S.9.4.1 Part 4: Technical Safety Report Section 1 Introduction

for the development of an STM ATB

Colophon	
Document ID	S9.4.1
Version	1.0
Revision	495150
Author	AVO
Reviewed	495150 ,STMA-78378
Approved	495150 ,STMA-74609
Archive	SID-2157
Date:	2020/03/27 13:37

Authorization

Compiled by: AVO Signature/E-sign: 495150 ,STMA-78387	Date: 2020/06/19 11:27
Reviewed by: AGP Signature/E-sign: 495150 ,STMA-78378	Date: 2020/06/19 09:23
Approved by: AZB Signature/E-sign: 495150 ,STMA-74609	Date: 2020/03/27 15:55

CONTENT

1 Preface 4
2 Summary of the STM ATB system description 4
3 Design 5
4 Technical safety principles 7
4.1 Faults potentially leading to CAT1 hazards 7
4.2 Faults potentially leading to CAT3 hazards 9
4.3 Faults potentially leading to CAT2/4 hazards 9
4.4 Faults potentially leading to CAT5 hazards 10

1 Preface

Apportionment, STMA-25925 - This document contains section 1, "Introduction", of the technical safety report. This section provides an overview description of the design, including a summary of the technical safety principles that are relied on for safety and the extent to which the system, subsystem or equipment is claimed to be safe in accordance with tNEN-EN50129:2003/C1:2010 .
The technical safety report consists of the following Polarion documents:

- S.9.4.1 Part 4: Technical Safety Report Section 1 Introduction
- S9.4.2 Part 4: Technical Safety Report Section 2 Assurance of correct operation
- S9.4.3 Part 4: Technical Safety Report Section 3 Effects of faults
- S9.4.4 Part 4: Technical Safety Report Section 4 Operation with external influences

Together the documents provide the "evidence of functional and technical safety" as mentioned in point 5.4 of STMA-26378

Text, STMA-73461 - The technical safety principles used depend on the safety category the item effects. Safety categories are defined as:

Definition, STMA-10870 - CAT1: The speed is not guarded while it should and the supervised speed indicated to the driver also gives a too high speed for more than 3 s AND with a speed error > 7 km/h.

Definition, STMA-10871 - CAT2: The speed is not guarded while it should and the supervised speed indicated to the driver also gives a too high speed less than 3 s OR with a speed error < 7 km/h/

Definition, STMA-10872 - CAT3: The speed is not guarded while it should, while the correct speed indication is given to the driver for more than 3 s.
(also not braking when switching on while driving is included in this category: no guarding, but correct DMI).

Definition, STMA-10873 - CAT4: The speed is not guarded while it should, while the correct supervised speed is indicated to the driver for less than 3 s.
If the driver is not attending, this could lead too passing a "signal at danger" at low speed.
This is comparable to the consequence of an ATBVv failure. Therefore also ATBVv is included in this case although it is explicitly stated in the specifications that ATBVv is not a safety function.

Definition, STMA-10874 - CAT5: the supervised speed indication to the driver also gives a too high speed for more than 3s, but the correct speed is guarded.

2 Summary of the STM ATB system description

Text, STMA-72789 - The ATBEG+Vv function is described in detail in D1.1 ATB system description.

Text, STMA-25806 - ATBEG is a function which was introduced at the Dutch Railway network in the late 1960's to enhance safety after an accident in 1962. The way-side part of the system is an addition to the "75Hz track circuits" used for train detection. Those "75Hz track circuits" (with a length between 50 and 1200m) cover almost the complete network. To communicate the maximum speed at the next signal, the 75Hz current of the track circuits is "amplitude modulated". The modulation frequency codes the maximum speed (at the next signal). On-board of the trains equipment is installed capable of detecting the 75Hz currents in the rails and decoding the "track signal". The on-board shall calculate the maximum speed at the next line side signal(*) base

d on the “track signal”.
If the train exceeds the maximum speed retrieved from the ATBEG code while the driver is not braking (during a situation depending time) then the ATB on-board shall apply the brakes.
The relation between the maximum speed and the ATBEG code is fixed. However alternative values are mentioned in the RIS (regeling indienststelling spoorvoertuigen), and speed levels can be changed dynamically using ATBNG technology (ATBM+ mode). The same is possible using ETCS technology.

(*) More detailed: the track signal gives the minimum of the maximum speeds at the previous and the next line side signal. Therefore the current maximum speed and the maximum speed at the next line side signal are monitored.)

Text, STMA-25807 - ATBVv was introduced to reduce the risk concerning passing signals at danger. As ATBEG function doesn't know the distance to the next signal, trains will always be allowed by the ATBEG function to proceed at a certain speed (40km/h), independent of the ATBEG code in the track. This has led to a number of incidents were a train passed a signal at danger at low speed (<40km/h).
To protect trains against this danger a functionality (ATBVv) was developed (and meanwhile installed at the majority of the signals) to communicate the distance to a signal at danger (at 3m, 30m or 120m), using an active (not fail-safe) EM signal near the rails.
Trains are equipped with the functionality to detect and evaluate the information at a voluntary basis. However all available ATB on-board systems are equipped with the function. As the way-side equipment is not fail safe and the system only provides background protection without information to the driver (thus no misleading of the driver possible), also the on-board functionality only has to comply with an availability requirement (i.e. no safety requirements). The availability of the train borne equipment shall at least be comparable to the availability of the track side equipment, and is specified in [D1.4.2.2].

Text, STMA-72790 - Summarizing:

Text, STMA-25932 - The ATBEG function consists of:

- Cab signaling: inform the driver about the maximum speed which may be driven at the next signal, and give an acoustical signal (warning) in case of “over speed”.
- Monitor the train speed: command the “emergency brake” (EB) via the ETCS on-board in case of over speed (too long) while the driver is not braking.

Text, STMA-25933 - The ATBVv function consists of:

- Monitor the distance to a signal at danger: command the “emergency brake” (EB) via the ETCS on-board in case of exceeding a braking curve.

3 Design

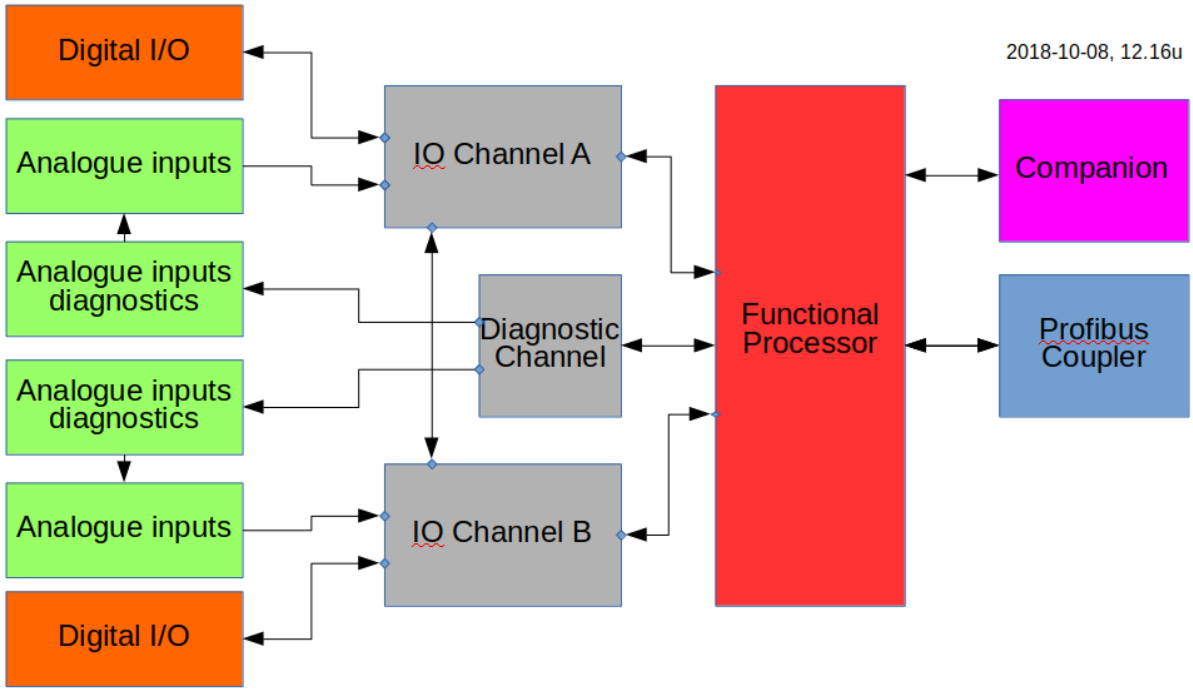
Text, STMA-25924 - The STM ATB architecture is described and underpinned in D5.0 SAS for STM ATB.
The STM ATB is divided in the following blocks (see STMA-12360):

- Power supply; a redundant power supply is foreseen. The outputs of both power supplies are combined in a way the correct operation of each of them can be monitored.
- Digital input circuits; two times three physically separated digital inputs which can be used in

independent pairs (for redundancy).

- Digital output circuits; two times three physically separated digital outputs which can be used in independent pairs (for redundancy).
- Analogue input circuits; two times four physically separated analogue inputs which can be used in independent pairs (for redundancy).
- An FPGA hosting two IO Channels, each controlling three digital inputs, three digital outputs and four analogue inputs, and hosting one “diagnostic channel”.
  The Diagnostic Channel is used to generate test signals added to the analogue (coil + configuration) input signals, and to provide software sequence checking for the Functional Processor.
  Independence between the different channels in the FPGA is reached using the Xilinx “isolation design flow” (certified reference design available), by shifting similar functions in the different channels in time and by diversity in functions whose simultaneous failure could lead to a CAT1 hazard.
- A Functional Processor at which the STM ATB behavior is implemented. The integrity of the processor is monitored by a wide range of on-chip diagnostics, of which the “lock step mechanism” and ECC checking combined with physical separation of memory are the most important functions used at each step (clock cycle).
  Further diagnostic functions are added to test the hardware integrity independent from the execution of the STM ATB function. The latter is done at a time bases shorter than the critical detection time for the STM ATB function.
- A Profibus Coupler to facilitate the communication with the ETCS on-board via Profibus. The Profibus Coupler consists of a “commercial of the shelf” component (netX51) which implements the Profibus “field data layer”, and a dedicated “host processor” to perform the interfacing to the netX51. The Functional Processor is not coupled directly to the netX51, because the short response time which might be necessary when reading data received from the Profibus, could hamper the safety functions. The netX51 also requires the usage of driver software at the host. This software is not certified against SIL3/4 requirements and may therefore not be mixed with the SIL3/4 software at the Functional Processor.
  The “Profibus Coupler” is protected by the safety mechanisms prescribed in ERA subsets D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0) and D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0).

Definition, STMA-12360 - figure: HW architecture including "Diagnostic Channel" and "Companion" chip.
note: separation of the blocks doesn't define the way the blocks are separated, this can vary from complete isolation (no energy exchange), galvanic isolation to implementation in isolated areas of the same chip.



4 Technical safety principles

4.1 Faults potentially leading to CAT1 hazards

Text, STMA-25930 - The most critical safety relevant hazards concern both ATBEG functions, i.e. the maximum speed displayed to the driver is too high and the maximum speed monitored is too high. Those hazards can occur in case the maximum speed, which is common to both functions, is determined too high. I.e. the single functional failures as listed in STMA-9024, those can be caused by the following technical faults:

1. The track signal is determined wrong OR
2. Configuration information received from the ETCS on-board is corrupted OR
3. Repetitive faults are made during the analysis of the coil signals affecting both, the DMI and the EB command.

Faults in communication of the outputs concern DMI information or EB commands, not both. Therefore the risk concerning those is lower.
note: The analogue configuration input information is not used for speed indications to the driver, therefore corruption of this configuration data will not lead to a CAT1 failure.

Text, STMA-25931 - *The track signal is determined wrong*
The track signal is provided to the train via the current in the left and via the current in the right rail. Due to disturbance currents a code can only be trusted, and thus may be accepted, if:

- The ATB code is found in both signals AND

- The phase of the current is left rail is opposite to the phase of the current in the right rail.

Therefore no corruption of a single signal (left or right) can lead to accepting a code which is not present in the track signal.
The safety of reading the track signals is based on independence of the analysis of the left and right signal up to the point where the information is combined (the ATBEG decoding module). In addition the input circuits and analysis is monitored by:

- Test signals added to the coil signal:
  - 2133.3 Hz (16/7.5 kHz) for fast detection of faults in the input circuits.
    (as the track signal will not contain long time high components at this frequency).
  - 145 Hz, intended for detection of faults in the input circuits only affecting the frequency range around 75 Hz (slow detection, app. 1s, due to possible disturbance by the track signal).
    However as the FMEA (D6.9.2 FMEA Hardware) didn't show faults which lead to a failure in the 75 Hz-145 Hz frequency range but not at 2133.3 Hz, the test at 145 Hz is obsolete. As disturbances due to traction harmonics can be expected at 145 Hz, the result of the 145 Hz test is only used to communicate to the JRU.
  - DC for detection of absence of the pick-up coils (very slow detection, app. 60 s, due to possible disturbance by the track signal).
- Partial duplication of the input processing (e.g. 75 Hz filtering in the IO Channels and the Functional Processor).

The safety of the analysis done in the functional processor is based on the (certified) diagnostics during execution (every clock cycle) and additional diagnostics implemented in the spare time during the 10 ms calculation cycle.

Text, STMA-25928 - *Configuration information received from the ETCS on-board is corrupted*
The braking performance and maximum speed of the train is communicated from the ETCS on-board to the STM ATB. It’s the responsibility of the ETCS on-board to sent the correct information, this is stated in the concerning ERA subsets.
Concerning the communication, the ERA specifications prescribe safety mechanisms to detect communication faults which are out of the control for the STM ATB or ETCS on-board. Those safety mechanisms are implemented at the Functional Processor, resulting in a sufficiently low risk on undetected communication failures.
The safety of the checks done in the Functional Processor is based on the (certified) diagnostics during execution (every clock cycle) and additional diagnostics implemented in the spare time during the 10 ms calculation cycle.

Text, STMA-25927 - *Repetitive faults are made during the analysis of the the coil signals*
The maximum speed to be displayed to the driver and brake commands to be sent are determined by the Functional Processor based on the analyzed input information.
The safety of this analysis is based on the (certified) diagnostics during execution (e.g. lock-step and ECC) and additional diagnostics implemented in the spare time during the 10 ms calculation cycle.

4.2 Faults potentially leading to CAT3 hazards

Text, STMA-72911 - Apart from faults in the Functional Processor (those can also lead to CAT1 hazards), the following functional faults can lead to CAT3 hazards. Those failures listed in STMA-9026 except those due to the Functional Processor. In addition the analogue configuration signal is relevant. According to D3.3 Tolerable Functional Fault Rates such a failure could lead to a CAT1 hazard, however as the information is not shown to the driver (mitigation by adapting the functionality) the maximum consequence is a CAT3 hazard:

1. Brake handle applied information is corrupted.
2. Analogue configuration input information is corrupted.

Text, STMA-72914 - *Brake handle applied information is corrupted*
Brake handle applied information is gathered via redundant (antivalent) digital input signals, and/or redundant analogue input signals. A sufficient level of safety is guaranteed by the implemented redundancy.

Text, STMA-25929 - *Analogue configuration input information is corrupted*
In addition to the braking performance information as communicated by the ETCS on-board, an analogue input signal is foreseen to determine the braking performance in case it is not provided by the ETCS on-board.
The safety of the analogue configuration information is guaranteed by using independent redundant input circuits up to the point where the information is checked and combined in the Functional Processor.
The safety of the analysis done in the functional processor is based on the (certified) diagnostics during execution (every clock cycle) and additional diagnostics implemented in the spare time during the 10 ms calculation cycle.
In addition, a significant fault in the configuration signal will also effect the level of the test signals which are added to the configuration signal.

4.3 Faults potentially leading to CAT2/4 hazards

Text, STMA-72921 - In addition to faults potentially leading to CAT1/3 hazards, CAT2/4 hazards can be caused due to communication delays. Because of the prescribed safety layers used for the communication between STM ATB and ETCS on-board, a telegram loss at the bus inevitably leads to a delay in presenting at the DMI and/or commanding the brakes. The Safety Layers are configured in a way the delay is guaranteed below 3 s.
To meet the safety requirements concerning CAT2/CAT4 hazards, the bit error rate shall be sufficiently low. However as the medium and environment are also prescribed, those faults are out of scope for the STM ATB.

4.4 Faults potentially leading to CAT5 hazards

Text, STMA-73463 - *The DMI messages are faulty*

In addition to faults potentially causing CAT1 hazards, faults concerning composing the DMI messages can also cause CAT5 hazards. Composing the DMI messages is fully handled in the Functional Processor.