S.9.4.3 Part 4: Technical Safety Report Section 3 Effects of faults

Effects of faults

Colophon	
Document ID	S9.4.3
Version	2.0
Revision	779344
Author	AVO
Reviewed	779344 ,STMA-82354
Approved	779344 ,STMA-82403
Archive	SID-2159
Date:	2022/11/15 11:44

CONTENT

1 Preface

Apportionment, STMA-27999 - In this section it is demonstrated that the STM ATB meets it's specified safety requirements, taking into account random hardware faults. In addition the measures taken to limit the risk due to systematic faults are described.

Linked Work Items	has parent: STMA-27471 - Preface , apportions: STMA-27466 - This section shall demonstrate that the system/sub-system/equipment continues to... , apportions: STMA-27998 - In addition, a systematic fault could still exist, despite the quality and safet...

1.1 EN50129 requirements

Text, STMA-28001 - The relevant topics are described in NEN-EN50129:2003/C1:2010, chapter 5.4. The conclusion on the compliance is included in document V5.91 Gate Review Report - Phase 5, STMA-42144 - It is recommended that the system architecture description should contain a gene... line 6 is in the table which a.o. refers to CLC/TR-50506-2.

Text, STMA-72061 - Section 3 Effects of faults

External Requirement, STMA-27466 - This section shall demonstrate that the system/sub-system/equipment continues to meet its specified safety requirements, including the quantified safety target, in the event of random hardware faults.

External Requirement, STMA-27998 - In addition, a systematic fault could still exist, despite the quality and safety management processes defined in 5.2 and 5.3 of this standard. This section shall demonstrate which technical measures have been taken to reduce the consequent risk to an acceptable level.

External Requirement, STMA-27467 - This section shall also include demonstration that faults in any system/sub-system /equipment having a Safety Integrity Level lower than that of the overall system, including Level 0, cannot reduce the safety of the overall system.

External Requirement, STMA-27468 - The following headings shall be used in this section, for which more detailed requirements are contained in B.3. Guidance is also given in Table E.5 and Table E.6.
3.1 Effects of single faults (see B.3.1);
3.2 Independence of items (see B.3.2);
3.3 Detection of single faults (see B.3.3);
3.4 Action following detection (including retention of safe state) (see B.3.4);
3.5 Effects of multiple faults (see B.3.5);
3.6 Defence against systematic faults (see B.3.6)

1.2 Generic approach

Text, STMA-72070 - The approach is to use an FTA (D3.3 Tolerable Functional Fault Rates) at the start of the project to determine safety requirements (D4.2 Safety requirements) and an architecture (D5.0 SAS for STM ATB) suitable to comply with those requirements.
After completing the design, the compliance of the quantitative safety requirements is shown using an FMEA (D6.9.1 FMEA Software, D6.9.2 FMEA Hardware, D6.9.3 FMEDA Hercules and Companion Chip and D6.9.5 Apportionment safety requirements) and compliance with the qualitative safety requirements (architecture) is show with a common cause failure analysis (D6.9.4 Common Cause Failure Analysis).

Text, STMA-29120 - Main steps:

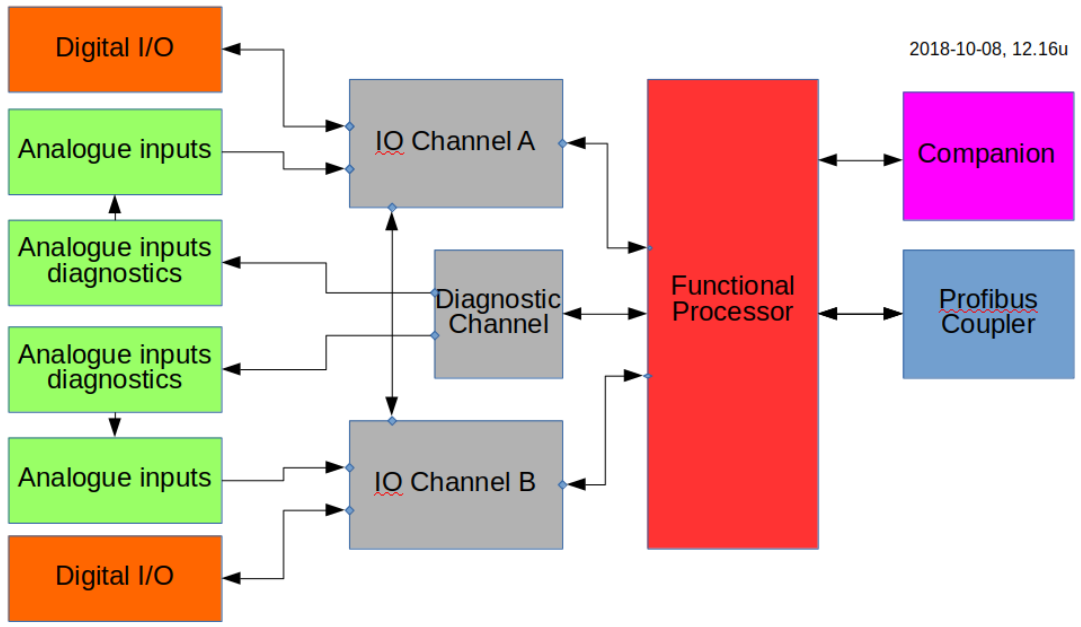
- FTA to assign safety requirements to the different modules (not a part of the proof, but a process step to assign

requirements to the different parts of the system).
This step results in an architecture and quantitative safety requirements.

- FMEA to prove that the resulting design meets the safety targets.
  The quantified methods to calculate the "undetected unsafe failure rate" for functions implemented at the Functional Processor, as provided by TI, will be used in the calculations.
  Usage of the calculation methods provided by TI proves the compliance of the design with IEC61508-1/2 requirements.
  Therefore the requirements resulting from EN5012x are compared to IEC61508-1/2

Below (figure STMA-12360) a block schematic view of the architecture defined in D5.0 SAS for STM ATB is shown:

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.



1.3 Technical concept

Text, STMA-72296 - SIL3 requirements apply to those subsystems whose failure could lead to a CAT1 failure. Monitoring functions capable of detecting any single or double similar fault outside the Functional Processor which could lead to a CAT1 hazard, are implemented at the Functional Processor. Therefore SIL3 requirements only apply to the Functional Processor, and diverse redundant monitoring functions.
An FMEA is used to prove that no single or double similar fault outside the Functional Processor can lead to a CAT1 failure, and that all faults which could lead to a CAT1 failure in combination with a different second fault will also be detected by the Functional Processor.

2 Effects of single faults

2.1 FTA

Text, STMA-27581 - An FTA is performed to determine tolerable hazard rates for "functional faults", in order to be able to assign safety requirements to the system parts relevant for those functions. Wherever one "functional fault" can lead to a safety relevant hazard (level is determined by the category: CAT1,..,CAT5 for safety relevant hazards), or if a combination of two, not fully independent, "functional faults" can lead to a safety critical hazard, measures shall be taken to assure that a single hardware failure will not lead to such functional faults.
The FTA is used to assign tolerable fault rates to "functional faults" in order to derive the safety requirements per technical function (storing, calculating, communicating, etc.) as input for the design process.

2.2 FMEA

Apportionment, STMA-27574 - Different techniques are used for different functions to assure that single random hardware component failures do not lead to a safety hazard. An FMEA (D6.9.2 FMEA Hardware and D6.9.3 FMEDA Hercules and Companion Chip) is performed to prove the effectiveness.
In the FMEA references are made to measures to guarantee safety. Common causes are analyzed in the common cause analysis (D6.9.4 Common Cause Failure Analysis).

Linked Work Items	has parent: STMA-25935 - System architecture description , apportions: STMA-27422 - - Whichever technique or combination of techniques is used, assurance that no si... , apportions: STMA-27447 - Additionally it shall be demonstrated that the safety-relevant application rules... , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

3 Independence of items

Text, STMA-27638 - Sufficient independence is shown between elements which together form "composite fail-safety" and between elements which together form "reactive fail-safety" (NEN-EN50129:2003/C1:2010) in D6.9.4 Common Cause Failure Analysis.
Freedom of common causes is investigated for the combination of faults which together lead to an unsafe state (CAT1 failure).
Double similar faults outside the Functional Processor which could lead to a CAT1 failure, are equally detected as single faults by diagnostics in the Functional Processor. Only diverse multiple faults occuring at the same time might not be detected. Therefore diversity is used to achieve independence of faults which together could lead to a CAT1 failure.

Apportionment, STMA-27515 - A general requirement concerning independence is defined in EN50129:2003, B3.2 (STMA-27514). This requirement is further detailed in STMA-27404, STMA-27405 and STMA-27410. In this paragraph the three detailed requirements are apportioned, therefore also covering the generic requirement.

Linked Work Items	has parent: STMA-25945 - Independence of items , apportions: STMA-27514 - Appropriate rules or guidelines shall be fulfilled to ensure this independence.....

Text, STMA-27518 - Common cause failures in different modules/components can arise from:

- modules influencing each other, e.g. due to unintended exchange of information (energy).
- influences from a common source, e.g. a common power supply or EM interference.

Text, STMA-42116 - Common causes can be:

- External influences: radiated EMI (C1, see STMA-27412),
  Disturbances via power supply (C2), Disturbances via other IO (C3).
  Mechanical influences (C1)
  Maintenance and installation (C1)
- Internal faults: defects influencing parts of the system "further" in the chain (C1, C2 and C3) or multiple channels influencing each-other (A).
- Functional faults will not influence safety in the STM ATB as,
  All input information is defined (D); system behavior is completely defined and parallel system parts don't have intentional connections fit for information exchange (other than through defects), (B).

Text, STMA-27519 - One way to limit the ability to exchange energy between modules/components is to insulate the systems from each-other for common mode voltages. The latter would prevent a first short circuit between the circuits to allow a current (thus information flow) between the modules/components, and enables the detection of the first short. This makes galvanic insulation especially useful between digital control system with long wires.
As electronic components used to realize galvanic insulation also behave as a (small) capacitor, galvanic insulation is not effective for high frequency signals, and thus not for guaranteeing independence between circuits in the STM ATB.

In the STM ATB galvanic insulation is used to avoid high DC (and low frequency) currents floating through the electronics. The casing of the system is connected to the shields of the cabling and internally bariers (galvanic insulation) are implemented.
Isolation between the input circuits is provided to allow the use of inputs at different voltage levels (i.e. battery related and ETCS supply voltage related) for anti-valent or redundant signals.
For the Profibus interface galvanic insulation is mandatory, to avoid DC (and low frequency) currents floating through the Profibus network.
The galvanic insulation is thus used for availability, safety is not reliant on it. Therefore insulation is not reinforced.

Apportionment, STMA-27520 - Galvanic insulation is used to prevent traction return currents and other high currents in the environment of the equipment, to float (partly) through the STM and cause EMI. However safety doesn't rely on the galvanic insulation as further measures are taken to mitigate the effect of double short circuits.

Measures to make the safety measures immune for short circuits:

- The test signals injected at the coil signals and configuration signal have different levels. A short circuit between the left and right coil signals will lead to a change in the test signals, thus a safe reaction. This difference is checked in the Functional Processor. If the difference is not correct (test-level: difference > 1A, see STMA-11882 - The output value of 2133.3 Hz filtering over an ATBEG window ( ) shall be used t...), measures will be taken.
  (relevant for the coil signals, i.e. for potential CAT1 failures)
- The digital input signals are read redundantly and antivalent. A short circuit will lead to equal signals, thus rejecting the information and enforcing a safe state.
  (relevant for the brake applied signals, i.e. for potential CAT3 failures)
- Between redundant analogue signals and between redundant digital signals, defined voltages (connected to the power supply) are routed. Creepage at the PCB will therefore lead to a short circuit to the power supply before it can hamper the information contained in the analogue and/or digital signals.
  (relevant for the brake applied signals, i.e. for potential CAT3 failures)
- Coil signals are out of phase, a short circuit between the two will lead to noCode, i.e. safe state.

Linked Work Items	has parent: STMA-25945 - Independence of items , apportions: STMA-27517 - Where safety is reliant on the clearance and creepage distances, the minimum cle...

Apportionment, STMA-27645 - For the Functional Processor a component with a safety approval for their generic product safety case, is used in the STM ATB; the RM48x. Proof that the "tolerable hazard rates" concerning the specific application are fulfilled, using this "generic product" is provided in D6.9.3 FMEDA Hercules and Companion Chip .

Linked Work Items	has parent: STMA-25945 - Independence of items , apportions: STMA-27643 - Hazards related to a system are identified and assessed with regard to their pot...

Apportionment, STMA-72703 - A common cause analysis has been performed, the results are listed in D6.9.4 Common Cause Failure Analysis.

Linked Work Items	has parent: STMA-25945 - Independence of items , apportions: STMA-27447 - Additionally it shall be demonstrated that the safety-relevant application rules...

3.1 Independence in the input circuits and IO Channels

Text, STMA-27648 - As shown in the D6.9.4 Common Cause Failure Analysis no two similar faults in the input circuits and IO Channels will lead to a CAT1 failure. This is achieved as all similar double faults concerning the coil signals are detected by diagnostic functions implemented in the Functional Processor, like single faults are detected. The circuits are independent as only multiple faults due to a different mechanism can hamper safety.
Below the measures to avoid simultaneous failures due to common mode influences are described, which make the system respond safely to multiple faults due to the same mechanism.

3.1.1 Input signals to determine if the brakes are operated

Text, STMA-39012 - As stated in the preface of this chapter:

Apportionment, STMA-27442 - Independence of the input circuits concerning the brake handle applied signals:
The consequence of a fault in brake handle detection is classified as CAT3 hazard. Therefore components only contributing to detection of brake operation (i.e. digital input circuits and analogue input circuits concerning the brake pipe pressure) shall comply with SIL1 requirements (STMA-27627). This concerns a.o. the DIO-Board.

The input circuits for brake handle applied signals are implemented as separated circuits with defined voltages in between:

- The analogue input circuits concerning the coil signals, the brake pipe pressure signal and configuration signal in one input channel share a power supply provided from the processor board. Faults in the power supply effecting the signal levels will be detected by diagnostic functions monitoring the coil signals and the test signal level at the configuration signal.
- Apart from the power supply the circuits for the redundant signals are completely separated and don't share components

The independence between digital input signals (including the digital brake handle applied signals) is further enhanced by using "anti-valent" inputs (the inputs concerning the same information are inversed: one high and one low is a valid signal). This way short circuits between the two signals will not lead to a common cause failure.

Linked Work Items	has parent: STMA-27895 - Input signals to determine if the brakes are operated , apportions: STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. N... , apportions: STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be a... , apportions: STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B... ,

	apportions: STMA-27445 - It has to be ensured that sufficient * physical, * functional, * process indepen...

3.1.2 Coil signals

Apportionment, STMA-27400 - Independence of the input circuits concerning the coil signals.
The input circuits for the left and right coil signal are implemented as separated circuits at one PCB:

- The circuits share a power supply (see STMA-27442) provided from the processor board.
- The same test signal source is used for both circuits (see D5.1.3.1) via two separate galvanic isolations.
  The test signal is also injected at the (constant) configuration signal. Therefore faults in the test signal generation will be detected.
- The test signals have different levels in each input circuit, this way short circuits leading to exchange of information will be detected.
- Deviations in the transfer of the coil signals (single and/or double faults) will be detected from faults in the test signals before becoming hazardous (lower tolerances than accepted in the decoder).
- Apart from the power supply and test signal generation the circuits don't share components.
  The power supply is also shared with the input circuits for the configuration signals. Therefore disturbances due to the power supply will also be detected at the (test signal levels at the) configuration signals.

Monitoring of faults in one input circuit and monitoring of faults in both input circuits is implemented in the Functional Processor (STMA-27399). In case of detected faults, the effect will be mitigated before a dangerous state is reached (0.8 s).

Linked Work Items	has parent: STMA-27894 - Coil signals , apportions: STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. N... , apportions: STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be a... , apportions: STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B... , apportions: STMA-27445 - It has to be ensured that sufficient * physical, * functional, * process indepen...

Apportionment, STMA-27403 - Independence of the IO Channels concerning the coil signals.
The IO Channels are both implemented in the same FPGA. Measures to avoid common mode and common cause faults:

- To separate the channels the "Isolation Design Flow Methodology" from Xilinx is used.
- All parts share the same power supply (derived from the train borne power supply). Power supplies are monitored to avoid/mitigate common cause failures due to "physical external influences" using independent monitoring outside the FPGA (external circuits plus the Functional Processor).

The safety critical signals are monitored in a way that similar (the same mechanism) faults will be detected by the diagnostics implemented in the Functional Processor:

- A (single or double) fault during sampling of analogue data will be detected via the test signals.
- The coil signals are summed. The summed signals are down sampled in the other IO Channel and passed to the Functional Processor. In the Functional Processor the signals are filtered at 75 Hz and the result is compared with the sum of the corresponding 75 Hz values of the corresponding coil signals, as calculated in the IO Channels.
  A fault concerning the summed signal in the FPGA is not similar to possible faults concerning the 75 Hz signal. I.e. only a diverse multiple fault can hamper safety.
- The processing of the input data (up to and including the CRC calculation for the output communication) is de-synchronized (i.e. one IO Channel is 5 ms delayed to avoid doing the same type of calculation at the same time in both channels). The time shift is such that it is guaranteed that diverse functions whose simultaneous failure could

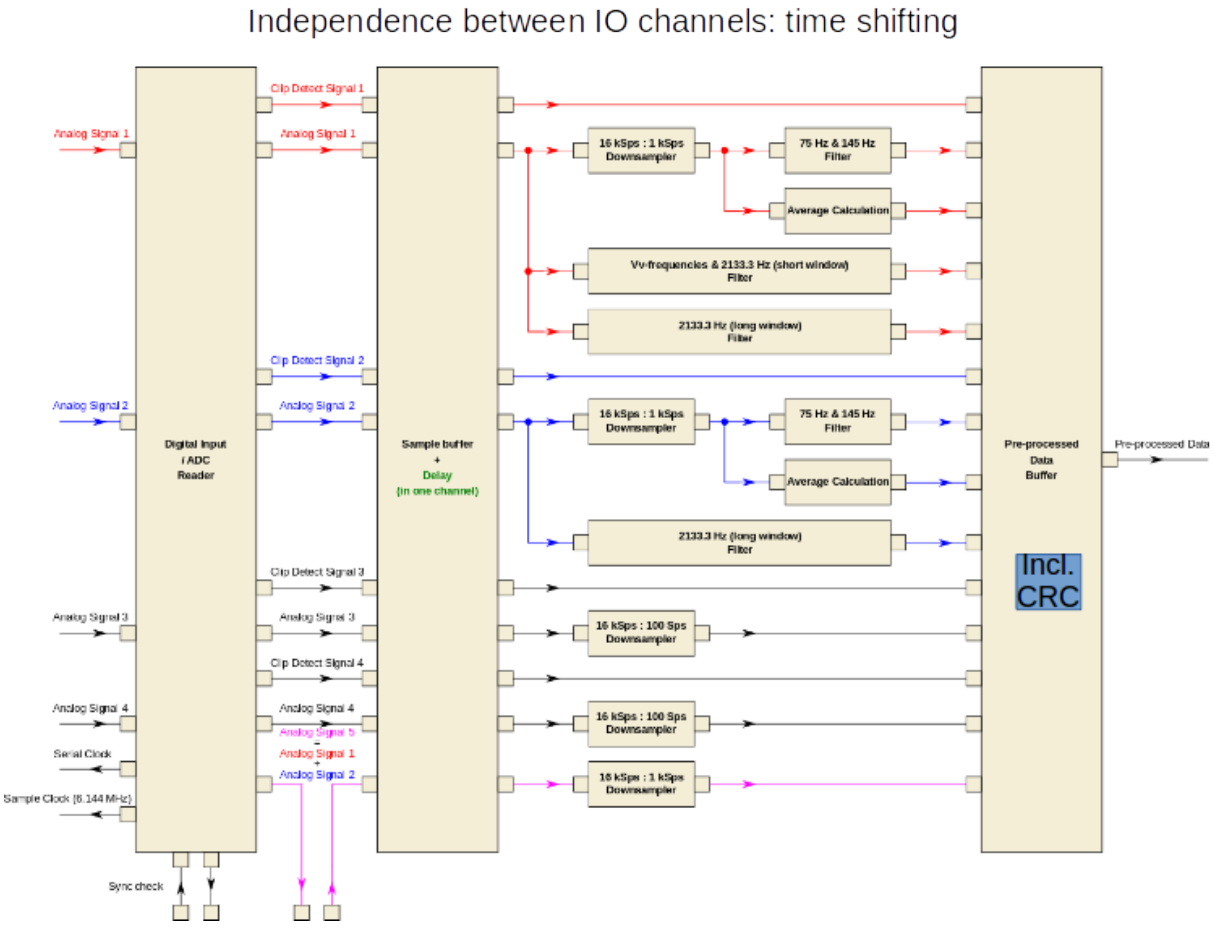
lead to a hazardous situation are not performed at the same moment (see STMA-29043).

- Before storing the data a CRC is calculated and added. Therefore simultaneous faults in the communication process will be detected.

Monitoring of faults in one IO Channel and monitoring of faults in both IO Channels is implemented in the Functional Processor
(STMA-27399). In case of detected faults, the effect will be mitigated before a dangerous state is reached (0.8 s). Therefore also similar double faults will not lead to a hazardous situation.

Linked Work Items	has parent: STMA-27894 - Coil signals , apportions: STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. N... , apportions: STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be a... , apportions: STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B... , apportions: STMA-27445 - It has to be ensured that sufficient * physical, * functional, * process indepen...

Definition, STMA-29043 - Figure: Time shifting between IO Channels
In one of the channels a buffer is introduced to delay the further processing (1 ms) up to the point the data is ready for communication (and thus protected with CRC).



3.2 Independence in the Functional Processor

Text, STMA-29121 - The examples given for avoidance of common cause failures given in annex D of the EN50129:2003 are not targeted at "System on Chip"s. Therefore the starting point to show sufficient technical and functional independence are the definitions: (NEN-EN50129:2003/C1:2010: STMA-42164 and STMA-42165).

Definition, STMA-42164 - freedom from involvement in the same intellectual, commercial and/or management entity

Definition, STMA-42165 - freedom from any mechanism which can affect the correct operation of more than one system/sub system/equipment as a result of random failures

Text, STMA-42170 - Requirements concerning the CCF analysis to show independence
A.4.2.2 Common Cause Failure (CCF) analysis (STMA-27445):

External Requirement, STMA-27445 - It has to be ensured that sufficient

- physical,
- functional,
- process

independence exists between sub-systems or system functions (see B.3.2 and B.3.6). If independence cannot be demonstrated completely then the common cause failures have to be modelled at an appropriate level of detail.

Text, STMA-42171 - The RM48x is certified against IEC 61508-2 and thus complies with the following requirement stated in IEC61508-2:
7.4.3.4 Sufficient independence, in the design between elements and in the application of elements, shall be justified by common cause failure analysis to show that the likelihood of interference between elements and between the elements and the environment is sufficiently low in comparison with the safety integrity level of the safety function under consideration.
i.e. a common cause failure analysis, showing that the likelihood of interference is sufficiently low, has been done.

Text, STMA-42175 - Paragraph 7.4.3.4 in the IEC61508-2 implies that a common cause analysis concerning the RM48x has been done at an appropriate level of detail.

Apportionment, STMA-42167 - The measures to avoid common causes between redundant parts and between other parts whose simultaneous failure could lead to a hazard, are described below.

Linked Work Items	has parent: STMA-25953 - Independence in the Functional Processor

3.2.1 Calculations

Apportionment, STMA-27419 -
Measures to avoid internal and external influences hampering independence between the two CPUs (which operate in lock step in the Functional Processor) are at least:

- Calculations are shifted in time, i.e. one CPU executes calculations two clock cycles before the other to avoid external disturbances to influence both processors in the same manner.
  (Even if a disturbance occurs with a frequency equal to the clock frequency, there will be a start and ending moment where only one of the processor results is affected).
  Therefore a fault due to external physical influence or via connections between the two CPUs cannot cause the same fault in both CPUs (as the progress of the execution of the program thus the internal state is different).
- The orientation of the CPUs is 90 degrees different (and flipped) to limit the susceptibility to EM-disturbances.

- A minimum distance of 100 um is kept between the CPUs (safety manual Functional Processor, section 6.6.1, p30).
- Voltage monitoring ring is implemented around the CPU, mitigating influences due to external voltages, and other physical interaction via unintended connections.
- The CPUs do not respond on each others state or result.
- As a response on differences in the results from the two CPUs the system will be reset.
- The diagnostic component ("CPU Compare Module" (CCM)) is checked at start-up and during operation
- The CPU are tested at start-up. This test is controlled from the "CPU Self-test Controller Module" (STC).
- Diversity: A hazardous situation due to faults in a CPU and in the CCM can arise only in case of specific faults in two (very) different circuits.

The effectiveness of the measures is shown with the FMEDA tooling provided by TI.
Quantitative analysis is done to prove the resulting "undetected unsafe failure rate" for the STM ATB application (D6.9.3 FMEDA Hercules and Companion Chip). The tooling provided by TI is certified against IEC61508-1/2, i.e. it is fulfilling the requirements of that standard.

Linked Work Items	has parent: STMA-25954 - Calculations , apportions: STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. N... , apportions: STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be a... , apportions: STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B...

3.2.2 Data storage

Text, STMA-29128 - The memory of the Functional Processor is protected with the following mechanisms:

- An 8 bit ECC code over a 64 bit value which is generated by a HW circuit inside the processors (i.e. in the redundant part) in case of writing data.
- When reading the data a HW ECC check is performed.

Apportionment, STMA-27420 - Measures to avoid internal and external influences hampering safety and the independence between the checking mechanism and the data storage:

- The result (72 bit) is divided into two parts which are stored in physically separated memory blocks (32 data bits + 4 ECC bits are stored in one part of the memory, and the other 32 bits + 4 ECC bits are stored in an independent part of the memory).
  This way faults in addressing will be detected, as the ECC will detect a fault if two 36 bit blocks from different addresses are combined.
- Bits in words are ordered in a way corruption of adjacent bits effects different words, therefore a transient fault concerning multiple adjacent bits will effect several words, which reduces the risk that the ECC will not detect memory faults.
- The ECC circuitry is checked by the application software at start-up and during operation (within the system safety time) using fault injection (known faulty information), using TI diagnostic software.
- The integrity of the memory is checked at start-up and during operation (within the system safety time).
- Quantitative analysis is done to prove the resulting "undetected unsafe failure rate" for the STM ATB application. The tooling provided by the supplier of the Functional Processor is certified to fulfill IEC61508-1/2 requirements.

Linked Work Items	has parent: STMA-25952 - Data storage , apportions: STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. N... , apportions: STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be a... , apportions: STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B... ,

	apportions: STMA-27445 - It has to be ensured that sufficient * physical, * functional, * process indepen...

Text, STMA-29129 - A high level explanation of the concept used for the Hercules series (including Functional Processor) is given in:
Hercules TM Microcontrollers: Real-time MCUs for safety-critical products
September 2011
authors: Karl Greb, Functional Safety Technologist at TI and Dev Pradhan, Hercules Product Line Manager at TI

Apportionment, STMA-27421 - The measures described above are checked against requirements in the IEC61508-2. In the scope of the certification of the Functional Processor against this standard by the manufacturer, detailed explanation of the measures has been made available. This level of detail is however not available to users of the device. Therefore requirements in the IEC61508 are compared to requirements in the EN5012x (S9.4.3.1 Annex EN5012x vs IEC61508).

Linked Work Items	has parent: STMA-25952 - Data storage

3.3 Communication

3.3.1 Communication ETCS <-> STM ATB via Profibus

Text, STMA-27959 - The communication concept for the communication with ETCS is based on "Reactive fail-safety" as described in the ERA specifications D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0), D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0) (safety layers) and D4.7.4 Specific Transmission Module (SS035 v3.2.0).
As stated in STMA-21903 this is sufficient to prove compliance with *STMATB/0_ Development/EN50159_2010*.
The Field Data Layer (FDL) as prescribed in the ERA documents is implemented using a COTS component (netX51 from Hilscher) which is used in various ETCS applications in combination with a host processor ("Profibus Processor" necessary to avoid the need for using interrupts in the Functional Processor). The communication channel including the "Profibus Processor" (TIVA) and netX51 is considered as a "black channel". The software used at those components doesn't have technical interfaces to the software at the "Functional Processor" (RM48x). Therefore the software used at those processors doesn't have to comply with all procedures needed for the SIL3 software at the "Functional Processor" (e.g.: the COTS components to control the netX51 from the Profibus Processor are not MISRA compliant). This allows the use of "not certified software" provided by Hilscher (netX51) supplier for communication with the netX51.

Apportionment, STMA-27960 -
Independence between the software at the Profibus Processor and Fieldbus Network Controller from the software at the Functional Processor is achieved while the only way to exchange information is via a SPI connection protected with a standardized CRC. The profibus telegrams included in the exchanged information are also (individually) protected with the CRC coding and with sequence numbers and time stamping as prescribed in the ERA specifications D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0) and D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0).

Linked Work Items	has parent: STMA-27947 - Communication ETCS <-> STM ATB via Profibus , apportions: STMA-27467 - This section shall also include demonstration that faults in any system/sub-syst...

Apportionment, STMA-27961 -
Telegrams received from the Profibus are delivered to the functional processor including safety coding (CRC and time stamp) in accordance to the ERA standards. All safety checks are done in the redundant CPUs of the Functional Processor (architecture based on reactive fail-safety). The selected minimum safety level (the actual is determined by the ETCS on-board) for the connections to ETCS functions is chosen to comply with the safety requirements (D5.0 SAS for STM ATB).

Linked Work Items	has parent: STMA-27947 - Communication ETCS <-> STM ATB via Profibus

Apportionment, STMA-27762 -
A detection mechanism, used to detect communication errors, is implemented in the functional processor.
Measures to further avoid internal and external influences between the communication (via Profibus, netX51 and "Profibus Processor") and the diagnostics are:

- A Profibus Processor is selected to communicate to the netX51.
  This way the netX51 can be polled at a sufficient high frequency. Therefore no interrupt based communication is required. Not in the "Profibus Processor", nor in the "Functional Processor".
- The "Profibus Processor" communicates with the "Functional Processor" via CRC protected connection (on top of the CRC protection according to subset-057)
- The information passed through the "Profibus Processor" is CRC and time stamp protected (according to ERA subsets 056/057). Therefore a sufficient safety level (depending on the selected safety level for the communication with the ETCS on-board) is achieved.
- The "Profibus Processor" and "Functional Processor" share the same power supply. This power supply is independently monitored by the Companion Chip.

Linked Work Items	has parent: STMA-27947 - Communication ETCS <-> STM ATB via Profibus

3.3.2 Internal communication between processors

Apportionment, STMA-27962 - Internal communication between the FPGA (IO Channels and Diagnostic Channel), the Functional Processor and the Profibus Processor is assured using CRC protection, i.e. "reactive fail safety".

Linked Work Items	has parent: STMA-27958 - Internal communication between processors

3.3.3 Communication with the netX51

Apportionment, STMA-27964 -
The SPI connection between the Profibus Processor and the netX51 is protected by the safety layers as described in D 4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0) and D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0) and as such part of the "black channel" communication between the STM ATB (Functional Processor) and the ETCS on-board.
The interface is implemented according to the guidelines given by the netX51 supplier (Hilscher).

Linked Work Items	has parent: STMA-27963 - Communication with the netX51

4 Detection of single faults

Text, STMA-29135 - The way single faults are detected in the STM ATB differs per part. The parts considered are the same as those considered concerning independence (chapter STMA-25945 - Independence of items) :

- Input circuits and IO Channels.
- Functional Processor.
- Communication.

Relevant is the assurance (= confidence) that a first fault will be detected before a second fault can become hazardous

(STMA-27422).

note: faults in monitoring functions which do not monitor a safety function, but conditions which shall be kept to fulfill calculated failure rates (e.g. temperature and voltage monitoring) are not considered as a first fault which shall be detected within the system safety time.

Text, STMA-38167 - The general principle is:

- Safety relevant circuits and functions are monitored using the Functional Processor.
- The FPGA functionality is monitored from the Functional Processor.
- The hardware integrity of the FPGA is checked at start-up and run-time.
- The hardware integrity of the CPU and memory in the functional processor are checked at start-up and run-time by peripherals (e.g. hardware ECC checkers and 2nd CPU plus CPU Compare Module) in the Functional Processor.
- The peripherals used for checking the CPU and memory are checked at start-up and run-time using software running at the CPU and memory.
- Software integrity is checked using run-time CRC checking on flash.
- All internal communication is protected using CRC.

Apportionment, STMA-72702 - The result of the FMEA performed to analyze the effect of single faults can be found in D6.9.2 FMEA Hardware.

Linked Work Items	has parent: STMA-27489 - Detection of single faults , apportions: STMA-27422 - - Whichever technique or combination of techniques is used, assurance that no si...

4.1 Input circuits

Apportionment, STMA-28973 - The architecture of items in the input circuits concerning the coil signals is based on:

- "inherent fail-safety" is defined as "all credible failure modes of the item are non-hazardous." The ATBEG concept is based on inherent fail safety. In the infrastructure all components used to generate and transmit the code are single systems, however it is assumed that the information is coded in such a way (75Hz and a specific modulation frequency) that it's not credible a fault would lead to generating such a complex signal. Any credible fault will lead to corruption of the signal, resulting in "noCode". This principle is extended to the on-board for the circuits which transmit the signal including the safety coding (modulated 75Hz signal), i.e. the analogue input circuits and the IO channels up to the 75Hz filters.
  and
- "reactive fail-safety"; a test signal is added to the coil signals in order to monitor for single (and multiple) faults. This diagnostic function is designed in a way it will detect faults before a hazardous state can be reached (i.e. before a false code is accepted, thus within 800 ms). The diagnostics are partly implemented in the IO Channels and Diagnostic Channels and partly in the MCU (Functional Processor). The part in the IO Channels and Diagnostic Channel is monitored by the decision algorithm implemented in the MCU; a fault in those parts will be detected like faults in the input circuits.

The integrity of the decision algorithm in the MCU is guaranteed via the mechanisms protecting the Functional Processor.

Linked Work Items	has parent: STMA-27753 - Input circuits

Apportionment, STMA-29045 -

A hazardous situation can only be reached due to a fault in case of a triple fault:

- Both channels are corrupted resulting in an intermittent generation of a 75 Hz signal (resulting in modulation with a code frequency) and
- The diagnostic protection is malfunctioning

or in case of a double fault in combination with specific disturbance from track side:

- One channel is corrupted resulting in an intermittent generation of a 75 Hz signal (resulting in modulation with a code frequency), and
- A disturbing modulated (at an ATBEG code frequency) 75 Hz current is present in the track,
  in the other channel at exactly the same carrier phase, modulation phase, and modulation frequency (independent fault), and
- The diagnostic protection is malfunctioning.

The diagnostic function is independent from the signal analysis as it's a different process, performed in a different type of component.

note: Due to a change in the design, highly unlikely, generation of 75 Hz via the test circuits will be detected. Therefore no credible (STMA-28995) single fault will lead to a hazardous situation.

Linked Work Items	has parent: STMA-27753 - Input circuits

Apportionment, STMA-28995 - No faults which effect 75 Hz without effecting the 145 Hz and 2133 Hz test signals were identified.

Linked Work Items	has parent: STMA-27753 - Input circuits

Apportionment, STMA-27779 - The architecture of items in the input circuits concerning the other (than the coil signals) input signals is based on "composite fail-safety". The comparison between the redundant input signals is done in the software module "Input Handler" (D5.2.1 SwRS for Input Handler) implemented at the Functional Processor, thus independent from the input circuits (STMA-27754 - Functional Processor (MCU: TI-RM48x)).
Faults concerning "the other input signals" have a maximum severity "CAT3", i.e. components implementing those signals shall at least fulfill SIL1 requirements.

Linked Work Items	has parent: STMA-27753 - Input circuits

4.2 IO Channels

Apportionment, STMA-28974 -
The architecture of items in the IO Channels concerning the coil signals is based on:

- "inherent fail-safety" is defined as "all credible failure modes of the item are non-hazardous." The ATBEG concept is based on inherent fail safety. In the infrastructure all components used to generate and transmit the code are single systems, however it is assumed that the information is coded in such a way (75Hz and a specific modulation frequency) that it's not credible a fault would lead to generating such a complex signal. Any credible fault will lead to corruption of the signal, resulting in "noCode". This principle is extended to the on-board for the circuits which transmit the signal including the safety coding (modulated 75Hz signal), i.e. the analogue input circuits and the IO channels up to the 75Hz filters.
- "reactive fail-safety". Concerning the latter a test signal is added to the coil signals in order to monitor for single (and

multiple) faults. This diagnostic function is designed in a way it will detect faults before a hazardous state can be reached (i.e. before a false code is accepted).
Test signals are added to the coil signals to detect single and multiple faults in the IO Channels. Monitoring of the test signals is done in the Functional Processor (RM48x). The integrity of the monitoring by the Functional Processor is guaranteed via the mechanisms protecting the Functional Processor (Functional Processor, see STMA-28957 - IO Channels).

- "composite fail-safety": the information from the coil signals is duplicated (one instance added to a sum) after digitalization and processed through the other IO Channel.
  The information is passed via the other IO Channel to the Functional Processor, which will check the 75 Hz filter using 75 Hz filtering at the summed coil signals. By using the summed signal also diversity in the data is created. On top of that a time shift (5 ms) between the two channels is implemented.
  The integrity of the monitoring by the Functional Processor is guaranteed via the the mechanisms protecting the Functional Processor (see STMA-28957 - IO Channels).

Linked Work Items	has parent: STMA-28957 - IO Channels

Apportionment, STMA-29046 - A hazardous situation can only be reached due to a fault in case of a triple fault:

- Both channels are corrupted resulting in an intermittent generation of a 75 Hz signal and
- The diagnostic protection is malfunctioning

or in case of a double fault in combination with specific disturbance from track side:

- One channel is corrupted resulting in an intermittent generation of a 75 Hz signal, and
- A disturbing modulated 75 Hz current is present in the track in the other signal at exactly the same modulation phase and frequency and phase, and
- The diagnostic protection is malfunctioning.

The diagnostic function is independent from the signal analysis as it's a different process, performed in a different type of component.

Linked Work Items	has parent: STMA-28957 - IO Channels

Apportionment, STMA-28972 - The architecture of items in the IO Channels concerning the other (than the coil signals) input signals is based on "composite fail-safety". The comparison between the redundant input signals is done in the software module "Input Handler" (D5.2.1 SwRS for Input Handler) implemented at the Functional Processor, thus independent from the input circuits (STMA-27754 - Functional Processor (MCU: TI-RM48x)).

In addition the configuration signal is protected with a 145 Hz and 2133 Hz test signal (the same as used for the coil signals). This way the configuration signal (which should be constant) is also used to detect illegal (75 Hz) injection via the test signals.
Before the signal is split (i.e. the 75 Hz is split from the test frequencies). The sum of two 75 Hz signals is redirected via the other IO Channel (diverse redundancy) to check the primary signals.

The brake pipe pressure signals are only protected by redundancy. However the requirements concerning those circuits are less strict as a fault concerning those signals leads (only) to a CAT3 hazard (i.e. SIL1 requirements apply to parts only used for the brake pipe pressure signals).

Linked Work Items	has parent: STMA-28957 - IO Channels

4.3 Diagnostics concerning analogue input signals

Text, STMA-29145 - To protect the coil signals (analogue inputs) a DC test signal and an AC test signal is summed up with the input signals (coil signals and configuration signal). Different categories of faults concerning the diagnostics are distinguished:

- Faults leading to unavailability of the diagnostic functions.
- Faults leading to "false alarms".
- Faults leading to generating a false (potentially valid ATBEG) signal.

The test signals protect the analogue input circuits as well as the IO Channels.

4.3.1 Unavailability of the test signals or false alarms

Text, STMA-29146 - The test signals are started after initial system testing. As only intermittent faults can be hazardous (a constant offset in the coil signal level will only lead to availability problems) the variation of the test signal level is continuously monitored.
The level of the test frequencies is calculated in the IO Channels.
The level of the test signals is monitored in the Functional Processor.

Text, STMA-72643 - Potential faults in test signal generation leading to unavailability of the diagnostic functions or false alarms:

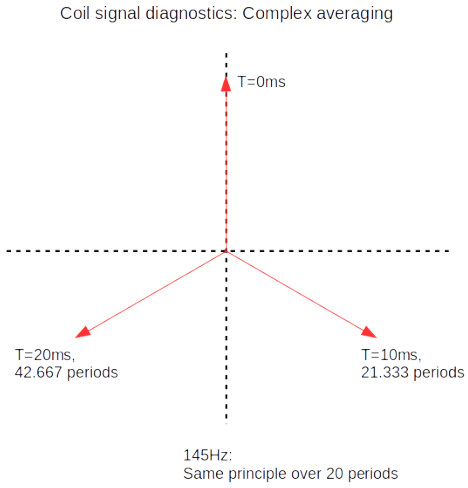
Definition, STMA-28983 - Disturbance (including the result of faults) of the test signals not leading to a signal comparable with a valid ATBEG signal.
Such a fault will either not effect the diagnostics or will lead to (false) detection of a fault, i.e. lead to an availability problem.

Definition, STMA-28984 - "Stuck at faults" at the calculation of the test frequency levels (in the IO Channels).
Such a fault would lead to not recognizing variations in the test signal level and thus lead to undetected unavailability of the diagnostic functions.

Text, STMA-72642 - Measures:

Definition, STMA-28979 - Complex averaging, detection of "stuck at" faults.
The level of the test frequency is calculated as a complex value. Even if the amplitude is constant, the phase of the value shall change every cycle as the cycle time (10 ms) is not a multiple of the period times of the test frequencies.
Therefore the complex average is calculated over a number of periods which should lead to "0" (see STMA-28992), if not then the diagnostic function cannot be trusted.

Definition, STMA-28992 - Figure: complex averaging



4.3.2 Unintended generation of a valid ATBEG signal

Text, STMA-29147 - If a fault in the generation of the test signal causes an injected signal with the characteristics of a valid ATBEG signal, then the diagnostic function could itself cause a hazardous situation.
An analysis (STMA-40816 - Annex D: Preliminary FMEA test signals) has been done to analyze the hardware defects and disturbance which could lead to such a fault. As a result of the analysis a read back of the test signal via the configuration signal has been implemented.
The configuration signal is a constant voltage (derived from the stabilized power supply with resistors). The test signals mixed on the configuration signal will not be disturbed by the measured signal. Therefore the 145 Hz and 2133 Hz components in the configuration signal shall be exactly equal to the injected values, and no 75 Hz component may be present.

Potential faults leading to generating an ATBEG signal like test signal are mitigated by guarding the harmonics in the configuration signal (which are mitigated by the read back via the configuration signal):

Definition, STMA-28988 - Intermittent disturbance of the clock line (or data line, however the impact on the data line will be lower) between the Diagnostic Channel and the DA converter.

Definition, STMA-28989 - Intermittent disturbance of the DA converter (or buffers used to sum the output signal of the DA converters
A fault which repeats at 75 Hz and which is switched on and off at an ATBEG code frequency.
A first fault will not lead to an unsafe state however a second fault will.
A first fault will likely lead to availability problems.

Definition, STMA-28978 - 75 Hz injection due to supply disturbances (e.g. switch off of negative supply).

Text, STMA-72641 - Measures:

Definition, STMA-28991 - Read back of the signal sent to the DA converters.
The output signal of the DA converters is summed to the coil signals as well as to the configuration signal. Monitoring the 75 Hz level in the configuration signal mitigates the risk of generating an ATBEG signal by the DA converter.

Definition, STMA-42187 - Switch off the positive supply of the analogue circuits if the negative side is not available.

4.3.3 Corruption of an ATBVv signal

Apportionment, STMA-74564 - The corruption of ATBVv signals will only (in a very little fraction of the cases) lead to a CAT4 failure, and thus a single fault leading to a failure is acceptable. However the 2133 Hz test signal is analyzed with an ATBVv window. Only in case of a corruption in the FPGA after splitting the signal an undetected fault is possible. A further measure as specified in requirement STMA-29935 could have further limited the risk. However as the risk was already sufficiently, implementation of the requirement was not necessary.

Linked Work Items	has parent: STMA-74563 - Corruption of an ATBVv signal , apportions: STMA-29935 - The ATBVv signal calculations shall all be executed at the same HW resources in...

4.4 Functional Processor (MCU: TI-RM48x)

Text, STMA-29148 - An MCU (Micro Controller Unit) designed for safety applications (TI-RM48x) is used as "Functional Processor". The safety relevant components in the MCU are:

- The CPU.
- The memory: SRAM, flash and static memory.

Other parts of the RM48x are protected by measures at application level (e.g. CRC protection of all communication)..
The way safety is reached differs per part of the RM48x. However overall the RM48x is classified as a system with a HFT=0 and SFF > 99 %. Concerning redundant parts the redundancy is used as mechanism to detect faults, and therefore according to the definitions in the IEC61508 not considered as redundancy but as a diagnostic function (with a high coverage, i.e. > 99 %).

The SIL according to IEC61508 is based on HFT=0 which in combination with a SFF >99 % leads to acceptability for SIL3. The certificate concerning the RM48x states “HFT=0”. According to the definition in IEC61508-2 the HFT is defined as the minimum number of faults which can cause a hazardous situation minus one, **excluding** measures to mitigate the consequences of a fault are **not taken into account**. Systems with a "reactive fail safety architecture" are classified with HFT = 0, even if a second fault in the monitoring part is necessary to reach a hazardous state.
Therefore "HFT=0" in terms of the IEC61508-2 cannot be translated in "a single fault can be hazardous" in terms of the EN50129. However in case "HFT=0" in terms of the IEC61508-2 it can also not be guaranteed that:
Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated (EN50129, B3.1 STMA-27422) and
“A first fault (single fault) which could be hazardous, either alone or if combined with a second fault, shall be detected and a safe state enforced...” (EN50129:2003, B3.3, STMA-27413).

Therefore additional proof is necessary concerning the effect of single faults.

Apportionment, STMA-72704 - The resulting risk concerning unsafe faults in the Functional Processor is analysed, the results are reported in D6.9.3 FMEDA Hercules and Companion Chip.
A short description of the measures in the Functional Processor to protect the calculations and data storage are described in:

- STMA-28762 - Redundant CPUs and
- STMA-28763 - Memory

Linked Work Items	has parent: STMA-27754 - Functional Processor (MCU: TI-RM48x) , apportions: STMA-27422 - - Whichever technique or combination of techniques is used, assurance that no si...

4.4.1 Safety concept of the application

Text, STMA-42186 - The application is built in a way that transient faults will not lead to an unsafe state (STMA-29136). In addition the number of relevant static faults is limited by recalculating all internal variables every cycle. This limits the safety critical stored data relevant for CAT1 faults, to the safety relevant input data (15 variables). This leads to a very high "safe failure fraction".

Text, STMA-29136 - As the ATB function is used to calculate the EB command (and indications different from the Cab signals), any delay has some impact on a safety function (faults leading to CAT3 or CAT4 failures). All faults shall be detected and mitigated (in a time sufficiently short to fulfill the safety targets). Detection and mitigation can take up to 2 s, e.g. in case of losing a telegram at the Profibus as the detection mechanisms prescribed by ERA allow those delays. As the safety target for short faults is less strict than the safety target for longer faults, this 2 s is defined as the "system safety time".
Faults in the "protected data" are detected within 10 ms (one cycle). This is sufficient to fulfill the specified quantified safety target (STMA-27413).
Simultaneous faults in the module calculating the EB command and the module calculating the CAB Signals are only safety critical if the cab signals are shown 2 s before the EB command is corrupted, as the driver needs time to respond to the faulty cab signals.

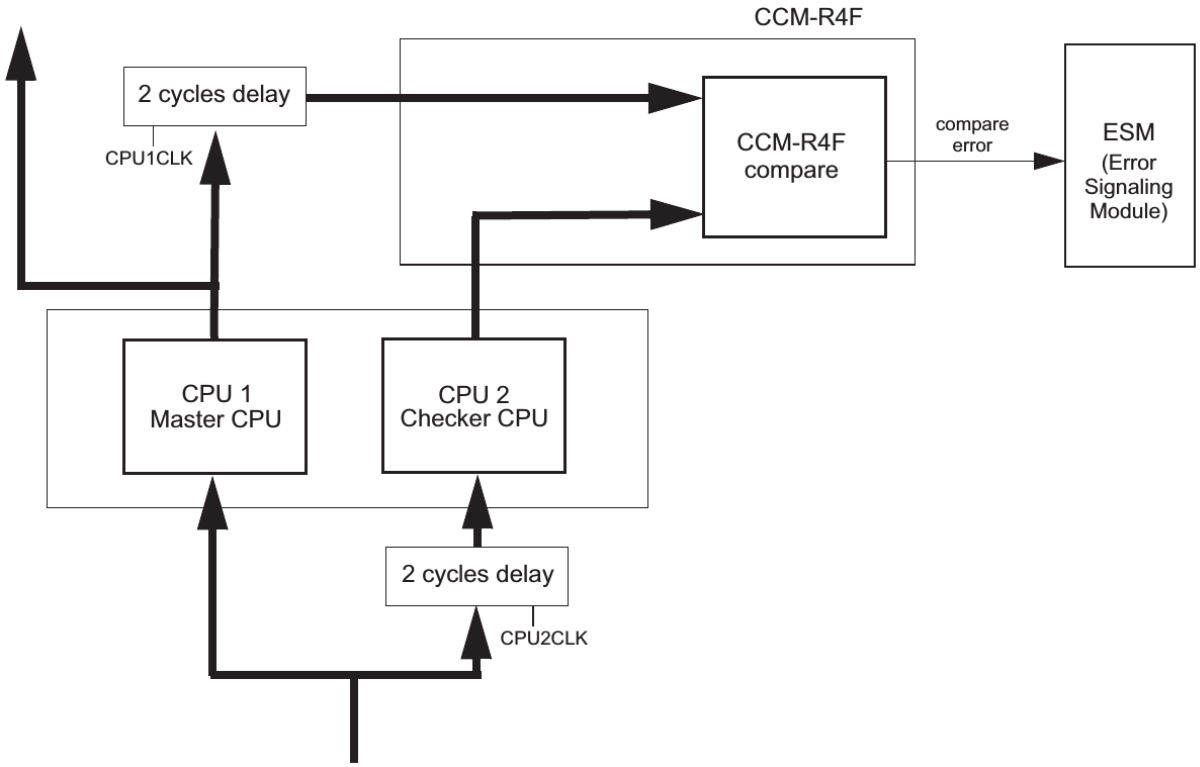
Text, STMA-72705 - The analysis concerning the criticallity of the stored and calculated variables is reported in D6.9.1 FMEA Software.

4.4.2 Redundant CPUs

Apportionment, STMA-27486 -
The CPU in the RM48x is implemented redundantly with external comparison (figure STMA-28720), i.e. a "composite fail safety" architecture, with the exception that no voting algorithm is implemented. The "checker CPU" plus "CCM" (see figure STMA-28720) is used to report eventual errors. Therefore the "checker CPU" plus "CCM" can also be regarded as a diagnostic function, thus a "reactive fail safety" architecture.

Linked Work Items	has parent: STMA-27538 - Calculations , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Definition, STMA-28720 -



Apportionment, STMA-29049 - A comparison is made between the results (a.o. the data and address bus) of both CPUs every clock cycle, i.e. every 5 ns by the CCM (CPU comparison module). This is much faster and effective compared to commonly used architectures (see STMA-72744).
Conclusion: requirement STMA-27413 is met for the redundant CPUs in combination with the CCM (CPU comparison module).

Independence between faults is provided by a time shift between the CPUs, by a difference in orientation and by the distance between the CPUs. Independence between the CPUs and the CCM is reached while the functional and technical implementation of the CCM is not comparable to the CPUs.
The CPUs are checked by the CCM and the CPUs are tested at start-up.
The CCM is run time checked using software running at the CPUs.
A CCF analysis concerning (o.a.) the CPUs is reported in D6.9.4 Common Cause Failure Analysis
The effectiveness of the measures is shown by the D6.9.3 FMEDA Hercules and Companion Chip performed according to the application conditions prescribed by TI.

Linked Work Items	has parent: STMA-28762 - Redundant CPUs

Text, STMA-72744 - Comparison with commonly used 2oo2/3 architectures
2oo2/3 architectures with redundancy at application level are commonly used. Below these architectures are compared to a lockstep architecture with two CPUs and a CCM (CPU Comparison Unit).
The more the testing of elements can be staggered, the lower the risk a second fault will occur before the first fault is detected and mitigated. Using redundant CPUs in lock step as described in STMA-29049, faults in the functional parts will be detected (nearly) immediately by hardware diagnostics (lock-step processor and ECC checking), and with a high coverage.
Detection of faults in the CCM (which can also be a first fault) is discussed in paragraph STMA-28808 - Diagnostics.

Compared to redundancy at application level (two separate systems, i.e. a 2oo2 architecture) this principle is much faster and has a much higher coverage.
(A "standard" comparison at application level is done typically 1 to 10 times per second, and is only taking into account (a part of) the results at application level.)
In case of using “composite fail-safety” at application level (commonly used 2oo2 architecture) only faults which have an effect of the output of the separate modules can be detected. Faults not effecting the output will remain in a dormant state until having effect or until being detected using additional diagnostics. System characteristics leading to a shorter time to detect faults and leading to a higher chance of detecting faults are:

- The frequency at which outputs are compared
  The higher the frequency the shorter the detection time
- The extent to which outputs are compared.
  If a comparison is only made at application level, faults will only be detected at the moment they have an impact at application level.
  If a comparison is made on a very low level, more faults will be detected

In general: the lower the level at which the comparison is done the sooner a fault will be detected. A fault which can lead to a faulty system output can also be detected before effecting the system outputs if checks are done on internal variables.

If a comparison at application level is made (commonly used 2oo2 architecture), faults can be dormant up to the moment a specific condition requiring the defect component is reached. Meanwhile a second fault might have occurred.
Therefore the lock-step principle (reactive fail safety at a technical level) is much more effective than composite fail safety with comparison at application level.

4.4.3 Memory

Apportionment, STMA-27488 - Reactive fail-safety concerning the data storage of the "Functional Processor":
SRAM, Flash and permanent memory in the RM48x are protected with ECC coding (see STMA-28765). Up to eight bits fault per 4 words (64 bits) will be detected and mitigated. i.e. memory is protected using a "reactive fail safety" architecture.
The ECC codes are calculated and checked in the redundant CPUs, therefore the memory as well as the connection between CPUs and memory is protected by two independent items. The CPU output is split in two parts (2x 36 bits) which are stored in separated memory (at different locations on chip).
In case of an ECC fault this is indicated to the application which initiates safe action (in case of an ECC fault this will be a complete system reset).

Linked Work Items	has parent: STMA-27541 - Data storage , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Definition, STMA-28765 -

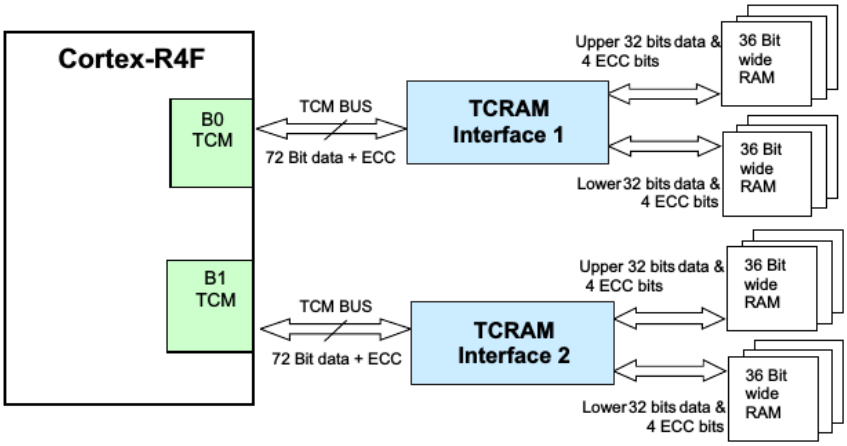


Figure 6-10. TCRAM Block Diagram

(document rm48l952, page 85)

Apportionment, STMA-29050 - Characteristics of the ECC code: Up to two bit faults in one word will be detected. Therefore single faults will be detected. According to the safety manual concerning the RM48x measures are taken to enhance independence.
As stated in paragraph paragraph 7.4, 7.5 and 7.6 in the safety manual the FEE (permanent), flash and SRAM memory "... have a bit multiplexing scheme implemented such that the bits accessed to generate a logical (CPU) word are not physically adjacent."
Although the measures help to achieve a very low unsafe undetected failure rate (see STMA-28764 - Conclusion concerning the Functional Processor), which is significantly lower than the overall safety target (app 2.6*10^-10/hour vs. the required 1.9*10^-8/hour).

*note: The calculated fault rate includes all clock faults although the clock is not safety critical for the application. TI can however, not guarantee that the clock is not safety relevant for technical functions (e.g. reading memory). If the clock is set to not safety critical the calculated fault rate drops below 5*10^-12/hour (lowest value), even with a safe failure fraction of 50 %.*
If the clock is safety critical due to the effect on technical functions (e.g. reading memory or common cause CPU faults) then the safe failure fraction concerning those faults will be very high (>>99 %) as most memory or CPU faults are either detected and/or lead to a safe response in the application.

*note: The calculated fault rate is based on a safe failure fraction of 50%. In practice this value will be much higher (expected > 99 %, see STMA-41102 - Underpinning the safe-dangerous ratio). If 99 % is used as safe failure fraction the calculated fault rate drops below 5*10^-12/hour (lowest value), even if the clock is considered to be safety critical.*

Conclusion:
If

- The faults are not considered "incredible" based on the quantitative analysis, and
- Multiple bit faults are considered to be one fault, or a common cause fault

then requirement STMA-27413 is not met with the "reactive fail safety architecture" as implemented in the RM48x, therefore additional measures are possible, as described below.

Linked Work Items	has parent: STMA-28763 - Memory

4.4.4 Additional measures to detect single memory faults

Text, STMA-29052 - Three types of storage are relevant concerning safety:

- The data and the stack stored in SRAM.
- The program code, stored in flash.
- Permanent data stored in flash (FEE).

Faults are divided in permanent faults and transient faults:

- Permanent fault: hardware defect.
- Transient fault: one time disturbance.

General principles to mitigate permanent faults:

- Run time self tests on memory.
- Recalculation of all derived safety relevant variables in every calculation cycle, in combination with only accepting a less restrictive state after 3 successive cycles confirming the conditions for the state change.
- Changing position of the stack in memory each cycle (at least three positions shall be defined) and accepting unsafe state transitions and timer changes only after 3 successive cycles giving the same result

The self test frequency is sufficient to detect defects within the “process safety time”.
Independence between multiple faults is provided by the difference in the type of fault. One fault concerns a hardware fault, the second fault concerns the execution of self tests (CPU or, another part, of the flash memory).

Text, STMA-38482 -
Transient faults could lead to an unsafe state due the following mechanisms. For those faults mitigation measures are defined below.

Definition, STMA-28781 - Input data concerning coil signals is corrupted while being stored.

Definition, STMA-28782 - Configuration information, speed information, state information or brake handle applied information is corrupted while being used.

Definition, STMA-28788 - Configuration information received from the ETCS on-board is corrupted while being stored.

Definition, STMA-28789 - Speed information received from the ETCS on-board is corrupted while being stored.

Definition, STMA-38476 - State information (timers, state machines and ATBEG code) is corrupted while being stored.

Definition, STMA-28779 - Faults in storing or reading intermediate results.

Definition, STMA-28784 - Due to corruption of program code (read from flash) the result of an if-then-else condition is inverted.

Definition, STMA-28786 - Due to corruption of program code (read from flash) a random jump in the execution is made.

Definition, STMA-28783 - Due to corruption of program code (read from flash) an operation is changed (e.g. replace addition by multiplication), leading to faulty calculation results.
note: as corruption of program code can occur outside the CPUs it's not always protected by CPU redundancy.

Text, STMA-29149 -
Measures mitigating transient faults:

Definition, STMA-42197 - *CRC check on the executable code (in flash)*
The flash is checked every 2 s as part of the HW monitor (D6.2.12 SDD Functional Processor Hardware Monitor).

Definition, STMA-38526 - *State checking*
States are coded in a way (using enums) that at least three bits shall be corrupted before a false valid state can be

selected.

Definition, STMA-28778 - *Limit the accepted deceleration in the train speed value (i.e. the decrease of the train speed) used for the ATBEG+Vv function*

Speed information is refreshed every 0.5 s (STMA-2763/STMA-11680). A fault could delaying an EB command.
To limit this risk in case of data corruption, physically impossible changes is the speed value are corrected. I.e. if the speed decreases faster than physically possible, the decrease is limited.
Measure: limit the speed at which the "current train speed used for the ATB function" decreases.
(included in STMA-2928 /STMA-3020)

Definition, STMA-28775 - *Limit the change in the 75 Hz level (absolute and relative between successive samples)*

A single corrupted sample (one output value of a 75 Hz filter) of the track signal can not cause a hazardous situation, however extremely high (clearly incorrect) values are not possible and are therefore an indication of a fault which justifies a "decoder reset".
Measure: if the change of the 75 Hz track signal (filter output as received from the IO Channels) exceeds feasible limits then the decoding will be reset.
(included in STMA-28692)

Definition, STMA-28776 - *Transitions to less restrictive states or timer values are only made after three successive cycles in which the conditions are met.*

A single corrupted sample of input information indicating that the brake handle is operated by the driver could reset the over speed timers and therefore lead to a delay of up to 5 s in applying the brakes. This mitigated by a delay in resetting the timers; i.e. only if the conditions for resetting the timers are confirmed three successive cycles, the timers will be reset.
Measure: the timers and only reset the safety critical timers if the conditions are met three times.
(STMA-15667 , STMA-15672 , STMA-15673).
Independence between multiple faults is provided by the time difference. As the typical time between two calculations is 10 ms (cycle time) one or multiple simultaneous transient faults will not lead to a fault in successive calculations.
The described measures are detailed below.

Definition, STMA-28785 - *Golden sequence (external software sequence monitoring)*

To protect against faulty jumps in the program (apart from redundancy in safety critical calculations) the software sequence is checked using codes generated at execution of the activities in the Functional Processor, by the Companion Chip (watch dog).

Definition, STMA-28787 - *Monitoring by the ETCS on-board*

Safety measures as defined in the Safety Layers protect against a (partial) "freeze".
If the program execution stops, no telegrams will be sent anymore. This is a safe state as ETCS has to take responsibility for safety if the connection with an STM in DA state is lost.

Apportionment, STMA-29053 - Linking measures to transient faults:

Below the mitigating measures are grouped per anticipated transient fault.

Speed information received from the ETCS on-board is corrupted while being stored (STMA-28789).
STMA-28778 - Limit the accepted deceleration in the train speed value (i.e. the decrease of t...

Coil signals are corrupted while being stored or used (STMA-28781).
STMA-28775 - Limit the change in the 75 Hz level (absolute and relative between successive sa...

State information is corrupted while being stored (STMA-38476)
STMA-38526 - State checking States are coded in a way (using enums) that at least three bits...

Input data concerning brake operation by the driver is corrupted while being stored or used (STMA-28782).
STMA-28776 - Transitions to less restrictive states or timer values are only made after three...

Configuration information or speed is corrupted while being read. (STMA-28779).
STMA-28776 - Transitions to less restrictive states or timer values are only made after three...

Due to corruption of program code (read from flash) the result of an if-then-else condition is inverted (STMA-28784).
Protected by RM48x safety measures (ECC).
STMA-28776 - Transitions to less restrictive states or timer values are only made after three...
As an unsafe result will be recalculated three times before becomming effective

Due to corruption of program code (read from flash) a random jump in the execution is made. (STMA-28786).
Protected by RM48x safety measures (ECC)
STMA-28774 - Regular resending of critical information At a few state (or state variable) tra...
STMA-28785 - Golden sequence (external software sequence monitoring) To protect against fault...
STMA-28787 - Monitoring by the ETCS on-board Safety measures as defined in the Safety Layers...

Due to corruption of program code (read from flash) an operation is changed (e.g. replace addition by multiplication), leading to faulty calculation results. (STMA-28783).
Protected by RM48x safety measures (ECC)

Conclusion concerning transient memory faults in the RM48x:
Concerning single transient memory faults requirement STMA-27413 is met because no single (or simultaneous multiple) transient faults will lead to a hazardous situation.

Linked Work Items	has parent: STMA-28770 - Additional measures to detect single memory faults

4.4.4.1 Permanent memory faults

Text, STMA-29054 - The measures used for transient faults are not all effective for permanent faults:
Recalculation (over three cycles or redundant calculation of state machines and timers) is not effective if the same defect can have the same effect twice.This can be the case due to (see below):

Definition, STMA-28803 - permanent faults in flash (program code),

Definition, STMA-28804 - permanent faults in SRAM, leading to repetitive faults in "intermediate" variables,

Definition, STMA-28802 - permanent faults in SRAM, leading to faults in data stored in the stack.

Text, STMA-73911 -
Measures (executed run time) concerning permanent faults:

Definition, STMA-28806 - Flash used for the program code is checked cyclically with a cycle time within the system safety time; a CRC check performed on the flash is sliced in a way the total check will not last longer than 2 s.

Definition, STMA-28805 - The position of the stack is moved slightly between two successive cycles.

Definition, STMA-28812 - CRC checking of flash memory
The checking mechanism is required to protect the flash, i.e. to guarantee absence of permanent faults. CRC checking of flash memory is used to guarantee the integrity of the program code. Therefore a CRC check is performed every cycle (every 10 ms) on a next part of the flash memory. The parts of flash to be checked are chosen in a way the whole program is checked every 2 s.

Text, STMA-29055 - In addition the integrity of the system is tested at start-up:

- SRAM checking

- Integrity tests CPUs

Apportionment, STMA-29056 - Conclusion concerning permanent memory faults in the RM48x flash and stack, based on measures described in STMA-28812 and STMA-28805:
Concerning single permanent memory faults requirement STMA-27413 is met because single permanent faults will be detected by diagnostic functions within the system safety time. (in addition to ECC coding)

Linked Work Items	has parent: STMA-28772 - Permanent memory faults

4.4.5 Diagnostics

Text, STMA-29057 - A first fault can concern a diagnostic function which is necessary to detect faults which could lead to a hazardous state. Therefore diagnostics shall be checked

Diagnostics needed to detect potential hazardous faults are:

Definition, STMA-28811 - The CCM (CPU comparison module).
This module is needed to detect faults in (one of) the CPUs.

Definition, STMA-28810 - The ECC checker.
This function is not required to comply with EN50129:2003, B3.3, STMA-27413, as additional measures concerning memory have been taken. However to comply with the quantitative requirements, figures based on an active ECC are used.

Definition, STMA-28815 - Memory checking
The SRAM can be tested using "write & read back tests", those tests are provided by the "TI safety library" and can be run at start-up.
Configuration data (technical processor configuration data) is also read back during runtime.

Apportionment, STMA-38586 - Measures concerning the CCM (STMA-28811):
The CCM is a hardware diagnostic system checking the CPUs. Tests are performed at start-up and run time within the "system safety time" (2s) (safety manual 7.10/7.11, & appendix A, table 4).
Defects in the CCM (leading to always accepting have to be detected within "a time sufficiently short to fulfill the specified quantified safety target" (EN50129:2003, B3.3, STMA-27413).

Linked Work Items	has parent: STMA-28808 - Diagnostics

Apportionment, STMA-38587 - Measures concerning the ECC (STMA-28810):
The ECC checker will be tested at start-up and run-time by reading (known) locations with ECC errors. The frequency of these tests will be such that faults are detected within the "system safety time".

Linked Work Items	has parent: STMA-28808 - Diagnostics

Apportionment, STMA-38584 - Measures concerning the flash memory (STMA-28812)
The CRC checking is implemented in hardware and cyclically called from the program running in the redundant CPUs. The hardware CRC calculation will return a result which will be compared with a stored CRC. Faults in the hardware CRC calculation parts will be detected as a faulty CRC. Faults in the CPU are protected using the "lock-step" diagnostics.

Linked Work Items	has parent: STMA-28808 - Diagnostics

Apportionment, STMA-38585 -

Measures concerning the SRAM (STMA-28815).
The SRAM tests use predefined diagnostic software. The software is protected by the CRC checking on the program code, and the execution of the in the CPUs is protected using the "lock-step" diagnostics.

Linked Work Items	has parent: STMA-28808 - Diagnostics

Apportionment, STMA-38583 - Conclusion: the integrity of the diagnostics is monitored within 2 s. A second fault after more than 2 s will therefore not lead to a CAT1 hazard.
A second fault within 2 s can lead, in combination with a second fault in the monitored system parts, to a CAT2 hazard, however the chance is sufficiently low to fulfill the safety target concerning CAT2 hazards (STMA-27631 - P_CAT2 < 2.0*10^-6/operational hour). Based on the safety analysis a higher fault rate is acceptable (STMA-34970), see also D 6.9.3 FMEDA Hercules and Companion Chip).

Linked Work Items	has parent: STMA-28808 - Diagnostics

Text, STMA-42209 - Detailed checks on the HW are defined in D5.2.12 SwRS for Hardware Monitor and D6.2.12 SDD Functional Processor Hardware Monitor.

4.4.6 Conclusion concerning the Functional Processor

Text, STMA-38596 - Safety critical functions used from the TI RM48x concern calculation and storage functions. Both are covered by the TI safety measures. The quantitative safety can be calculated using the “FMEDA tool” provided by TI (D 6.9.3 FMEDA Hercules and Companion Chip). This tool is certified against IEC61508-2. The requirements concerning FMEA in the EN50126-129 are covered by the requirements in IEC61508-2. Therefore quantitative safety can be proven using the FMEDA tool.
The resulting "unsafe undetected failure rate" concerning all aspects of the RM48x which are safety relevant for the STM ATB is app. 2.6*10^-10/hour, taking into account the safety measures provided by TI, but not taking into account the additional safety measures to protect the memory (see STMA-28763 - Memory).

The additional safety measures lead to a very high "safe failure fraction". However as the requirements are already met with a standard "safe failure fraction" of 0.5, no detailed calculations have been done. (see D6.9.1 FMEA Software, chap ter STMA-41102 - Underpinning the safe-dangerous ratio). As only faults concerning one of the 15 critical variables can hamper safety the realistic safe failure fraction will be << 1%
Taking into account a higher safe failure fraction would lead to an unsafe failure rate of arround 10^-12/hour.
However as the requirements are already met with a standard "safe failure fraction" of 0.5, no detailed calculations have been done.

If the clock is marked as not safety critical, the unsafe failure rate drops to below 5*10^-12/hour (i.e. below the resolution of the calculation). As clock faults are guarded by ETCS (safe time layer) and from the FPGA, it is realistic to assume that no clock fault will lead to an unsafe state.
However as the requirements are already when taking into account the clock as safety critical, no detailed analysis concerning its safety relevance have been done

As the resulting "undetected unsafe failure rate" is far lower than the system safety target for CAT1 hazards (>3s), it can be concluded that the time to detect first faults is sufficiently short to fulfill the quantified safety target.

Additional measures (STMA-42188 - Safety concept of the application and STMA-28770 - Additional measures to detect single memory faults) have been taken on top of standard diagnostics provided for the RM48x to guarantee the mitigation of single faults. However for the quantitative safety targets is not necessary.

4.5 Communication

4.5.1 Communication ETCS <-> STM ATB via Profibus

Apportionment, STMA-38598 - The mechanisms to detect communication faults at the profibus (corruption of the telegrams. loss of telegrams or delays out of specification) are detected according to prescribed tests (D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0) and D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0)).
Therefore communication faults will be detected with an assurance as specified in those subsets (depending on the failure rate at the Profibus outside the STM ATB). The method described in those subsets complies with *STMATB/0_ Development/EN50159_2010*.

Linked Work Items	has parent: STMA-27971 - Communication ETCS <-> STM ATB via Profibus

Text, STMA-38599 - Conclusion:
According to the calculations provided in the ERA specifications (D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0)) there is a remaining risk concerning undetected unsafe communication faults. However as the communication is prescribed via a single link (optional redundancy is only used for availability), there is no alternative for the chosen implementation.
The measures prescribed in the ERA subsets lead to disconnection (followed by resending information). The consequence is a delay in the communication which a.o. depends on the performance of the ETCS on-board, however delays between 30 ms and 3 s are in all cases possible. Therefore a disturbance can lead to a CAT2 or a CAT4 failure.

4.5.2 Communication between processors

Apportionment, STMA-38600 - The CRC protection used for internal communication is copied from the CRC protection as defined in D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0). As the basic failure rate of a SPI connection is significantly lower than the basic failure rate of a profibus connection, the connections are sufficiently protected against unsafe failures according to *STMATB/0_ Development/EN50159_2010*. In addition single faults (even if not detected) in the internal communication cannot cause an unsafe situation:

- Functional Processor <-> IO Channels:
  - single faults in the coil signals (one 75 Hz value) cannot lead to accepting an invalid code
  - single faults in information concerning brake application cannot lead to resetting the warning state as a delay of three cycles has been implemented.
  - Single faults in the ATBVv signal can contribute to missing an ATBVv signal, however a signal will only be missed in such a case in combination with high speed (>70 km/h, thus outside the speed range in which ATBVv shall be active) and a signal level out of specification.
- Functional Processor <-> Diagnostic Channel: faults will lead to faults in the diagnostic functions, i.e. unnecessary safety measures thus availability problems.
- Functional Processor <-> Profibus Processor: Faults in this communication channel will effect the profibus communication and will therefore be detected by the Safety Layers as prescribed by the ERA subsets (D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0) and D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0))

Linked Work Items	has parent: STMA-27970 - Communication between processors

4.6 Timing of the detection

Apportionment, STMA-27671 - The minimum mitigation time of a single fault depends on the type of fault, and the expected rate of the fault.
Note: EN50129:2003 B3.3 (STMA-27413) requires a time "sufficiently short to fulfill the specified quantified safety target". Therefore if the fault rate of the detection mechanism and the fault rate of the monitored function are low, then a longer mitigation time is acceptable.
The times mentioned below are the times within no hazard can arise from the detected fault:

- Faults in the input circuits or IO Channels leading to a less restrictive code: 0.8 s
  The minimum time for the decoder to detect a valid code is 0.8 s
- Storage or calculation faults in the Functional Processor: 30 ms (three calculation cycles).
  A less restrictive state will only be accepted if the conditions are fulfilled at least three calculation cycles
- Faults potentially leading to CAT1 or CAT3 hazards: 2 s
  Only faults which have an effect longer than 3 s, can lead to a hazard of the category CAT1 or CAT3 (per definition: STMA-10870 and STMA-10872). Therefore all faults shall be mitigated within 3 s. Mitigation is done via isolation of the Profibus, after which the ETCS on-board shall guarantee the safe state. An ETCS processing time of 1 s is taken into account.
  Therefore the remaining time for mitigation of the concerned faults is 2 s. (This time is taken into account in all above analysis)

Linked Work Items	has parent: STMA-27759 - Timing of the detection , apportions: STMA-27413 - A first fault (single fault) which could be hazardous, either alone or if combin...

5 Action following detection

Apportionment, STMA-27677 - The safe state for the STM ATB depends of the type of fault to be mitigated:

- In case of faults with an unpredictable consequence (e.g. most faults detected at hardware level in the Functional Processor) the most restrictive measure is isolation from the Profibus. After isolation from the Profibus it's the responsibility of the ETCS on-board to guarantee safety (e.g. by applying the emergency brake).
- In case of faults which effect the ATBEG decoder, a decoder reset is sufficient. The decoder reset will lead to restarting with "noCode" (i.e. speed monitoring against the lowest speed level).
- In case detection of brake operation by the driver fails, ignoring the concerning input will lead to not detecting brake operation by the driver, which is the safe state for this sub function.

The detailed relation between detected faults (events) and measures is described in D5.2.11 SwRS for Event Handler.

The response after fault detection is taken into account in the FMEAs (D6.9.x) therefore those documents provide proof for the effectiveness of the safe states selected per situation.

Linked Work Items	has parent: STMA-27491 - Action following detection , apportions: STMA-27495 - After detection of a first fault, the system/sub-system/equipment shall enter, o... , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

Apportionment, STMA-27678 - Measures may lead to switching off the ATB function by the driver. In such a case the train can run without speed monitoring (STMA-5115 - The train shall provide means to power off/deactivate the STM ATB and inform the...). The resulting risk shall be mitigated by user of the STM ATB (D6.5.2 Technical documentation).

Linked Work Items	has parent: STMA-27491 - Action following detection , apportions: STMA-27493 - The system/sub-system/equipment shall remain in a safe state if further faults o... , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

5.1 Input circuits and IO Channels

Apportionment, STMA-27765 - If a fault concerning the coil signals is detected, the decoder will be reset. After a reset it will take between 0.9 s and 2.8 s (decoding time plus 75 Hz filtering time) before a code will be detected again. During this time the maximum speed monitored is 40 km/h and the driver will be warned for overspeed if the actual train speed exceeds 40 km/h plus margin.
Repetitive faults will lead to operational hindrance, thus taking the train out of service or replacing the STM ATB.

Linked Work Items	has parent: STMA-27764 - Input circuits and IO Channels

Apportionment, STMA-27766 - If a fault concerning the signals indicating that the brake is applied by the driver, is detected, then the concerning input will not be taken into account for "detection of brake operation by the driver" anymore, up to switching off the system. If the measure is due to a fault, the remaining information could be too limited to detect brake operation which will lead to an unexpected and unnecessary EB command.
Such faults will lead to operational hindrance, thus taking the train out of service or replacing the STM ATB.

Linked Work Items	has parent: STMA-27764 - Input circuits and IO Channels

Apportionment, STMA-27768 - If a fault concerning the configuration information (derived from the analogue configuration signal) is detected, then the concerning information will not be used.
Such faults will lead to operational hindrance if no information from the ETCS on-board is available, thus taking the train out of service or replacing the STM ATB.

Linked Work Items	has parent: STMA-27764 - Input circuits and IO Channels

5.2 Functional Processor

Apportionment, STMA-27770 - In case of a fault detected by the diagnostics implemented in the "Functional Processor", the STM ATB will be reset via the "Companion Chip" which also provides power supply and watch dog functions for the "Functional Processor".
The consequence of a system reset is a reset of the decoding (the STM ATB will start monitoring the lowest speed level) and a loss of all profibus connections and configuration data. The STM ATB can only become active again after having received all configuration data (again).
Details of all safety measures in the Functional Processor, including those when detecting faults in o.a. power supply, PCB temperature, the IO Channels or input circuits are described in D5.2.11 SwRS for Event Handler.
After 4 resets the system will not be reset automatically anymore (up to power off).

Linked Work Items	has parent: STMA-27767 - Functional Processor

5.3 Communication ETCS <-> STM ATB via Profibus

Apportionment, STMA-27771 -
Communication faults in the communication between the STM ATB and the ETCS on-board are handled according to the ERA specifications, i.e. a fault will cause a "disconnection" at application level, a second fault will cause a "final disconnection".
In case a fault is detected at the Profibus (either corruption of the data, loss of a telegram or delay) the logical connection (at application level) will be reset. After resetting all relevant state information (EB command and DMI including cab signals) will be resent by the STM ATB. This way the fault is mitigated before it can cause a CAT3 hazard. A CAT4 hazard is possible due to the response time of the ETCS on-board system).
Multiple faults leading to rejection or losing a telegram will lead to final disconnection from the Profibus (i.e. safe state). In the latter case the STM ATB (or the ETCS on-board if the fault was detected there) has to be restarted before a new connection can be set up.

Linked Work Items	has parent: STMA-27966 - Communication ETCS <-> STM ATB via Profibus

5.4 Overview measures to enter into a safe state

Text, STMA-38911 - Different measures are taken depending on the type of fault which is detected. Details are described in D5.2.11 SwRS for Event Handler.

6 Effects of multiple faults

Text, STMA-29306 - The first two requirements (STMA-27499 and STMA-27500) in B3.5 concern the time in which a fault is mitigated. The third requirement (STMA-27497) concerns independence of items. The latter has been discussed in chapter STMA-25945 - Independence of items.

Requirement STMA-27499 states:
A multiple fault (for example, a double or triple fault) which could be hazardous, either directly or if combined with a further fault, shall be detected and a safe state enforced (i.e.: negated) in a time sufficiently short to fulfil the specified safety target.

This could be read as *"Any multiple fault"* however there will always be a number of simultaneous faults which can lead to a hazardous situation. Below a comparison is made between "state of the art" solutions and the STM ATB solution.

The requirement is interpreted as: "a first fault shall be detected in time to fulfill the specified safety target".

comparison:
State of the art in on-board ATP (automatic train protection, like ATB, PZB, ETCS etc.) systems is the use of 2oo2 or 2oo3 systems. Those systems combine a number of outputs every cycle, i.e. typically every 100 ms. If two similar faults occur within the cycle time the faults will not be detected. Faults which only effect an output in a specific situation will not be detected up to the moment the situation occurs.
The architectures chosen for the STM ATB provide a much faster and much more complete detection of faults, e.g.:

- The CPUs are compared every 5ns. At every compare the complete output including addressing is compared. Due to the time shifting, simultaneous multiple faults will greatly be detected, as the execution of similar code is done at different moments.

- ECC checks are done at every usage.
  Memory checking en CRC checking on flash is performed run-time within the system safety time while existing ATB systems only check at start-up and (very limited compared to the current design) run-time with checking times up to several minutes.
- Apart from duplication of the coil signals after digitalization, continuous monitoring is implemented using three test signals.

Text, STMA-72764 - Below mechanisms to detect multiple faults will be described for the different components in the STM ATB in the paragraphs below.

Apportionment, STMA-27751 -
The effect of multiple faults is shown using the FMEA's and CCF analysis (D6.9.2 FMEA Hardware , D6.9.3 FMEDA Hercules and Companion Chip and D6.9.4 Common Cause Failure Analysis).

Linked Work Items	has parent: STMA-27492 - Effects of multiple faults , apportions: STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance... , apportions: STMA-27500 - A suitable method, for example Fault Tree Analysis (FTA), shall be used to demon...

6.1 Multiple faults concerning "brake handle applied information"

Text, STMA-29307 - In case of faults in the input signals or in the input circuits/IO Channel handling "brake handle applied information" single faults will be detected by comparison of the two (diverse in case of digital) signals by the Functional Processor (independent from the input circuits/IO Channels), and will be mitigated before a second fault occurs.
Faulty brake handle applied information can lead to a CAT3 failure. Therefore the function has been categorized as SIL1.

Apportionment, STMA-29010 - Simultaneous multiple identical faults in the analogue brake handle applied signal (currently only used for the black and yellow fleet) will not be detected, however those become visible for the driver; the "white lamp" indication while the brake is not operated. In such a case the driver is responsible for taking the train out of service: D6.5.2 Technical documentation.
Simultaneous multiple inverse faults in the digital brake handle applied signals, will not be detected, however those become visible for the driver; the "white lamp" indication while the brake is not operated. In such a case the driver is responsible for taking the train out of service: D6.5.2 Technical documentation.

Linked Work Items	has parent: STMA-27795 - Multiple faults concerning "brake handle applied information" , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

Apportionment, STMA-27908 - The detection of faults concerning "brake handle applied information" cannot result in a "fail state" in a time shorter than 30 ms (to avoid any effect) while the ATBEG state machine will not respond within this time.
If single faults are detected in the input circuits and IO Channels and also circuits external to the STM (detection time =<5 s: STMA-7820, STMA-7823, STMA-7842 and STMA-7822) then the input will no longer be taken into account (and a safe assumption of the input value is used.
In the meantime (between 30 ms and mitigation) the inputs are conflicting and therefore the safe state for the concerning input data "driver is not operating the brakes" is used (STMA-16606 and STMA-16607).
Not having any brake handle applied information makes it difficult to run the train and will therefore lead to taking the train out of operation at the next main station.

Linked Work Items	has parent: STMA-27795 - Multiple faults concerning "brake handle applied information" , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

6.2 Mitigation of multiple faults concerning the coil signals.

Apportionment, STMA-27912 - Single faults in one of the coil signals with an effect which is big enough to lead (in combination with a similar fault in the other coil signal) to an invalid code, will (without second fault in the other coil signal) cause disturbances in the decoding leading to "noCode". As "noCode" leads to monitoring the lowest speed level, such a fault will disturb train operation, and will therefore lead to switching off the system and taking the train out of operation at the next main station (according to current procedures).|
Single and double faults concerning the track signals will be detected before having an unsafe effect (see STMA-27917)
.

Linked Work Items	has parent: STMA-27773 - Mitigation of multiple faults concerning the coil signals. , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

Apportionment, STMA-27917 - Faults in a coil signal, or in both coil signals, will be detected using an added diagnostic signal (2133.3 Hz; STMA-11882). Faults are analyzed over 0.8 s, the minimum decoding time. Multiple similar faults (in both channels) will be mitigated to guarantee safety. Such faults will lead to resetting the input channels and decoding. In case of multiple resets a system reset will follow. After 4 resets the system is blocked. In that case the user of the STM ATB is responsible for measures to guarantee safety (D6.5.2 Technical documentation .).

Linked Work Items	has parent: STMA-27773 - Mitigation of multiple faults concerning the coil signals. , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

Apportionment, STMA-74562 - Multiple faults in the FPGA after the diagnostic signals have been split from the 75Hz signal (down sampler) are detected with the 75 Hz filtering of the "sum-signal" in the Functional Processor, therefore requirements STMA-29641 and STMA-30223 are not necessary anymore.

Linked Work Items	has parent: STMA-27773 - Mitigation of multiple faults concerning the coil signals. , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou... , apportions: STMA-29641 - The 75 Hz calculation and the 145 Hz calculation shall use the same stored infor... , apportions: STMA-30223 - The ATBEG Fourier Transform calculator shall use the same hardware resources for...

6.3 Multiple faults in the Functional Processor

6.3.1 Multiple faults in CPUs and CCM

Apportionment, STMA-27780 - Multiple faults are avoided by mitigation measures after detecting a first fault. Due to the short detection times the risk that a random second fault can cause a hazard is sufficiently low

- A simultaneous fault in the two CPUs will be detected as the CPUs operate 2 cycles shifted in time.
- A similar fault in the two CPUs but shifted in time is also a multiple fault.
  As the comparison is more extensive and the compare frequency is much higher than in currently used systems, the risk resulting from multiple faults is much lower compared to currently used systems
- A fault in the CCM and a fault in the "master CPU" (see figure STMA-28720) can together lead to a hazardous situation. However the fault in the CCM will be detected using software diagnostics at start-up.
  As shown in D6.9.3 FMEDA Hercules and Companion Chip this test frequency is sufficient to meet the safety

requirements

Additional measures (STMA-42188 - Safety concept of the application and STMA-28770 - Additional measures to detect single memory faults) have been taken on top of standard diagnostics provided for the RM48x.

Linked Work Items	has parent: STMA-29011 - Multiple faults in CPUs and CCM , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

6.3.2 Multiple memory faults

Apportionment, STMA-29014 - Multiple faults concerning memory will be a fault in the functional part (storage) and a fault in the diagnostics (ECC checking).
Both are checked using software diagnostics within the "process safety time" and will therefore be detected before a hazardous situation can arise. In addition measures are taken in software to prevent one undetected memory fault to become hazardous (see STMA-28770 - Additional measures to detect single memory faults).
A third fault is necessary
Conclusion: requirement STMA-27499 is met for a double fault (transient as well as permanent; one in memory and one in the ECC checking) and for triple permanent faults (two in memory and one in ECC checking).
Therefore the coverage of the diagnostics is much higher compared to existing systems, which cross check results at application level.

Additional measures (STMA-42188 - Safety concept of the application and STMA-28770 - Additional measures to detect single memory faults) have been taken on top of standard diagnostics provided for the RM48x.
With those measures single (safety critical) storage faults are detected independent from the HW diagnostics implemented in the RM48x.

Linked Work Items	has parent: STMA-29013 - Multiple memory faults , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

6.4 Multiple faults concerning communication

6.4.1 Communication ETCS <-> STM ATB via Profibus

Apportionment, STMA-29015 - Faults concerning the profibus communication can become hazardous in combination with an (undetected) fault in the diagnostics (Safety Layers). The latter are implemented at the Functional Processor which is checked continuously using its own hardware diagnostics. The hardware diagnostics are monitored (run time) using software tests.
As shown in D6.9.3 FMEDA Hercules and Companion Chip the resulting failure rate is far below the tolerable fault rate (STMA-21149 and STMA-21151).
Conclusion: a multiple (fault at the bus in combination with a fault in the safety layers) undetected unsafe fault concerning profibus communication is possible, however the concept is prescribed and the resulting risk is determined by the safety level chosen for specific connections (see D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0)). The resulting risk is taken into account in the FMEA concerning the STM ATB and cannot be further mitigated within the concept prescribed by the ERA requirements which are compliant with *STMATB/0_ Development/EN50159_2010*.

Linked Work Items	has parent: STMA-27924 - Communication ETCS <-> STM ATB via Profibus , apportions: STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance... , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou... ,

	apportions: STMA-27500 - A suitable method, for example Fault Tree Analysis (FTA), shall be used to demon...

6.4.2 Communication between processors

Apportionment, STMA-29016 - The following communication between processors is implemented:

- Functional Processor (MCU) with the IO Channels (FPGA)
- Functional Processor (MCU) with the Profibus Processor (TIVA)
- Functional Processor (MCU) with the Diagnostic Channel (FPGA)

The first two communication links are protected with the same CRC as prescribed for SL4 profibus communication. The third according to the CRC for SL2 profibus communication. As the HW and EMI failure rates on these (internal links) is much lower than at the external profibus, the resulting remaining risk will be lower.
In addition single (transient) faults in the system will not lead to a hazardous state. Therefore only multiple undetected unsafe communication faults will lead to a hazardous situation.
Faults in the communication with the diagnostic channel will lead to an availability problem.
Conclusion: the risk resulting from internal communication is many orders of magnitude lower than the risk resulting from the prescribed external communication.

Linked Work Items	has parent: STMA-27925 - Communication between processors , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

6.4.3 Communication with the netX51

Apportionment, STMA-29020 - Communication with the netX51 is included in the (black) profibus channel. Therefore communication is protected with the prescribed safety measures described in 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).

Linked Work Items	has parent: STMA-27952 - Communication with the netX51 , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

6.4.4 Communication with the DA converters

Apportionment, STMA-29021 - Faults in the communication with the DA converters could lead to injection of ATBEG like 75 Hz signals (although it would require a very specific fault which seems to be incredible if the complexity of the signal is taken into account).

To avoid the detection of a valid code from a signal which is generated by the DA converters, the resulting signal is also added to the configuration signal (a DC signal).
The configuration signal will be checked for the absence of 75 Hz signals and the presence of the injected test signals. If 75 Hz is found in the configuration signal then the input block (FPGA plus DA and AD converters) will be reset.

Linked Work Items	has parent: STMA-27920 - Communication with the DA converters , apportions: STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance... , apportions: STMA-27500 - A suitable method, for example Fault Tree Analysis (FTA), shall be used to demon...

6.4.5 Communication with the AD converters

Apportionment, STMA-29022 - If both links between the AD converters and the IO Channels are corrupted at the same time while the following conditions are fulfilled:

- The faults both lead to 75 Hz in the input signals.
- The 75 Hz signal in both channels has the same phase.
- Both fault are intermittent with the same ATBEG frequency.
- The intermittent faults are synchronized (occur and disappear at the same time).
- The faults do not influence the test signals (e.g. while the faults have a frequency of 75 Hz and are only adding, or distracting; multiplication (e.g. an interruption is a multiplication with "0") would lead to influencing the other frequencies).

then this double fault could be hazardous.

Although the number of conditions is such that the fault can be considered to be "incredible", an AD converter has been selected which is equipped with CRC protected communication. This measure eliminates the described risk.

Linked Work Items	has parent: STMA-27921 - Communication with the AD converters , apportions: STMA-27499 - A multiple fault (for example, a double or triple fault) which could be hazardou...

7 Defense against systematic faults

Text, STMA-38958 - Proof concerning processes used to avoid systematic faults is given in S9.4.2 Part 4: Technical Safety Report Section 2 Assurance of correct operation. In this chapter, measures are described which further limit the effect of systematic faults:

Apportionment, STMA-27508 - Monitoring input circuits and IO Channels
The monitoring of the input circuits and IO Channels using injected test signals is also effective against a number of systematic faults in the concerning parts of the system. Fault types covered are faults leading to (repetitive) corruption of the signal. Faults in the 75 Hz filter will not be covered.

Linked Work Items	has parent: STMA-27490 - Defense against systematic faults , apportions: STMA-27504 - In addition, the system/sub-system design hall be arranged to minimise potential...

Apportionment, STMA-27512 - Defensive programming, the measures below are not complete, a complete overview is given in Q2.10.1 Workinstruction for software design and development
Range testing (intern, extern):

- Intern: if variables calculated by the STM ATB are outside a feasible range the system will go into a safe state.
- Extern: if received variables are outside a feasible range the system will not use the value and take measures to ensure safety.

Check on initialization: At every usage of a software module, it is checked if the module was initialized, then the system will go into a safe state (disconnect the Profibus) and the system will be reset.
Test on stack overflow: (non mask-able interrupt): If the stack space is insufficient, then the system will go into a safe state (disconnect the Profibus) and the system will be reset.

Linked Work Items	has parent: STMA-27490 - Defense against systematic faults ,

	apportions: STMA-27504 - In addition, the system/sub-system design hall be arranged to minimise potential...