
4.2.4.4	BIU	15
4.2.4.5	Odometer	16
5	Storing data	16
5.1	Storage related to CAT1 hazards	17
5.2	Storage faults related to CAT3 hazards	19
5.3	Storage related to CAT2/CAT4 hazards	22
5.4	Storage related to CAT5 hazards	23
5.5	Generic safety requirement concerning storing data	24
6	Calculations	24
6.1	Calculation faults concerning CAT1 hazards	25
6.2	Calculation faults concerning CAT2	25
6.3	Calculation faults concerning CAT3	26
6.4	Calculation faults concerning CAT4	27
6.5	Calculation faults concerning CAT5	28
6.6	Generic safety requirement concerning calculations	29
7	Input faults (other than via Profibus)	29
7.1	Faults concerning CAT 1 hazards	29
7.2	Faults concerning CAT3 hazards	31
7.3	Faults concerning CAT4 hazards	32
8	Miscellaneous	32
9	Common cause faults	33

9.1 Common cause failures concerning communication . . . . .	34
9.2 Common cause faults concerning storage . . . . .	35
9.3 Common cause faults concerning calculations . . . . .	35



## 1 References

### Text, STMA-14296 - Reference documents



All the documents references used in this document can be found in the document  [P6.1](#)

[Bibliography](#) available in the Polarion folder  [Processes](#)


### Abbreviations, definitions and terminology

An overview of the abbreviations, definitions and terminology used in this document can be found in document  [P6.2 List of abbreviations, definitions and terms](#) available in the Polarion folder  [Processes](#)


### Requirement identification

The STM ATB project makes use of an automated requirement management system. In this system each requirement has been identified as a work item. Each work item has been automatically assigned with a unique ID, with the format "STMA-<number>". As a result requirement ID's are not in logical order. An overview of all the used STMA-numbers is given in document  [P6.3 Requirement Overview](#) available in the Polarion folder  [Processes](#)

**Text, STMA-20011** - In this document requirements are based on tolerable fault rates assigned to specific faults.

**Text, STMA-28792** - Required legal standards and norms applicable to the STM ATB project and product are listed in  [D3.0 Legal framework standards and norms](#)




## 2 Preface

**Text, STMA-19973** - This document is the safety requirement specification for STM ATB. The input for this document is based on the tolerable functional fault rates as defined in  [STMA-8974 - D3.3 Tolerable Functional Fault Rates](#).

In this document safety requirements concerning the technical implementation will be derived from the functional fault rates.

**Text, STMA-19974** - The tolerable fault rates will be grouped per type of fault, i.e. for similar faults, the same safety requirements are applicable. This is done while those will concern similar technical solutions.

**Text, STMA-19966** - Groups with similar expected solutions for which the same safety requirement shall apply are:

- Profibus communication (see chapter:  [STMA-14780 - Communication via Profibus](#))
- Data storage (see chapter:  [STMA-14785 - Storing data](#))
- Calculations (see chapter:  [STMA-14787 - Calculations](#))

Other safety requirements concern faults in the input circuits of the STM (see chapter: [STM-14788 - Input faults \(other than via Profibus\)](#)).

**Text, STMA-19964** - A difference is made between detected and undetected losing a telegram as action can be taken to guarantee safety in the first case.

The interface specification as given in the ERA specifications (subset056 and subset057) include mechanisms to detect loss, delay and corruption of a telegram. Corruption or loss which shall be detected according to these requirements is considered as "detected corruption" or "detected loss".

In order to have margin to the 3 s which distinguish between CAT1 and CAT2 hazards and between CAT3 and CAT4 hazards a fault is considered to be detected if it is mitigated within 2 s instead of 3 s ( [STMA-11377](#)).

**Definition, STMA-11377** - A fault is considered as "detected" if it should (according to ERA specifications) be recognized and mitigated within 2 s.

**Text, STMA-28985** - In [STMA-8974 - D3.3 Tolerable Functional Fault Rates](#) definitions for hazard, failure and fault as copied from EN50129:2003 are used. A fault is defined as a function which is not performed correctly (i.e. a "functional fault"). In this document the term "hardware failure" is used for defects and transient faults which might (but not have to) lead to a "functional fault".

A hardware failure (a failure of a hardware component) will only lead to a functional fault if the concerning function is required at the moment of the hardware failure. E.g. losing a telegram is only possible in case a telegram is sent. Therefore "functional fault" rates may be translated in to safety requirements concerning the technical implementation expressed in "technical failure/case".

**Text, STMA-19971** - The exact scope of safety relevant variables can only be determined based on the design, and shall be used in the FMEA (see Development plan, D0.4.1). Information mentioned in this document is used for determining safety requirements as a basis for the system architecture only.

**Text, STMA-19968** - After tolerable fault rates are assigned to specific faults, the effect of common cause ( [STMA-16891 - Common cause faults](#) ) is considered.

### 3 Assumptions

**Text, STMA-28986** - To determine safety requirements concerning the hardware (acceptable failure rates for hardware components), assumptions have to be made concerning the frequency at which specific functions (for which tolerable fault rates have been defined in [STMA-8974 - D3.3 Tolerable Functional Fault Rates](#)) are used ("demanded").

As far as possible those assumptions will be based on documented studies, however those are often not available. In the latter cases an underpinned figure will be used.

### 4 Communication via Profibus

**Text, STMA-20013** - In this chapter all faults which can be caused due to communication errors at the profibus (including interfaces at the STM) are gathered. Faults concerning the Profibus communication can be distinguished in "losing a telegram" (including corrupting in a way the CRC check according to subset057 from ERA is refused) and "corrupting a telegram" in a way the CRC check still results in a valid telegram. Further the consequence of a communication error at the Profibus differs between faults which are detected and faults which are not detected.

**Text, STMA-20009** - The different categories will be handled in the paragraphs below. Communication error rates are specified as fraction of the communicated data. Tolerable hazard rates are specified in [D2.2] as a rate per hour. Therefore a translation shall be made between the THR in hazards per hour to communication faults per case.

**Text, STMA-20007** - The effect of detected corruption of a telegram is equal to losing a telegram as the telegram will be rejected, however corruption is detected faster as detection of a loss as the latter will only be detected at reception of the next telegram (or after a time-out).

#### 4.1 Detected losing one telegram at the profibus

**Text, STMA-19998** - The fault rate concerning detected losing one telegram at the Profibus is equal for all types of information exchanged with the same ETCS function (STM controller, BIU, DMI etc).

Therefore the tolerable fault rate is determined by the most critical information.

As different safety levels can be selected for different connections, the TFR can differ per type of connection.


**Text, STMA-20008** - The following faults due to (detected) losing a telegram at the Profibus are

identified as leading to one of the CAT4 or CAT5 hazards. As losing a telegram is normally defined as the chance of losing a telegram if sent ("on-demand") the tolerable fault rate will be expressed in faults/case.



Below only single faults are considered. Contributions to hazards resulting from combinations of faults are analyzed in a later stage in this document.

**Fault, STMA-9651** - Losing one Profibus telegram containing a new (higher) current train speed.

**Text, STMA-19999** -

Fault  STMA-9651 leads to a CAT4 hazard if the EB should have been commanded at the old (lower speed level). This is the case app. every 1000 hours.



In 1000 hours app  $10^7$  speed telegrams are sent. Therefore the risk that losing one telegram containing speed information leads to a CAT4 hazard is negligible.




Further Fault  STMA-9651 can contribute to a CAT2 hazard (EB commanding branch). Therefore the tolerable fault rate is  $3.3 \cdot 10^{-4}$ /hour (see  STMA-21062). A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $5.5 \cdot 10^{-5}$ /case.

**Fault, STMA-9078** - Detected losing an EB command at the Profibus.

**Fault, STMA-9076** - An error in the communication of an EB command; CRC failure, time stamping failure, sequence number



**Text, STMA-20000** -

Losing a telegram containing an EB command ( STMA-9076 and  STMA-9078) leads to a CAT4 hazard in all cases. Taking into account the demand (app once per 1000h), the risk that losing one telegram containing an EB command leads to a CAT4 hazard is negligible.

Losing a telegram containing an EB command ( STMA-9076 and  STMA-9078) can contribute to a CAT2 hazard (EB commanding branch). Therefore the tolerable fault rate is  $3.3 \cdot 10^{-4}$ /hour (see  STMA-21062). A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $5.5 \cdot 10^{-5}$ /case.

**Fault, STMA-10635** - Detected losing one DMI telegram at the Profibus.

**Fault, STMA-10636** - Corrupted DMI telegram (leading to CRC failure).

**Text, STMA-19997** - Losing or corrupting (leads to losing) one DMI telegram ( STMA-10635 and  STMA-10636) leads to a short fault in the presented cab signals. The tolerable fault rate concerning this fault is  $5 \cdot 10^{-4}$ /hour. A DMI telegram containing cab signals is sent at every



change of the cab signal. This will be app. 25 times per hour. Therefore the tolerable fault rate assigned to losing a DMI telegram is  $2 \cdot 10^{-5}$ /case.

**Text, STMA-19996** - Common cause failures don't lead to more strict requirements:

A combination of losing an EB command and losing a DMI telegram will only result in a CAT2 hazard in case of very specific timing (see chapter: [STMA-16891 - Common cause faults](#)). The common cause failure will only lead to a CAT2 hazard if a DMI telegram is lost, leading to overspeed and an EB command is lost just after the driver reaction time. Meanwhile the DMI will have been reconnected, however too late. As there is a strict timing requirement concerning the relation between the failures the common cause factor is limited.

**Safety Requirement, STMA-11343** - The fault rate concerning "losing of one telegram" (according to subset057 to be detected by the safety layers) containing the following information:

- train speed ([STMA-9651](#)).
- EB telegram ([STMA-9076](#) and [STMA-9078](#)).
- DMI telegram containing CAB signals ([STMA-10635](#) and [STMA-10636](#)).

shall be less than  $2 \cdot 10^{-5}$ /case.

This includes the risk on corrupting a telegram in a way the corruption is detected in the CRC check.

#### 4.2 Undetected losing telegrams at the Profibus

**Text, STMA-19994** - The profibus communication as specified in the ERA ERTMS specification subset057 prescribes measures to detect the loss of a telegram; each telegram shall have a sequence number. It shall be checked if the prescribed protection, in combination with the fault rate of communication via the Profibus, is sufficient to reach the safety targets (tolerable fault rates) as specified in this paragraph.

#### 4.2.1 Safety levels of connections

**Text, STMA-21140** - For each logical connection a minimum safety level shall be specified. The minimum safety level depends on the acceptable fault rate for "undetected losing/corrupting telegrams at the Profibus, the undetected fraction when using CRC protection (safety level 2 and safety level 4) and the risk of losing or corrupting a telegram.

In this paragraph those figures (except the acceptable fault rate) are derived in order to determine the minimum safety level based on the acceptable fault rate.

**Text, STMA-20010** - The communication via Profibus is protected using a CRC (except for SL0 connections):

- SL0: no CRC
- SL2: 32 bit CRC, PU (undetected failure fraction according to ss057, 11.4.2):  $1.32 \cdot 10^{-8}$
- SL4: 48 bit CRC, PU (undetected failure fraction according to ss057, 11.3.4):  
 $3.564 \cdot 10^{-15}$

A safety factor  $k=10$  shall be taken into account when calculating the risk reduction due to

Tests performed in a lab environment showed a lost or corrupted fraction less than  $1 \cdot 10^{-7}$ . However for train circumstances a 1000 times higher failure rate is assumed:  $1 \cdot 10^{-5}/\text{case}$

The above leads to, a risk per sent telegram of undetected loss/corruption equal to  $P_{\text{the\_telegram\_is\_lost\_or\_corrupted}} \cdot P_{\text{loss\_or\_corruption\_is\_not\_detected}} \cdot k$ :

- SL0:  $1 \cdot 10^{-5}/\text{case} \cdot 1 \cdot 10 = 1 \cdot 10^{-4}/\text{case}$
- SL2:  $1 \cdot 10^{-5}/\text{case} \cdot 1.32 \cdot 10^{-8} \cdot 10 = 1,32 \cdot 10^{-12}/\text{case}$
- SL4:  $1 \cdot 10^{-5}/\text{case} \cdot 3.564 \cdot 10^{-15} \cdot 10 = 3.564 \cdot 10^{-19}/\text{case}$

Therefore the risk concerning an undetected corruption of a telegram depends on the safety level of the connection. Concerning the safety level of the connection with the STM controller the STM has to propose the safety level (will be SL4 for the STM controller). For the other connections the safety level is determined by the ETCS on-board and communicated to the STM's (packet STM-2). This could lead to a safety level which is too low to reach the safety targets of the STM ATB. Therefore minimum safety levels are defined for the connections. If the safety level communicated by the STM controller is lower, the connection shall be refused.

## 4.2.2 Not detecting the loss of one telegram

### 4.2.2.1 DMI telegrams

**Fault, STMA-10902** - Undetected losing a DMI telegram.

**Text, STMA-19990** - The tolerable fault rate to losing or corrupting a DMI telegram (🔴 STMA-10902) is  $5 \cdot 10^{-6}$ /hour (see **T** STMA-21061). The demand of 25 times per hour, the chance of undetected losing a DMI telegram shall be less than  $2 \cdot 10^{-7}$ /case.

**Safety Requirement, STMA-21144** - The failure rate concerning "not detecting the loss of a DMI telegram" (i.e. not detecting a missing sequence number), while one or more telegrams are lost shall be less than  $2 \cdot 10^{-7}$ /hour per case.

### 4.2.2.2 STM controller telegrams

**Text, STMA-19995** - The following faults due to (undetected) losing a telegram at the profibus concern the STM controller.

**Fault, STMA-9069** - Undetected loss of a Profibus telegram containing more restrictive brake parameters.

**Fault, STMA-9103** - Undetected loss of a Profibus telegram containing lower speed levels. (Option).

**Fault, STMA-9122** - Undetected loss of a telegram containing a state order.

**Text, STMA-19992** - Brake parameters (🔴 STMA-9069) are used for the ATBVv braking and for the ATBEG speed levels. Brake parameters are sent to the STM at startup. Speed levels are sent at startup, in case of changing direction, in case of change of the train composition and/or in case of the reception of a packet-44 containing new speed levels.

Brake parameters are sent only at startup (app. once per hour). Speed levels can also be sent while driving, however this will be more rare.

The tolerable fault rate to be assigned to 🔴 STMA-9069 is  $1 \cdot 10^{-9}$ /h (see **T** STMA-21070). Taking into account a demand of once per hour, the acceptable fault rate is  $1 \cdot 10^{-9}$ /case.

**Fault, STMA-9104** - Undetected loss of a Profibus telegram containing adhesion information.

**Text, STMA-19993** - The adhesion information is used for ATBVv, i.e. faults might lead to a CAT4 hazard. In combination with the low rate at which the function is used this type of fault is negligible compared to  $1 \cdot 10^{-9}$ /case.

**Fault, STMA-9126** - Undetected loss of a Profibus telegram containing the ETCS mode.

**Text, STMA-19991** - Assuming the wrong ETCS mode (🔴 STMA-9126) can lead to a transition to DA while the STM is not guarding the speed. This will be clear from the DMI and can therefore be handled as a availability failure, thus negligible compared to losing brake parameters.

#### **Safety Requirement, STMA-10883 -**

The failure rate concerning "not detecting the loss of an STM controller telegram" (i.e. not detecting a missing sequence number), while one or more telegrams are lost shall be less than  $1 \cdot 10^{-9}$ /case.

This relates to

- 🔴 STMA-9103 - Undetected loss of a Profibus telegram containing lower speed levels. (Option).
- 🔴 STMA-9069 - Undetected loss of a Profibus telegram containing more restrictive brake paramet...
- 🔴 STMA-9104 - Undetected loss of a profibus telegram containing adhesion information.
- 🔴 STMA-9126 - Undetected loss of a Profibus telegram containing the ETCS mode.
- 🔴 STMA-9122 - Undetected loss of a telegram containing a state order.

### **4.2.3 Not detecting the loss of multiple telegrams**

#### **4.2.3.1 Odometer**

**Text, STMA-19987** - Undetected losing multiple successive telegrams:

**Fault, STMA-9111** - Undetected and successive (>3 s) losing Profibus telegrams containing a new (higher) train speed.

**Text, STMA-19985** - Assuming the wrong train speed longer than 3 s will lead to a CAT3 hazard (🟡 STMA-8950 - CAT3 hazards, <  $7 \cdot 10^{-6}$ /operational hour). The acceptable fault rate assigned the undetected loss of multiple telegrams containing the train speed (🔴 STMA-9111) shall be less than app.  $2 \cdot 10^{-7}$ /hour (see 🟡 STMA-21072) . In one hour app.  $10^4$  telegrams containing speed information are sent (depending on the ETCS system app. between 1 and 5 per second). Therefore the acceptable fault rate is  $2 \cdot 10^{-11}$ /case (where a case is losing all telegrams during > 3 s without mitigation measure).

Therefore measures shall be taken in case the time since the last received speed information

exceeds a predefined time.

#### **Safety Requirement, STMA-16919 -**

The fault rate concerning not detecting or not mitigating the loss of multiple telegrams from the odometer containing the current train speed shall be less than  $2 \cdot 10^{-11}$ /case:

-  STMA-9111 - Undetected and successive (>3 s) losing Profibus telegrams containing a new (hig...


#### **4.2.4 Undetected corrupting a telegram**

**Text, STMA-19982** - The profibus communication as specified in the ERA ERTMS specification subset057 includes CRC protection for safety level 2 and safety level 4 communication to detect the corruption of a telegram. The required minimum safety level of the connections with ETCS on-board functions depend on the acceptable "failure rate".

**Text, STMA-21152** - The safety level can be defined per logical connection. Therefore the minimum safety requirements are derived per logical connection.

##### **4.2.4.1 DMI telegrams**

**Fault, STMA-9082** - An error in the communication of the DMI information, corrupting the CRC in a way the telegram is accepted by the ETCS on-board.

**Text, STMA-19980** - The tolerable functional fault rate concerning  STMA-9082 is  $7.5 \cdot 10^{-7}$ /h (see **T** STMA-21072). A DMI telegram containing cab signals is sent at every change of the cab signal. This will be app. 25 times per hour. Therefore the tolerable fault rate assigned to undetected corruption of a DMI telegram is  $3 \cdot 10^{-8}$ /case, therefore:

#### **Safety Requirement, STMA-21147 -**

The fault rate concerning corrupting a telegram to the DMI containing new cab signals shall be less than  $3 \cdot 10^{-8}$ /case,

#### 4.2.4.2 STM controller telegrams

**Fault, STMA-9084** - The brake parameters received via the Profibus are corrupted while being communicated.

**Fault, STMA-9066** - The speed levels received via the Profibus are corrupted while being communicated (Option).

**Text, STMA-19977** - Brake parameters (🔴 STMA-9084) are used for the ATBVv braking and for the ATBEG speed levels. Therefore corrupting brake parameters and corrupting speed levels (🔴 STMA-9066) will lead to the same type of hazard (level).

Undetected corruption of one of those telegrams leads to a hazard (wrong speed at the DMI and guarding the wrong speed: 🟡 STMA-8948 - CAT1 hazards,  $< 2 \cdot 10^{-8}$ /operational hour).

The tolerable fault rate to be assigned to this fault shall be less than  $1 \cdot 10^{-9}$ /h (see 🟡 STMA-21070). Brake parameters and speed levels are sent when starting up the system (app. once per hour). Therefore the acceptable fault rate is  $1 \cdot 10^{-9}$ /case.

**Fault, STMA-10899** - The adhesion information received via the Profibus are corrupted while being communicated.

**Text, STMA-19976** - Corrupted adhesion information (🔴 STMA-10899) can lead to a CAT4 hazard (🟡 STMA-8951 - CAT4 hazards,  $< 3.3 \cdot 10^{-3}$ /hour). The risk on overpassing the ATBVv braking curve and the frequency of sending adhesion telegrams is very low ( $\ll$  once per hour), therefore the tolerable fault rate is high (several orders of magnitude) compared to the tolerable fault rate concerning other types of telegrams.

#### **Safety Requirement, STMA-21149** -

The fault rate concerning corrupting a telegram from the STM controller shall be less than  $1 \cdot 10^{-9}$ /case,

#### 4.2.4.3 TIU

**Fault, STMA-17344** - Communication fault concerning the cabin selection.

**Text, STMA-19972** - A fault in the cabin selection (🔴 STMA-17344) only affects the coil selection as the DMI is selected independent from the cabin (DMI channel). Therefore this fault can lead to a CAT1 hazard (wrong speed at the DMI and guarding the wrong speed: 🟡

STMA-8948 - CAT1 hazards, <  $2 \cdot 10^{-8}$ /operational hour). The tolerable fault rate to be assigned to this fault shall be less than  $1 \cdot 10^{-9}$ /h (see 🟡 STMA-21070). As approximately every hour a telegram containing the cab selection is sent the tolerable fault rate concerning undetected corruption of a telegram containing the selected cabin is  $1 \cdot 10^{-9}$ /case.

The concerning information is sent by the TIU function (SL4 connection).

#### **Safety Requirement, STMA-21151** -

The fault rate concerning undetected corrupting a telegram from the TIU shall be less than  $1 \cdot 10^{-9}$ /case,

#### 4.2.4.4 BIU

**Fault, STMA-9079** - An undetected communication fault concerning an EB command (once).

**Fault, STMA-10064** - Multiple undetected communication faults concerning an EB command (>3 s).



**Text, STMA-19975** - An undetected communication fault concerning one or more EB commands (🔴 STMA-9079 and 🔴 STMA-10064) will lead to a CAT3 hazard (🟡 STMA-8950 - CAT3 hazards, <  $7 \cdot 10^{-6}$ /operational hour). The acceptable fault rate assigned the undetected loss of multiple telegrams containing the an EB command shall be less than app.  $1 \cdot 10^{-6}$ /hour. A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account).

This results in an acceptable fault rate <  $1.7 \cdot 10^{-7}$ /hour.

**Safety Requirement, STMA-22515** - The fault rate concerning undetected corrupting a telegram from the BIU shall be less than  $1.7 \cdot 10^{-7}$ /hour.

#### 4.2.4.5 Odometer



**Fault, STMA-10053** - The current train speed received via the Profibus is (undetected) corrupted while being communicated.

**Text, STMA-19978** - Assuming the wrong train speed during a short time (app. 0.5 s) (  STMA-10053) leads to a CAT4 hazard (sending the EB command too late,  STMA-8951 - CAT4 hazards,  $<3.3 \cdot 10^{-3}/\text{hour}$ ) in case the loss of the telegram containing the current train speed coincides with the necessity to sent an EB command.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account).

Therefore the acceptable fault rate is  $5.5 \cdot 10^{-4}/\text{case}$ .

**Fault, STMA-9085** - The current train speed received via the Profibus is (undetected) corrupted while being communicated multiple times in the same way.

**Text, STMA-19970** - Assuming the wrong train speed longer than 3s will lead to a CAT3 hazard (  STMA-8950 - CAT3 hazards,  $<7 \cdot 10^{-6}/\text{operational hour}$ ). The acceptable fault rate assigned the undetected loss of multiple telegrams containing the train speed shall be less than app.  $1 \cdot 10^{-6}/\text{hour}$ . In one hour app.  $10^4$  telegrams containing speed information are sent. A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000, see  D2.2 Current RAMS performance and RAMS targets, is taken into account).

Therefore the acceptable fault rate is  $1.7 \cdot 10^{-7}/\text{case}$ .

**Text, STMA-37265** - The odometer connection (multicast) is prescribed at SL4

## 5 Storing data

**Text, STMA-19939** - The impact of storage faults depends on the safety relevance of the data. As technical difference can be made between the way different types of data are calculated (e.g. redundant calculation, checks etc.), separate safety requirements will be set for different groups of data.

**Text, STMA-19937** - It is taken into account that all data except input data is recalculated every cycle, therefore only corruption of input data and state information will have an impact longer than one cycle. Faults having effect less than 30 ms are not assumed to be relevant.

**Text, STMA-20259** - Faults in storing data include the process of storing, being stored and



reading of the data. As it is likely that data for different functions will be stored in the same (type of) environment there is a dependence between the faults. If a part of the memory gets corrupted it is more likely other parts of the same memory will also be corrupted. The assumption that all data is stored in the same environment is a worst case assumption.

**Text, STMA-19962** - The impact of storage faults depends on the safety relevance of the data. As technical difference can be made between the way different types of data are stored (e.g. double storage, extra coding etc.), separate safety requirements will be set for different groups of data.

### 5.1 Storage related to CAT1 hazards

**Text, STMA-19960** - Storage faults concerning input (or default) information potentially leading to a CAT1 hazard are divided in different groups, however the same technical safety requirement shall apply as the assigned tolerable fault rates to these faults are equal. Storage faults are divided in critical fault rates (difficult to implement) and other storage faults. Concerning the critical faults individual tolerable fault rates are derived. Concerning the other fault rates a general figure is given.

**Text, STMA-37266** - Faults concerning configuration information:

**Fault, STMA-9064** - The default speed values in permanent memory of the "ATB function processor" are corrupted.

**Fault, STMA-9065** - The speed levels received via the Profibus are corrupted while being stored in memory. (Option).

**Fault, STMA-9068** - The brake parameters received via the Profibus are corrupted while being stored in memory.

**Fault, STMA-17345** - Storage fault concerning the cabin selection.

**Fault, STMA-9091** - Multiple storage faults: The ATBEG code is corrupted while being stored  $\geq 3$  s.

**Text, STMA-19961** - A possible consequence of these faults (🔴 STMA-9064, 🔴 STMA-9065, 🔴 STMA-9068, 🔴 STMA-17345) is that faulty speed levels are shown to the driver and the speed is guarded accordingly.

The tolerable fault rate assigned to single storage faults potentially leading to these faults is  $1 \cdot 10^{-9}$ /hour (see **T** STMA-21070).

The fault can be distinguished in "corrupting stored data" and "read/write faults". The latter shall be defined per case:

- demand concerning writing: app. once per hour
- demand concerning reading: several times every 10 ms, however only in case of a permanent fault which causes every read (during at least 3 s, i.e. 300 times) to be faulty in the same manner will lead to a hazard. Therefore the fault rate per time is relevant.

**Text, STMA-37267** - Faults concerning the ATBEG code:

**Fault, STMA-9110** - The track signal is intermittent corrupted while being stored.

**Text, STMA-19959** - A possible consequence of these faults (🔴 STMA-9110 and 🔴 STMA-9091) is that faulty speed levels are shown to the driver and the speed is guarded accordingly. The tolerable fault rate assigned to multiple storage faults potentially leading to a CAT1 hazard is  $1 \cdot 10^{-9}$ /hour (see 📄 STMA-21070).

The fault can be distinguished in "corrupting stored data" and "read/write faults". The latter shall be defined per case:

- demand concerning writing: every 10 ms, however only in case of a permanent fault which causes every read (during at least 3 s, i.e. 300 times) to be faulty in the same manner will lead to a hazard. Therefore the fault rate per time is relevant.
- demand concerning reading: every 10 ms, however only in case of a permanent fault which causes every read (during at least 3 s, i.e. 300 times) to be faulty in the same manner will lead to a hazard. Therefore the fault rate per time is relevant.
- demand concerning intermittent corruption of the track signal: >16 times during 0.8 s. To cause a hazard multiple faults are needed. Therefore the requirement shall be formulated as a incident frequency per time of multiple failures  
The time 0.8 s is the "minimum decoding time" necessary to recognize a valid code.  
Therefore shorter disturbances cannot be recognized as a valid code.

**Safety Requirement, STMA-10880** -

The fault rate concerning corruption in memory of the following information:

- default speed levels
- speed levels, brake parameters or cab selection

shall be less than  $1 \cdot 10^{-9}$ /hour

**Safety Requirement, STMA-21156** -

The fault rate concerning the process of writing the following information

- speed levels, brake parameters or cab selection

shall be less than  $1 \cdot 10^{-9}$ /case.

#### **Safety Requirement, STMA-21157 -**

The fault rate concerning a permanent fault (> 3s) while reading the following information:

- default speed levels
- speed levels, brake parameters or cab selection
- ATBEG code

shall be less than  $1 \cdot 10^{-9}$ /hour.

#### **Safety Requirement, STMA-10878 -**

The fault rate concerning intermittent faults concerning the track signal (🔴 STMA-9110), during > 0.8s, intermittent with an ATBEG code frequency and a valid duty cycle, while reading or writing the following information shall be less than  $1 \cdot 10^{-9}$ /hour.

## **5.2 Storage faults related to CAT3 hazards**

**Text, STMA-19956 -** Storage faults concerning input (or default) information potentially leading to a CAT3 hazard are divided in different groups, however the same technical safety requirement shall apply as the assigned tolerable fault rates to these faults are equal.

**Fault, STMA-9127 -** A storage fault concerning "MODE\_STM".

**Text, STMA-19957 -** The consequence of a fault in the stored value of "MODE\_STM" (🔴 STMA-9127) can be (if sleeping or non-leading is stored) that the STM ATB reports "DA" while not guarding the train speed. In that case no cab signals will be shown to the driver, i.e. a CAT3 fault.

The acceptable fault rate concerning the latter fault is  $2.4 \cdot 10^{-8}$ /hour (see 📖 STMA-21063).

The fault can be distinguished in "corrupting stored data" and "read/write faults". The latter shall be defined per case:

- demand concerning writing: app. once per hour
- demand concerning reading:
  - every 10ms (a CAT3 hazard will only be caused in case of multiple identical faults),
  - A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account).

**Fault, STMA-9075** - A storage fault concerning the conditions over speed and brake operation, or concerning timers (>30 ms).

**Text, STMA-19944** - The overspeed condition, brake operation (>30 ms) and timers affect the time before an EB command is sent (🔴 STMA-9075). This can lead to a delay in commanding the EB for more than 3 s (as timers run for more than 3 s, a reset has an effect longer than 3 s). CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see 📄 STMA-21072), CAT3:  $<2.4 \cdot 10^{-8}$ /hour (see 📄 STMA-21063).

The fault can be distinguished in "corrupting stored data" and "read/write faults". The latter shall be defined per case

- demand concerning reading/writing:

Every 10ms, i.e. continuously.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account).

The effect disappear if the fault is not made anymore (i.e. transient faults have a one time effect, static faults shall be detected)

Therefore the fault will cause a hazard if it coincides with the moment the EB should have been commanded, i.e. 6 times per hour.

**Fault, STMA-43705** - A storage fault; The EB command is not stored correctly (once).

**Text, STMA-19954** - If an EB command is not stored correctly (e.g. is stored as release instead of command, 🔴 STMA-43705) then a valid telegram (valid time stamp, CRC and sequence number) will be sent with the wrong information, leading to not commanding the EB.

CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see 📄 STMA-21072), CAT3:  $<2.4 \cdot 10^{-8}$ /hour (see 📄 STMA-21063).

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $4 \cdot 10^{-9}$ /case. An EB command is not stored for a long time (it shall be sent immediately), therefore the fault rate per time (hour) is not relevant.

**Fault, STMA-9098** - A storage fault concerning the ATBEG or Vv state.

**Text, STMA-19945** - A fault in the ATBEG or ATBVv state (🔴 STMA-9098) can have effect for a longer period (>3 s) as timers leading to a state transition are reset when entering a state. A faulty ATBEG state could lead to not sending an EB command in case of overspeed.

CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see **T** STMA-21072),  
CAT3:  $< 2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

The fault will only have effect in case an EB command has to be sent.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $4 \cdot 10^{-9}$ /case. The ATBEG and ATBVv state are recalculated and stored every 10 ms (as a safety measure to limit the number of safety critical variables), therefore the fault rate per time (hour) is not relevant.

**Fault, STMA-10052** - The current train speed information is corrupted while being stored in memory (once).

**Text, STMA-19952** - Fault **STMA-10052** can result (if the faulty value is too low) to a reset of the timers (as the current train speed is refreshed less often than every 30 ms), timing the over speed. Therefore an EB command can be delayed by more than 3 s.

CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see **T** STMA-21072),  
CAT3:  $< 2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

The fault will only have effect in case an EB command has to be sent.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $4 \cdot 10^{-9}$ /case. A new value for the current train speed is stored at least every second, therefore the fault rate per time (hour) is not relevant.

**Fault, STMA-10060** - A storage fault concerning timers.

**Text, STMA-19953** - The overspeed condition, brake operation (>30 ms) and timers affect the time before an EB command is sent.

Fault **STMA-10060** can lead to a delay in commanding the EB for more than 3 s.

CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see **T** STMA-21072),  
CAT3:  $< 2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

The fault will only have effect in case an EB command has to be sent.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $4 \cdot 10^{-9}$ /case. The longest times to be measured are app. 5 s (warning time for the driver), after 5 s a fault doesn't have effect, therefore the fault rate per time (hour) is not relevant.

**Text, STMA-19935** - Multiple storage faults leading to:

CAT1 (and condition, in combination with another fault):  $<2 \cdot 10^{-7}$ /hour (see **T** STMA-21072),  
CAT3:  $<2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

**Fault, STMA-9074** - A storage fault concerning input information concerning brake operation,  $\geq 3$  cycles.

**Fault, STMA-9087** - The current train speed information is corrupted while being stored in memory multiple times.

**Fault, STMA-10063** - Multiple storage faults concerning the ATBEG or Vv state ( $>3$  s).

**Fault, STMA-10068** - Multiple storage faults; The EB command is not stored correctly ( $>3$  s).

**Fault, STMA-10066** - Multiple storage faults concerning an EB telegram, i.e. the telegram is not correctly stored ( $>3$  s).

**Fault, STMA-11595** - Multiple storage faults: The ATBEG code is corrupted while being stored  $\geq 3$  times.

**Text, STMA-19942** - The tolerable fault rate concerning the above faults ( **F** STMA-9074, **F** STMA-9087, **F** STMA-10063, **F** STMA-10066, **F** STMA-10068 and **F** STMA-11595 ) is  $2 \cdot 10^{-8}$ /hour.

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the tolerable fault rate per case is  $4 \cdot 10^{-9}$ /case  
The values are refreshed every cycle, therefore the fault rate per time (hour) is not relevant.

### 5.3 Storage related to CAT2/CAT4 hazards

**Text, STMA-19950** -

Storage faults potentially leading to a CAT4 hazard:

CAT4:  $<5 \cdot 10^{-5}$ /hour,

**Fault, STMA-9086** - The adhesion information is corrupted while being stored in memory.

**Fault, STMA-9092** - The ATBVv code is corrupted when being stored in memory.

**Text, STMA-19948** - The tolerable fault rates concerning ( **F** STMA-9086 and **F** STMA-9092 ) is  $5 \cdot 10^{-5}$ /hour.

The function is demanded every time a signal at danger (fitted with ATBVv) is approached (twice per hour).

This leads to a tolerable fault rate per case of  $2.5 \cdot 10^{-5}$ /case.

**Text, STMA-63510** - Storage faults potentially leading to a CAT2 hazard (and condition) or a CAT4 hazard concerning the EB command

CAT2 (and condition):  $< 2.5 \cdot 10^{-6}$ /hour (see **T** STMA-21065) , CAT4:  $< 5 \cdot 10^{-5}$ /hour (see **T** STMA-21060).

**Fault, STMA-9094** - A storage fault concerning an EB telegram, i.e. the telegram is not correctly stored (once).

**Fault, STMA-11290** - A storage fault concerning input information concerning brake operation,  $< 3$  cycles.

**Text, STMA-21938** - The tolerable fault rates concerning ( **🔴** STMA-9094 and **🔴** STMA-11290) is  $2.5 \cdot 10^{-6}$ /hour (see **T** STMA-21065).

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the tolerable fault rate per case is  $4 \cdot 10^{-7}$ /case.

**Text, STMA-63512** - requirement, see **📄** STMA-21940 - [Generic safety requirement concerning storing data.](#)

#### 5.4 Storage related to CAT5 hazards

**Text, STMA-63505** - Storage faults potentially leading to a CAT2 hazard (and condition) or a CAT5 hazard concerning DMI items

CAT2 (and condition):  $< 1 \cdot 10^{-5}$ /hour (see **T** STMA-21065), CAT4:  $< 5 \cdot 10^{-5}$ /hour (see **T** STMA-21060).

**Fault, STMA-9083** - One storage fault; No or wrong DMI telegram is build/stored while the cab signal changed.

**Text, STMA-21939** - The tolerable fault rates concerning ( **🔴** STMA-9083) is  $1 \cdot 10^{-5}$ /hour (see **T** STMA-21065).

It is assumed the cab signal will change 25 times per hour.

(leading to  $4 \cdot 10^{-7}$ /case).

**Text, STMA-63506** - requirement, see **📄** STMA-21940 - [Generic safety requirement concerning storing data.](#)

### 5.5 Generic safety requirement concerning storing data

**Text, STMA-63514** - From paragraph [STMA-21163 - Storage faults related to CAT3 hazards](#) and paragraph [STMA-21933 - Storage related to CAT2/CAT4 hazards](#) the most restrictive requirement is used as a generic requirement concerning data storage for variables in general:

#### **Safety Requirement, STMA-11338 -**

The fault rate concerning "storage faults" concerning the corruption of stored data shall be less than  $2 \cdot 10^{-7}$ /hour.

#### **Safety Requirement, STMA-11339 -**

The fault rate concerning "storage faults" concerning the corruption of data while reading or writing shall be less than  $3.3 \cdot 10^{-8}$ /case.

## 6 Calculations

**Text, STMA-19938** - Faults in calculations include all aspects between reading the data from memory and storing the results. The safety relevance of calculation faults depends on the output information which is generated. As it is likely that calculations will be performed at the same processor, however calculations concerning EB commands are different from calculations concerning DMI commands. Therefore those are considered independent.

**Text, STMA-19926** - The impact of a calculation fault concerning specific information will be similar to the impact of a storage fault concerning the information. Therefore for underpinning the assignment a reference to the previous chapter, [STMA-14785 - Storing data](#), is made.

**Text, STMA-19927** - As calculations are repeated every cycle based on the (stored) input data and the state variables, and as transitions to less restrictive states are only made after 3 cycles, single calculation faults cannot prevent the STM from commanding the EB due to overspeed (ATBEG). Single faults can prevent commanding the EB due to ATBVv requirements as those conditions can be present very short only (e.g. passing a "stop beacon" at a high speed).



## 6.1 Calculation faults concerning CAT1 hazards

**Text, STMA-19924** - Calculation faults potentially leading to a CAT1 failure, i.e. tolerable fault rate:  $< 1 \cdot 10^{-9}$ /hour (see **T** STMA-21070).

**Fault, STMA-9042** - Multiple calculation faults: The wrong ATBEG code is calculated during  $>3$  s.

**Fault, STMA-16986** - Multiple calculation faults ( $>3$  s) concerning the speed levels.

**Text, STMA-21954** -

The calculation of the speed levels is based on the default speed levels and the braking parameters.

The calculation of the ATBEG code is a.o. based on the cabin selection.

**Text, STMA-21956** -

The tolerable fault rate concerning **STMA-9042** and **STMA-16986** is  $1 \cdot 10^{-9}$ /hour (see **T** STMA-21070). The demand is continuous and only static failures leading to the same fault every cycle during  $>3$  s (i.e.  $>300$  times) are relevant.

Therefore these fault rates are defined per hour, not per case.

**Text, STMA-63503** - requirement, see **STMA-21989** - [Generic safety requirement concerning calculations](#)

## 6.2 Calculation faults concerning CAT2

**Text, STMA-21968** -

The tolerable fault rate assigned to calculation faults leading to a CAT2 hazard, can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT2:  $< 3 \cdot 10^{-7}$ /hour (see **T** STMA-21064).

**Fault, STMA-10074** - Multiple calculation faults: The wrong ATBEG code is calculated due to a random fault.  $\geq 3$  times. ( $<3$  s).

**Text, STMA-21988** - The tolerable fault rate concerning **STMA-10074** is  $3 \cdot 10^{-7}$ /hour (see **T** STMA-21064). This figure concerns multiple calculation faults ( $> 3$ ), thus a permanent failure (static). Therefore this fault rate is defined per hour, not per case.

**Text, STMA-21979** -

The tolerable fault rate assigned to calculation faults leading to a CAT2 hazard in combination

with another fault, can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT2 (and condition):  $< 1 \cdot 10^{-5}$ /hour (see **T** STMA-21065).

**Fault, STMA-10637** - Failure in a CRC calculation of a DMI telegram to the ETCS on-board.

**Text, STMA-21992** - The tolerable fault rate concerning **STMA-10637** is  $1 \cdot 10^{-5}$ /hour, the function is demanded 25 times per hour, leading to a tolerable fault rate per case of  $4 \cdot 10^{-7}$ /case.

**Text, STMA-63504** - requirement, see **STMA-21989 - Generic safety requirement concerning calculations.**

### 6.3 Calculation faults concerning CAT3

**Text, STMA-21969** -

The tolerable fault rate assigned to calculation faults leading to a CAT3 hazard, i.e. not sending an EB command, and which can contribute to a CAT1 hazard can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT1 (and condition):  $< 2 \cdot 10^{-7}$ /hour (see **T** STMA-21072) , CAT3:  $< 2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

**Fault, STMA-9073** - Multiple calculation faults concerning train speed for more than 3 s.

**Fault, STMA-9096** - A calculation fault concerning input information concerning brake operation,  $\geq 3$  cycles.

**Fault, STMA-10062** - Multiple calculation faults concerning the ATBEG or Vv state ( $> 3$  s).

**Fault, STMA-10065** - Multiple calculation faults concerning an EB telegram, i.e. the telegram is not correctly constructed ( $> 3$  s)

**Fault, STMA-10067** - Multiple calculation faults; The EB command is not determined although the ATBEG or Vv state is intervention ( $> 3$  s).

**Text, STMA-21993** - The tolerable fault rate concerning **STMA-9073**, **STMA-9096**, **STMA-10062**, **STMA-10065** and **STMA-10067** is  $2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063). A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the tolerable fault rate per case is  $4 \cdot 10^{-9}$ /case.

**Text, STMA-19932** -

The tolerable fault rate assigned to calculation faults leading to a CAT3 hazard, i.e. not sending

an EB command, and which can contribute to a CAT2 hazard can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.




CAT2 (and condition):  $< 2.5 \cdot 10^{-6}$ /hour (see **T** STMA-21065) , CAT3:  $< 2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

**Fault, STMA-9077** - EB command is not given while the ATBEG or Vv state changed to intervention/STS,  
e.g. a calculation fault when building the EB command message and/or telegram.

**Fault, STMA-9081** - A calculation fault; The EB command is not determined although the ATBEG or Vv state is intervention (once).

**Fault, STMA-10061** - A calculation fault concerning timers .

*note: Depending on the implementation this will have effect on the state of the timer, or will only have effect one cycle.*

**Text, STMA-21994** - The tolerable fault rate concerning  STMA-9077,  STMA-9081 and  STMA-10061 is  $2.4 \cdot 10^{-8}$ /hour (see **T** STMA-21063).

A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account). Therefore the on-demand fault rate may be  $4 \cdot 10^{-9}$ /case.

**Text, STMA-63508** - requirement, see  STMA-21989 - [Generic safety requirement concerning calculations.](#)

#### 6.4 Calculation faults concerning CAT4

**Text, STMA-21960** -

The tolerable fault rate assigned to calculation faults leading to a CAT4 hazard , i.e. not sending an EB command, and which can contribute to a CAT2 hazard can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT2 (and condition):  $< 3 \cdot 10^{-7}$ /hour (see **T** STMA-21064), CAT4:  $< 5 \cdot 10^{-5}$ /hour (see **T** STMA-21060).

**Fault, STMA-9093** - A calculation fault concerning the conditions over speed and brake operation, or concerning timers.







**Fault, STMA-9080** - A calculation fault concerning an EB telegram, i.e. the telegram is not correctly constructed (once).

**Fault, STMA-9097** - A calculation fault concerning the ATBEG or Vv state.

**Fault, STMA-11291** - A calculation fault concerning input information concerning brake

operation, < 3 cycles.


**Fault, STMA-10054** - Calculation fault concerning train speed for more than three periods.

**Text, STMA-21995** - The tolerable fault rate concerning  STMA-9093,  STMA-9080,  STMA-9097,  STMA-11291 and  STMA-10054 is  $3 \cdot 10^{-7}$ /hour (see  STMA-21064). A lower speed is supervised app. 6 times per hour (in the tolerable hazard rate, a driver failure rate of 1:6000 is taken into account).


Therefore the tolerable fault rate per case is  $5 \cdot 10^{-8}$ /case.

**Text, STMA-21963** -

The tolerable fault rate assigned to calculation faults leading to a CAT4 hazard , i.e. not sending an EB command, can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT4:  $< 5 \cdot 10^{-5}$ /hour (see  STMA-21060),

**Fault, STMA-9058** - Calculation fault concerning the ATBVv signal.

**Text, STMA-21996** - The tolerable fault rate concerning  STMA-9058 is  $5 \cdot 10^{-5}$ /hour.

Stopping in rear of a signal at danger is guarded by ATBVv app. twice per hour.

Therefore the tolerable fault rate per case is  $2.5 \cdot 10^{-5}$ /case

**Text, STMA-63509** - requirement, see  STMA-21989 - [Generic safety requirement concerning calculations](#)



## 6.5 Calculation faults concerning CAT5

**Text, STMA-21965** -

The tolerable fault rate assigned to calculation faults leading to a CAT5 hazard , i.e. cab signal fault, and which can contribute to a CAT1 hazard can be the same for all faults. The most restrictive requirement is determined by the tolerable fault rate and the demand frequency of the function.

CAT1 (and condition):  $< 7.5 \cdot 10^{-6}$ /hour (see  STMA-21072) , CAT5:  $< 5 \cdot 10^{-6}$ /hour (see  STMA-21061),

**Fault, STMA-9099** - One calculation fault; wrong cab signal determined from the code or telegram with wrong cab signal (text) is sent.




**Text, STMA-21997** - The tolerable fault rate concerning  STMA-9099 is  $7.5 \cdot 10^{-5}$ /hour (see  STMA-21072). The function demand is 25 times per hour.

Therefore the tolerable fault rate per case is  $2 \cdot 10^{-6}$ /case.

Text, **STMA-63507** - requirement, see  **STMA-21989** - [Generic safety requirement concerning calculations](#).

## 6.6 Generic safety requirement concerning calculations

**Safety Requirement, STMA-10879** - The fault rate concerning "multiple calculation faults" concerning the following information

- ATBEG code ( **STMA-9042** and  **STMA-10074**).
- Speed levels ( **STMA-16986**).


shall be less than  $1 \cdot 10^{-9}$ /hour, thus less than  $1 \cdot 10^{-12}$ /case.

**Safety Requirement, STMA-11340** - The fault rate concerning calculation faults (all faults mentioned in chapter) shall be less than  $2.4 \cdot 10^{-8}$ /hour and less than  $2 \cdot 10^{-6}$ /case.



## 7 Input faults (other than via Profibus)

Text, **STMA-63511** - Faults in the input circuits are not categorized according to the technical implementation as those are too diverse.



### 7.1 Faults concerning CAT 1 hazards

Text, **STMA-21999** - Below input faults potentially leading to a CAT1 failure, i.e. tolerable fault rate:  $< 1 \cdot 10^{-9}$ /hour (see  **STMA-21070**) are detailed. Those faults will also lead to a CAT2 hazard, however long (CAT1) and short (CAT2) faults are not distinguished.

**Fault, STMA-9040** - The "input circuit" generates an AM modulated 75 Hz signal in the right and left coil signal, meeting the requirements for a valid code.

Text, **STMA-19920** - The tolerable fault rate concerning  **STMA-9040** is  $1 \cdot 10^{-9}$ /hour (see  **STMA-21070**). The function is executed continuous, the fault rate per case is not relevant.

### **Safety Requirement, STMA-9002** -

The fault rate concerning intermittent faults in the analogue input circuits ( **STMA-9040**), during  $> 0.8$  s ("minimum decoding time", see  **STMA-19959**), intermittent with an ATBEG code frequency and a valid duty cycle, shall be less than  $1 \cdot 10^{-9}$ /hour.

**Fault, STMA-9041** - The "input circuit" introduces a delay in the input circuits for the coil signal

with a difference in delay between left and right in the order of a halve period of 75 Hz (i.e. app. 6,5 ms). This way signals from an external source can meet the requirements for a valid code.

**Text, STMA-19921** - Due to a phase shift between the left and the right coil signal (app. 180 degrees for valid codes) code from external sources will be accepted and code from the current section will not be accepted. The risk that this fault leads to a CAT1 hazard shall be less than  $1 \cdot 10^{-9}$ /hour (see **T** STMA-21070).

This fault can either lead to a lot of disturbance, or to accepting unsafe code. The latter is reached if an ATBEG code (with a sufficient amplitude) with an external source is found in the track signal before a valid ATBEG code shall be recognized. This will be the case in at most (very conservative estimation) 10 % of the faults.

Resulting tolerable fault rate: The acceptable fault rate concerning this fault is  $1 \cdot 10^{-8}$ /hour.

**Safety Requirement, STMA-9003** - The fault rate for differences in delays (i.e. a delay in one of the input circuits/IO Channels  $> 0,5$  ms compared to the other) between different analogue input signals (🔴 STMA-9041) shall be less than  $1 \cdot 10^{-8}$ /h.

**Fault, STMA-9043** - The “input circuit” modulates the present 75 Hz signal in the left and right coil signal with the same modulation frequency and phase.

**Text, STMA-19919** - Due to an intermittent fault causing modulation of both, the left and right coil signal, at the same frequency and phase a valid ATBEG signal could be simulated. The risk that this fault (🔴 STMA-9041) leads to a CAT1 hazard shall be less than  $1 \cdot 10^{-9}$ /hour (see **T** STMA-21070).

This fault can lead to disturbance, or a constant 75 Hz signal can be modulated. The latter will lead to simulating a valid code, thus presenting and guarding an unsafe speed level. This will be the case in at most (very conservative estimation) 10 % of the faults.

Resulting tolerable fault rate: The acceptable fault rate concerning this fault is  $1 \cdot 10^{-8}$ /hour.

**Safety Requirement, STMA-9004** - The input circuits shall not modulate the left and right input signal simultaneously with an ATBEG frequency (🔴 STMA-9043) with a chance higher than  $5 \cdot 10^{-10}$ /h.

**Safety Requirement, STMA-22484** - The connectors shall not modulate the left and right input signal (e.g. due to a loose connector) simultaneously with an ATBEG frequency (🔴 STMA-9043) with a chance higher than  $5 \cdot 10^{-10}$ /h.

**Fault, STMA-9044** - The “input circuit” corrupts both coil signals in a way a part of the pulses (e.g. 50%) will not be (sufficiently) visible for the decoder. I.e. the decoder will detect a lower code frequency.

**Text, STMA-20005** - Blocking a part of the pulses from both coil signals can lead to code simulation, thus presenting and guarding an unsafe speed level (CAT1). The chance that this fault, when occurring, will lead to a hazard is high, therefore 100 % is taken into account.

**Safety Requirement, STMA-9005** - The fault rate for intermittent blocking the analogue input signals (🔴 STMA-9044) shall be less than  $1 \cdot 10^{-9}/h$ .

**Fault, STMA-33645** - Analogue configuration signal corrupted.

**Safety Requirement, STMA-33646** - The fault rate concerning undetected corruption of the configuration signal shall be less than  $2.4 \cdot 10^{-8}/hour$ .

## 7.2 Faults concerning CAT3 hazards

**Fault, STMA-9089** - The “input circuit” for digital brake applied information corrupts the information consequently  $\geq 3$  cycles.

**Fault, STMA-9090** - The “input circuit” for analogue brake applied information corrupts the information consequently  $\geq 3$  cycles.

**Text, STMA-20006** - Corruption of brake handle applied information longer than 30 ms can lead to a delay in commanding the EB in case of overspeed of more than 3 s (app. 5 s). This is a CAT3 hazard with a tolerable fault rate  $2.4 \cdot 10^{-7}/hour$ . Further the fault contributes to a CAT1 hazard (no EB command), thus a tolerable fault rate  $2 \cdot 10^{-7}/hour$ .

It is assumed that the fault will be recognized and mitigated within 1 hour (as the fault is visible to the driver).

**Safety Requirement, STMA-9006** - The fault rate for corrupting digital brake applied information  $\geq 3$  cycles (🔴 STMA-9089) shall be less than  $2 \cdot 10^{-7}/h$ .

**Safety Requirement, STMA-9007** - The fault rate for corrupting analogue brake applied information  $\geq 3$  cycles (🔴 STMA-9090) shall be less than  $2 \cdot 10^{-7}/h$ .

**Fault, STMA-11289** - The “input circuit” for digital brake applied information corrupts the information  $< 3$  cycles.

**Text, STMA-20003** - Corruption of brake handle applied information during less than 3 cycles may not be regarded as initial brake operation, otherwise the effect of the fault would last longer than 3 cycles.

**Requirement, STMA-11346** -

Corruption of "brake applied" information (BHA, BSO or brake pipe pressure) during less than 30 ms (3 cycles) shall not have any effect longer than 30 ms.





### 7.3 Faults concerning CAT4 hazards



**Fault, STMA-9056** - The right coil is not connected (e.g. defect in the connector).



**Fault, STMA-9057** - The "input circuit" doesn't pass and digitize the analogue signal containing a ATBVv frequency.



**Fault, STMA-9062** - The "input circuit" generates a digitized signal not present in the analogue input at exactly one of the ATBVv release frequencies.

**Text, STMA-20004** - The above faults can lead to not guarding the distance to a signal at danger (ATBVv).

The tolerable fault rate concerning  STMA-9056,  STMA-9057 and  STMA-9062 is  $5 \cdot 10^{-5}$ /hour (see  STMA-21060) . The demand concerning this function is at every passage of a beacon announcing a signal at danger, i.e. 6 times per hour.

**Safety Requirement, STMA-9013** - The right coil connector shall not be loose ( STMA-9056) with a chance higher than  $5 \cdot 10^{-5}$ /h. (see  STMA-21060).


**Safety Requirement, STMA-9014** - The input circuit shall pass the right analogue coil signal" ( STMA-9057) with a fault rate lower than  $5 \cdot 10^{-5}$ /h (see  STMA-21060).

**Safety Requirement, STMA-10886** - The input circuit for the right coil signals shall not generate a component with an ATBVv frequency in the input signal, with a sufficient magnitude" ( STMA-9062) with a chance higher than  $5 \cdot 10^{-5}$ /h (see  STMA-21060).

## 8 Miscellaneous

**Text, STMA-20001** - Other fault which can cause CAT1 to CAT5 hazards are defined below:  
CAT1:

**Safety Requirement, STMA-11948** - An undetected storage fault in the program code, leading to a CAT1 failure.

**Requirement, STMA-16892** - The fault rate for  STMA-11948 shall be less than  $1 \cdot 10^{-10}$ /hour.



## 9 Common cause faults

### Text, STMA-22136 -

CAT1 and CAT2 hazards can be caused by combinations of faults, one leading to false cab signals at the DMI and one leading to not braking. Those faults are included in the analysis of the previous section. To have some margin for "common cause/mode" faults, leading to an increased fault rate concerning the combination of the faults, a margin (factor 0.1) has been added to the tolerable fault rates. However in case of faults with a high "common cause factor" this margin could be insufficient. Therefore possible common cause and common mode faults are analyzed in this chapter, in order to formulate requirements preventing those faults.

### Text, STMA-20002 -

Common mode faults in displaying cab signals and not commanding the EB, will only have an effect if they occur long enough to first mislead the driver and afterwards due to the same failure the EB is not commanded.

**Text, STMA-63513** - Common cause faults (one leading to displaying the wrong cab signal and the other one leading to not braking) could concern:

- Communication via the Profibus.
- Storage of data.
- Calculations.

**Text, STMA-19983** - To avoid a design leading to critical common cause faults, requirements concerning the design will be derived based on the fault analysis above. The following faults can expected to have a common cause factor:

- Communication faults at the same channel concerning different information.  
In the case of the STM ATB different safety critical information is communicated via the Profibus connection between STM ATB and ETCS on-board.
- Storage faults, as far as the information concerned is stored in the same device.  
All information needed in the ATBEG calculations will be stored at the same device.  
Therefore storage faults concerning this information will have a common cause factor.
- All faults concerning calculations which have to be done at the same device will be dependent.  
For some calculations it's unavoidable to do them at the same processor, some

calculations could be split. However as the STM ATB application is not very demanding, it is assumed that all safety critical calculations will be done in one device. Therefore all safety critical calculations are assumed to be dependent.

### 9.1 Common cause failures concerning communication

**Text, STMA-19955** - Undetected corruption of multiple telegrams (leading to a CAT1 hazard): -

Communication faults can lead to corrupted DMI data and to not sending an EB command. Because of the timing constraints concerning the time between the faults the common cause factor is assumed to be low. This is checked in the FMEA which is (to be) performed on the design.

**Text, STMA-19981** -

Faults causing lost telegrams have a high common cause factor, as it can be assumed that if the Profibus communication is disturbed more telegrams will be effected (unless the disturbance is a single spike).

However multiple failures lead to the same hazard category as a single failure (CAT 1). Thus the risk of having common mode faults is low, while those would lead to the same tolerable fault rate.

**Text, STMA-20014** -

Therefore the common mode factor concerning random faults, the common mode factor concerning faults with a short duration and common cause faults which are detected within 2 s will be very small (to be proven in the design). Longer lasting defects, especially undetected, can lead to both a CAT3/4 and CAT5 hazard and thus to a CAT1 hazard. Fault types to be considered:

- Undetected loss of a telegram at the Profibus;  
If a DMI telegram got lost (e.g. due to a loose cable) and this is not detected, it is likely the EB command following the cab signal change will also be lost.  
*note: if a separate sound module is used, this fault is partly mitigated.*
- Storage faults: if a part of the memory is defect (e.g. cannot be changed anymore), the system could freeze thus not pass DMI nor EB telegrams.
- Detected faults will not lead to CAT1/2 hazards due to combination with other faults because of the time slack between the concerning DMI and EB telegram (>2 s).

**Text, STMA-22143** - Undetected successive corruption of telegrams at the profibus (the detection shall be done in the ETCS on-board) can lead to taking into account false DMI information and corrupted EB commands. However the detection shall be done in the ETCS on-board and is therefore out of the scope of the STM ATB.

Faults in the STM ATB would concern faulty storage or calculation of the data before calculating the CRC.

## 9.2 Common cause faults concerning storage

**Text, STMA-22144** - A combination of faults leading to CAT3 hazards and faults leading to CAT5 hazards can lead to a CAT1 hazard. It is assumed that storage faults concerning EB commanding (CAT3) and concerning cab signals (CAT5) can have common causes or modes.

The concerning faults are described in:

 [STMA-21163 - Storage faults related to CAT3 hazards](#)

 [STMA-22139 - Storage related to CAT5 hazards](#)

Common cause/common mode faults can occur in case of multiple storage faults effecting different variables during at least 2 s. The tolerable failure rate concerning the total combination is  $1 \cdot 10^{-9}$ /hour (see **T** STMA-21070), 50 % can be assigned to storage faults.

**Requirement, STMA-22145** - The risk on undetected multiple storage faults concerning different variables during more than 2s shall be less than  $5 \cdot 10^{-10}$ /hour.

## 9.3 Common cause faults concerning calculations

**Text, STMA-22146** - A combination of faults leading to CAT3 hazards and faults leading to CAT5 hazards can lead to a CAT1 hazard. It is assumed that calculation faults concerning EB commanding (CAT3) and concerning cab signals (CAT5) can have common causes or modes.

The concerning faults are described in:

 [STMA-21948 - Calculation faults concerning CAT3](#)

 [STMA-21966 - Calculation faults concerning CAT5](#)

Common cause/common mode faults can occur in case of multiple calculation faults effecting different variables during at least 2 s. The tolerable failure rate concerning the total combination is  $1 \cdot 10^{-9}$ /hour (one CAT1 branch, see **T** STMA-21070), 50 % can be assigned to storage faults.

**Requirement, STMA-22147** - The risk on undetected multiple calculation faults concerning different variables during more than 2s shall be less than  $5 \cdot 10^{-10}$ /hour.