S.9.4.2 Part 4: Technical Safety Report Section 2 Assurance of correct operation

Assurance of correct functional operation

Colophon	
Document ID	S9.4.2
Version	3.0
Revision	789115
Author	AVO
Reviewed	789115 ,STMA-82353
Approved	789115 ,STMA-82402
Archive	SID-2158
Date:	2023/05/08 13:16

Authorization

Compiled by: Jw Signature/E-sign: 789115 ,STMA-82271	Date: 2023/05/08 14:34
Reviewed by: HRi Signature/E-sign: 789115 ,STMA-82353	Date: 2023/05/09 07:51
Approved by: BvB Signature/E-sign: 789115 ,STMA-82402	Date: 2023/05/09 09:39

CONTENT

1 Preface

Apportionment, STMA-27996 -

Content of section 2 of the technical safety report

This section contains evidence to demonstrate correct operation of the system/sub- system/equipment under fault-free normal conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements. The following aspects are included:

1. System architecture description (see B.2.1 and Table E.4);
2. Definition of interfaces (see B.2.2);
3. Fulfilment of System Requirements Specification (see B.2.3);
4. Fulfilment of Safety Requirements Specification (see B.2.4);
5. Assurance of correct hardware functionality (see B.2.5);
6. Assurance of correct software functionality (see B.2.6).

Apportionment items in this document are linked to the requirements in NEN-EN50129:2003/C1:2010 which they concern.

Linked Work Items	has parent: STMA-27540 - Preface , apportions: STMA-27997 - EN50129:2003/C1:2010 - section 5.4 - evidence of functional and technical safety

2 System architecture description

Apportionment, STMA-27570 - The STM ATB architecture is described in D5.0 SAS for STM ATB.

Linked Work Items	has parent: STMA-25935 - System architecture description , apportions: STMA-27571 - EN50129:2003/C1:2010 - section B.2.1 - System architecture description

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)

STMA-42332 - Below references of the used safety architecture as described in NEN-EN50129:2003/C1:2010 are made for each part of the STM ATB (implicit, reactive and/or composite).

2.1 Input circuits and IO Channels

STMA-42333 - In this paragraph it is described how fail safety is achieved for the "input circuits" and the "IO Channels".

2.1.1 Brake operation by the driver (CAT3 function)

STMA-42331 - The architecture used for determining if the driver has operated the brakes, is less critical compared to other inputs as the fault is visible to the driver and it doesn't affect the cab signal aspects which are displayed, "only" the EB command is affected (CAT3 hazard, i.e. SIL1 requirements apply).
Brake operation can be determined based one input signal or a combination of input signals out of three inputs:

- An analogue input.
- A digital input giving the brake handle position.
- A digital input giving information concerning the requested brake power.

All three signals are read redundantly with a check in the Functional Processor (composite fail-safety).

Apportionment, STMA-27440 - Composite fail-safety (STMA-27389) concerning the digital inputs:

- Two separate input circuits to condition the digital input signals are used (antivalent).
- Two separate IO Channels are used to pass the conditioned information to the Functional Processor.
- The Functional Processor compares the information received via the two input circuits.
- In case the information from two functionally identical inputs are conflicting the information from the specific input will be interpreted as "brakes not operated by the driver" (safe state concerning this information).
- In case the information from two functionally identical inputs are conflicting longer than a predefined time, the input will be ignored up to switching off the system.

Linked Work Items	has parent: STMA-27536 - Brake operation by the driver (CAT3 function) , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Apportionment, STMA-27441 - Composite fail-safety (STMA-27389) concerning the analogue inputs:

- Two separate analogue input circuits to condition the analogue input signal and to digitize it (AD conversion).
- Two separate IO Channels are used to execute a range check, to down-sample the digitized signal and to pass the information to the Functional Processor.
- The Functional Processor compares the information received via the two input circuits, and checks if the signals are within a feasible range.
- In case one of the signals is out of range or the difference between the signals exceeds a predefined limit, the input will be interpreted as "brakes not operated by the driver" (safe state).
- In case the difference between the signals exceeds a predefined limit too long or one of the signals is outside the feasible range, the input will be ignored up to switching off the system.

Linked Work Items	has parent: STMA-27536 - Brake operation by the driver (CAT3 function) , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Definition, STMA-73236 - Safe state concerning "brake handle applied" inputs:
The information from a specific input is not used, this means that it can no longer provide the information that the brake is operated by the driver. This will lead to interventions in any case the target speed for the next signal is overpassed too long.

2.1.2 Coil signals (CAT1)

STMA-42334 - The coil signals (EM field due to current in the rails + disturbances in the environment) contain an eventual ATBEG code. A valid code is present in the left and right coil signal with an opposite phase at the carrier frequency.

Apportionment, STMA-27392 - Inherent fail-safety (STMA-27390) concerning the coil signals:
Disturbances in one of the coil signals shall not be recognized by the ATBEG decoder as a valid code (STMA-2265). Therefore a disturbance (fault) in one of the input channels or IO Channels cannot generate a signal which is interpreted by the ATBEG decoder as a valid code. Further a disturbance significant enough to simulate a code in one channel, is also significant enough to corrupt a valid code present in the track signal. Therefore such a fault will cause multiple disturbances hindering operation. In such cases the driver will switch off the ATBEG function in order to be able to continue train operation, and the train shall be taken out of service (D6.5.2 Technical documentation).

Linked Work Items	has parent: STMA-27537 - Coil signals (CAT1) , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Apportionment, STMA-27399 - Reactive fail-safety (STMA-27391) concerning the coil signals:
Test signals are added to the coil signals to detect faults in a single channel (IO circuit or IO channel). The tests are described in STMA-16390.
In case the test signals are corrupted, no code in the track signal will be accepted, which leads to a safe state (see D5.2.11 SwRS for Event Handler). The detection time for defects is set to 0.8 s (STMA-11882, STMA-12370 and STMA-6865) which is shorter than the shortest time necessary to detect a valid code (STMA-4754).

Linked Work Items	has parent: STMA-27537 - Coil signals (CAT1) , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Apportionment, STMA-29047 - Composite fail-safety concerning the coil signals:
Immediately after digitizing the coil signals the two coil signals are summed and communicated to the other IO Channel. There the other signal is down sampled and passed to the Functional Processor (MCU, RM48x). In the Functional Processor the 75 Hz component in the signal is calculated and compared to the sum of the 75 Hz values as calculated in the other IO Channel.

Linked Work Items	has parent: STMA-27537 - Coil signals (CAT1) , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

2.2 Functional Processor (relevant for CAT1 functions)

STMA-42342 - In this paragraph it is described how fail safety is achieved for the "Functional Processor".
To comply with the safety requirements an RM48x lock step processor (RM48L952) supplied by "Texas Instruments" (TI) has been used. This processor has been tested for the use in applications up to SIL3 according to IEC61508-1 and IEC61508-2 (TUV SUED, certificate No. Z10 16 01 84071 009).
The RM48x is a "System on Chip" (SoC) which includes a lock-step processor and protected memory.
According to the test results accompanying the above mentioned certificate, the use of the MCU (RM48x), shall be in compliance with the safety relevant parts of the user documentation. The following list describes the main conditions and restrictions of use:

- The guidelines and requirements specified in the user documentation shall be followed. Especially the requirements of the system integration section of the safety manual have to be regarded.
  Evidence for compliance with those requirements is provided via the import in D5.1.5.1 SAP Board design items.
- The impact on the overall safety concept and the safety function has been analysed if a safety mechanism described in the Safety Manual is not used.
  Evidence for compliance with this requirement is provided in the FME(D)A (see D6.2.12 SDD Functional Processor

Hardware Monitor and D6.9.3 FMEDA Hercules and Companion Chip)

- All safety mechanisms implemented by the system integrator have to be developed and verified according to the targeted safety standards (i.e. EN50126, EN50128, EN50129).
- All specific required characteristics and behavior of the Safety MCU required by the final safety function have to be developed and verified according to the targeted safety standards (i.e. EN50126, EN50128, EN50129). This includes also timing aspects like reaction times, test intervals or test execution times.
- The system integrator has to make sure that the conditions and restrictions defined in the documentation of the Safety MCU are understood and followed. (see D6.2.12 SDD Functional Processor Hardware Monitor)

The concerning requirements are taken into account and compliance is shown as described in chapter STMA-27554 - Fulfillment of System Requirements Specification.

Below a description of the safety architectures used in the Functional Processor are described.

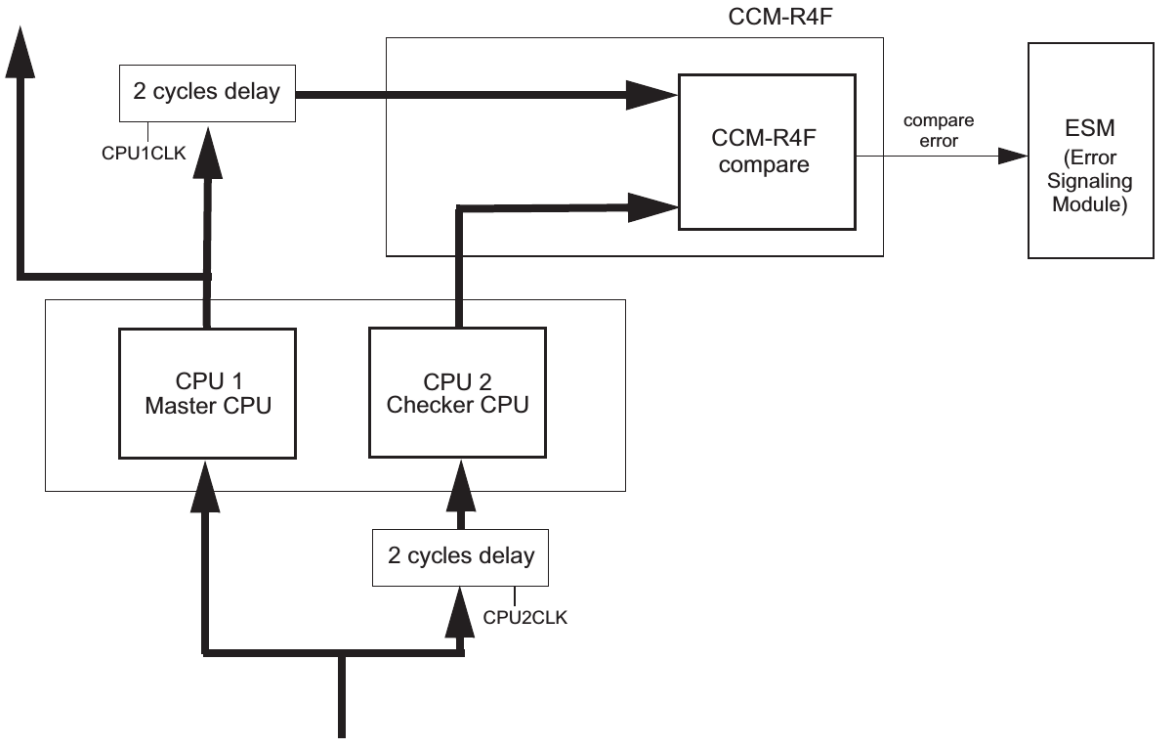
2.2.1 Calculations

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 -



2.2.2 Data storage

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 -

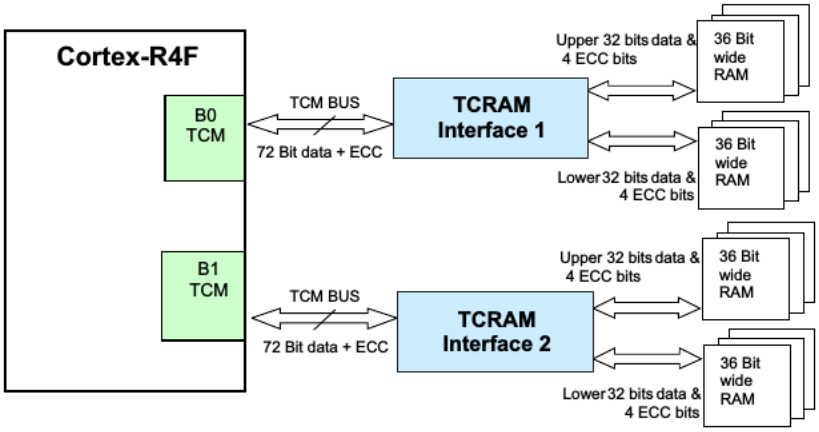


Figure 6-10. TCRAM Block Diagram

(document rm48l952, page 85)

2.3 Profibus Coupler

STMA-27525 - Reactive fail safety is pre-scribed by ERA concerning communication between the ETCS on-board and STM's (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))

Apportionment, STMA-27524 - Reactive fail safety concerning the communication between the ETCS on-board and the STM ATB.
Mechanisms are implemented to detect transmission times which are out of specification and to detect bit-errors during communication. Concerning the latter different safety levels are defined, the size of the CRC and therefore the resulting risk on undetected communication faults differs. A sufficient minimum safety level has been defined for each connection based on the tolerable fault rates (concerning communication).

Linked Work Items	has parent: STMA-27542 - Profibus Coupler , apportions: STMA-73482 - EN50129:2003/C1:2010 - Table E4 (informative)

Definition, STMA-29051 - Figure: (IEC61508-2 figure 7b)

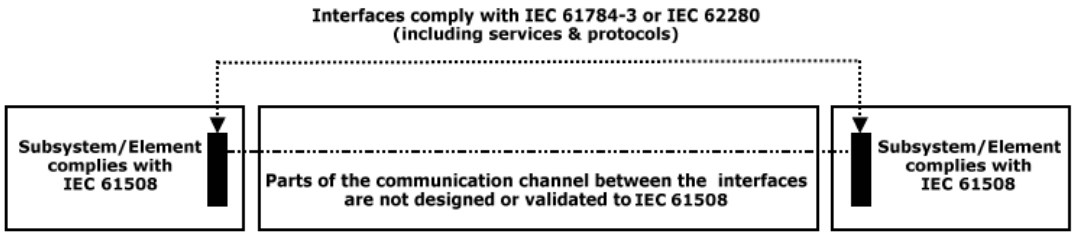


Figure 7 (b) Black channel

3 Definition of interfaces

3.1 Man machine interfaces

Apportionment, STMA-27559 - Requirements concerning installation, maintenance and operation are gathered in D6.5.2 Technical documentation. Those requirements (exported constraints to installation, maintenance and operation) are elaborated in the concerning manuals (9. Manuals).

- The installation manual describes the requirements to be taken into account at installation, e.g.:
  - Mechanical aspects
  - Environmental aspects (temperature etc.)
  - Coil (antenna) type dependent configuration in the train-borne installation.
- The STM ATB is foreseen to be maintenance free. Only in case of defects, maintenance (exchanging the system) is required. The state of the STM ATB will be indicated at the front by 4 bi-color LEDs. The meaning of the LEDs and the necessity to exchange the system is described in the maintenance manual.
- The interaction with the driver is fully specified in the RIS (D3.1 Requirements from Regeling Indienststelling Spoorvoertuigen).

Linked Work Items	has parent: STMA-27558 - Man machine interfaces , apportions: STMA-27555 - EN50129:2003/C1:2010 - section B.2.2.1 Man-machine interfaces - Maintenance , apportions: STMA-27556 - EN50129:2003/C1:2010 - section B.2.2.1 Man-machine interfaces - Operator , apportions: STMA-27557 - EN50129:2003/C1:2010 - section B.2.2.1 Man-machine interfaces - configuration

3.2 External interfaces

Apportionment, STMA-27563 - Interfaces external to the STM ATB are defined in D4.1 Interface Requirements Specification (IRS)

Linked Work Items	has parent: STMA-27562 - External interfaces , apportions: STMA-27561 - EN50129:2003/C1:2010 - section B2.2.2 - system interfaces - external

3.2.1 Communication ETCS <-> STM ATB via Profibus

STMA-42345 - Communication between the STM ATB and the ETCS on-board is implemented according to the relevant ERA specifications including safety measures (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)).are reference to the

3.3 Internal interfaces

Apportionment, STMA-27565 - Internal hardware interfaces are defined in D5.1 HwAS for STM ATB

Linked Work Items	has parent: STMA-27564 - Internal interfaces , apportions: STMA-27560 - EN50129:2003/C1:2010 - section B.2.2.2 System interfaces - internal

Apportionment, STMA-27566 - Internal software interfaces are defined in D5.2 SwAS for STM ATB

Linked Work Items	has parent: STMA-27564 - Internal interfaces , apportions: STMA-27560 - EN50129:2003/C1:2010 - section B.2.2.2 System interfaces - internal

STMA-73237 - Requirements concerning internal interfaces are gathered in D5.3.x documents.

3.3.1 Communication between processors

STMA-42346 - The following connections are implemented between the on-board "processors":

- Functional processor <-> IO Channels: an SPI connection.
- Functional processor <-> Diagnostic Channel: serial link (UART).
- Functional processor <-> Profibus Processor: SPI connection.

To ensure safe and reliable communication between the processors a protocol including a resent mechanism and CRC protection has been implemented.

3.3.2 Communication with the netX51

STMA-42344 - The SPI connection between the Profibus Processor and the netX51 is build according to the requirements provided by the supplier of the netX51 (Hilscher), and is not safety critical as the communication is part of the "black channel" interface with the ETCS functions.

3.3.3 Communication with the DA converters

STMA-42397 - Faults in the communication with the DA converters are detected using a "read-back" of the injected signal via the "configuration signal" (superimposed on the DC signal).

3.3.4 Communication with the AD converters

STMA-42398 - Single faults in the communication between the AD converters and the FPGA will not lead to an unsafe state as for simulating code both coil signals have to be corrupted. To detect multiple (possibly common cause) faults, the communication between the AD converters and the FPGA is protected using CRC coding according to the application conditions of the AD converter.

4 Fulfillment of System Requirements Specification

STMA-73203 - The system requirements are derived from legislation and standards applicable for ATBEG systems. As the scope of the STM ATB development is only a part of those requirements (others apply, e.g., to the ETCS on-board system), the STM ATB requirements are mainly requirements derived from those input documents.

STMA-73202 - The system requirements are gathered in the following documents:

- Functional requirements: D4.3 System Requirements Specification (SRS)
- Interface requirements: D4.1 Interface Requirements Specification (IRS) (this document partially applies to the installation).
- Functionality concerning the interface to the ETCS on-board system: D4.7.4 Specific Transmission Module (SS035 v3.2.0), D4.7.3 STM FFFIS Application Layer (SS058 v3.2.0), D4.7.2 STM FFFIS Safe Time Layer (SS056 v3.0.0),

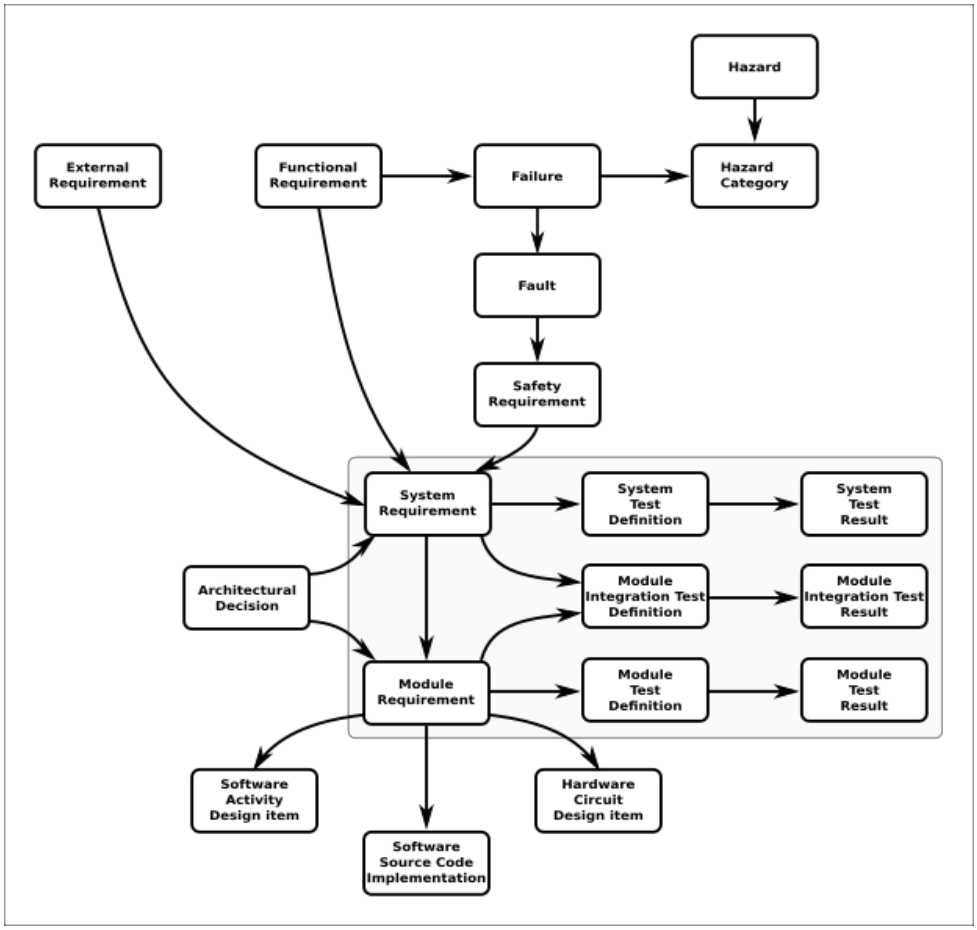
D4.7.1 STM FFFIS Safe Link Layer (SS057 v3.1.0) and D4.7.5 Performance requirements (SS059 v3.1.0).

- Environmental requirements: D4.5 Environmental Requirement Specification (ERS).

Apportionment, STMA-73205 - All requirements, system requirements and derived requirements, are managed in a database structure. The chosen tool "Polarion" supports the definition of multiple kinds of "work items". Each type has its own role in the dossier, e.g. defining a requirement, a test, a verification item etc. Work items can be linked. The links are stored in the data base an can automatically give an overview if all system requirements are covered by lower layer requirements, if al requirements are verified and tested, if all links are verified etc.
The system requirements are refined to (hardware and software) modules defined in the system, hardware and software architecture. Those requirements, contained in the D5.x documents, are linked using links of the type "refines" to the system requirements.
An overview of the linking of system requirements is given in figure STMA-45815 - Figure: Polarion data model for STM ATB.

Linked Work Items	has parent: STMA-27554 - Fulfillment of System Requirements Specification , apportions: STMA-27579 - EN50129:2003:/C1:2010 - section B.2.3 - Fullfilment of system requirements speci...

STMA-45815 - Figure: Polarion data model for STM ATB



STMA-73206 - R1.0 Verification Plan contains a detailed description of how fulfillment of the specifications is proven.
The resulting proof is contained in the Verification Reports and checked at the gate review of each phase.

4.1 Deviations

Apportionment, STMA-75097 - Initially an EB-feedback signal to inform the STM that the EB has been commanded by the ETCS on-board system has been foreseen (STMA-2206). With this feedback the loss of an EB command message at the Profibus had to be mitigated, if the EB command was not confirmed the EB command would be resent.
This function is replaced by unconditional resending of the EB command as long as the EB conditions are fulfilled (STMA-10599).

Linked Work Items	has parent: STMA-75096 - Deviations , apportions: STMA-2206 - In case of an ATBEG or ATBVv intervention the STM ATB shall resend an EB command...

5 Fulfillment of Safety Requirements Specification

STMA-74078 - The tolerable failure rates concerning functional behavior are derived, based on a risk analysis, in *STMATB/2_ System definition and operational context/D2_2 Current RAMS performance and RAMS targets*. The results are summarized in STMA-34960.

STMA-34960 - RAMS requirements are summarized as:
Reliability/availability: < 1.7*10^-4 failures / operational hour for failures during operation.
Improvements decided on business case basis.
Maintenance:
Required maintenance effort shall be justified, target is

- no preventive maintenance,
- no configuration at installation
- defects shall be indicated at the front of the system
- corrective maintenance limited to exchanging the complete unit.
- Small (< 5 dm3) and light (<5 kg) unit, exchangeable by one person

Safety:

- CAT1: failures leading to not braking and wrong DMI indication: < 2*10^-8/operational hour
- CAT2: idem, during a time <3 s: <2*10^-6/operational hour
- CAT3: failures leading to not braking while DMI indications are correct: < 7*10^-6/operational hour
- CAT4: idem, during a time <3 s, or ATBVv failure leading to not braking: <6.6*10^-4/hour
- CAT5: unsafe speed indication at the DMI >3 s, while speed monitoring is working correctly: <2*10^-5/hour.

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

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

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

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

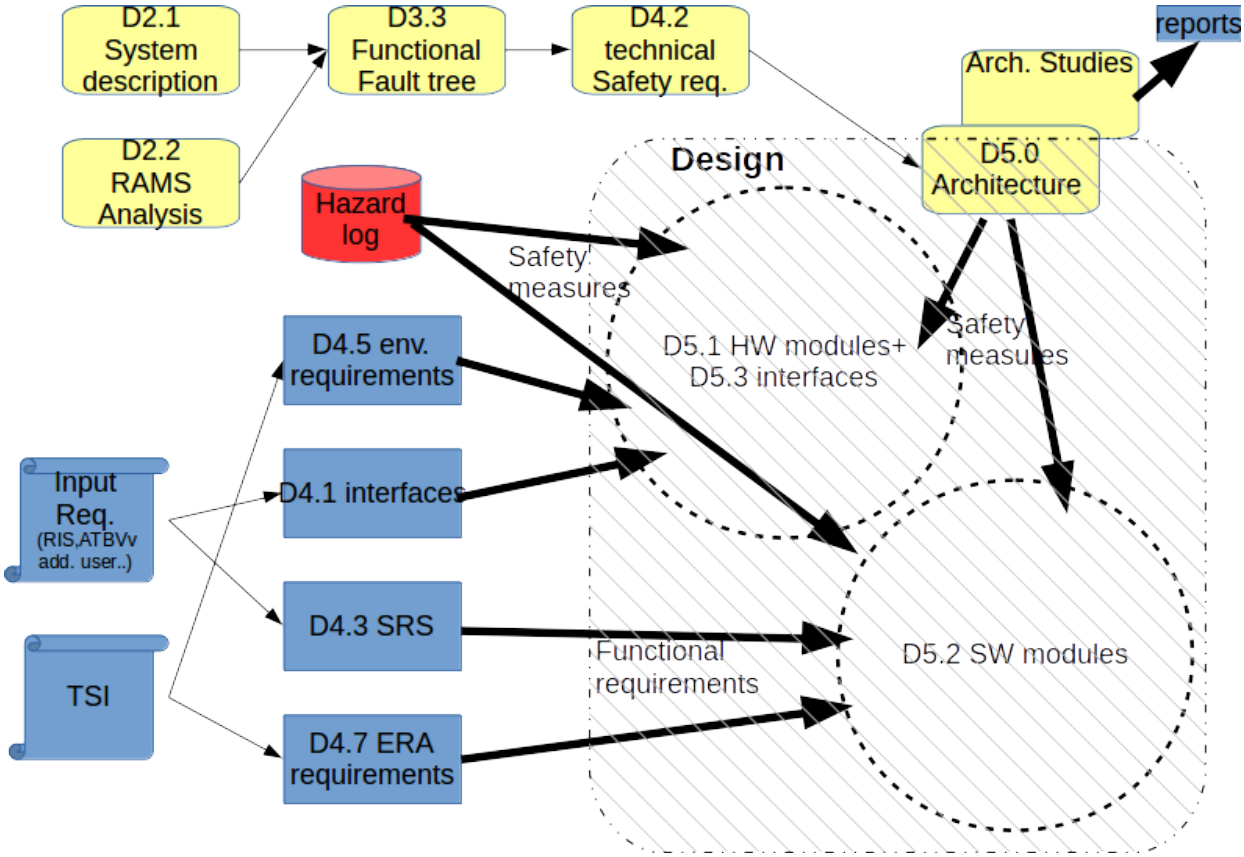
Definition, STMA-10874 - CAT5: the supervised speed indication to the driver also gives a too high speed for more than 3s, but

the correct speed is guarded.

Apportionment, STMA-73214 - Using an FTA analysis (D3.3 Tolerable Functional Fault Rates) the acceptable functional failure rates are assigned to more detailed functional failures (D4.2 Safety requirements) and further to acceptable technical fault rates (D5.0 SAS for STM ATB), functional requirements and an architecture which together should lead to meeting the safety targets. (see figure STMA-30040).

Linked Work Items	has parent: STMA-27551 - Fulfillment of Safety Requirements Specification , apportions: STMA-27985 - EN50129:2003/C1:2010 - section 5.3.6. safety requirements specification , apportions: STMA-27986 - EN50129:2003/C1:2010 - section 5.3.7 System/subsystem/equipment design , apportions: STMA-73484 - EN50129 - Table E.2 - System requirements specification (referred to in 5.3.6)

Definition, STMA-30040 - Main steps in the design process



Apportionment, STMA-73215 - In D6.9.5 Apportionment safety requirements it is explained that/how the "safety requirements" defined in D4.2 Safety requirements are met. Functional requirements added to enhance safety as defined in D5.0 SAS for STM ATB are handled equal to other functional requirements as described in chapter STMA-27554 - Fulfillment of System Requirements Specification.

Linked Work Items	has parent: STMA-27551 - Fulfillment of Safety Requirements Specification , apportions: STMA-27985 - EN50129:2003/C1:2010 - section 5.3.6. safety requirements specification , apportions: STMA-73484 - EN50129 - Table E.2 - System requirements specification (referred to in 5.3.6)

Apportionment, STMA-73494 - In D5.0 SAS for STM ATB the architecture is determined and (also graphically, E.2.2) presented in logical blocks, assigning the safety functions to the Functional Processor (E.2.1). Interfaces between the blocks are further specified in D5.2 SwAS for STM ATB. Specifications are assigned based on the architecture to the different blocks (E.2.3), and traced using the Polarion database to the input requirements and the hazard log (E.2.7) (upwards), and the design

and implementation (downwards) (E.2.4 and E.2.5). Special verification documents are build using Polarion items to log the verification of all linking (check lists, E.2.6), and the database tooling allows automated checking of the linking and its verification.
For verification of the correctness of the requirements further verification documents are build using Polarion (E.2.8).
(note: E.2.x is used as reference to EN50129 STMA-73484 - EN50129 - Table E.2 - System requirements specification (referred to in 5.3.6)

Linked Work Items	has parent: STMA-27551 - Fulfillment of Safety Requirements Specification , apportions: STMA-73484 - EN50129 - Table E.2 - System requirements specification (referred to in 5.3.6)

Apportionment, STMA-74565 - In addition to the safety requirements derived with the RAMS analysis and fault tree analysis, also RAMS requirements are imported from the RIS. Those requirements are translated into STMA-2258, STMA-2259 and STMA-2260. As those requirements do not impose more servere requirements than resulting from D3.3 Tolerable Functional Fault Rates no further refinement of those requirements was necessary.

Linked Work Items	has parent: STMA-27551 - Fulfillment of Safety Requirements Specification , apportions: STMA-2258 - The STM ATB failure rate concerning failures causing an unsafe situation for max... , apportions: STMA-2259 - The STM ATB failure rate concerning failures causing an unsafe situation longer... , apportions: STMA-2260 - The STM ATB failure rate concerning failures leading to unsafe false information...

6 Assurance of correct hardware functionality

Apportionment, STMA-73216 - The hardware functionality is specified in the D5.1.x documents. Those contain the module specifications (requirements) which are linked to the designs as shown in figure STMA-45815 - Figure: Polarion data model for STM ATB. Using Polarion the work items of the type "hardware design" are linked to the concerning requirements, and the "hardware designs" as well as the links are verified to guarantee that all requirements are correctly implemented.
Hardware requirements concerning the SAP Board are provided to Neways Technologies (sub-contractor) who imported the requirements into their own Polarion database.
A cross reference between the projects requirements ("STMA-xxxx") and the Neways requirements is included in D6.1.5 HDD SAP Board.

Linked Work Items	has parent: STMA-27552 - Assurance of correct hardware functionality , apportions: STMA-27578 - EN50129:2003/C1:2010 - section B.2.6 - Assurance of correct software functionali...

7 Assurance of correct software functionality

Apportionment, STMA-73235 - The software functionality is specified in the D5.2.x and D5.3.x documents. Those contain the module specifications (requirements) which are linked to the designs and source code as shown in figure STMA-45815 - Figure: Polarion data model for STM ATB. All requirements are linked to a software design work item ("activity") and to the related source code. The links have been verified to be complete and correct, which assures the requirements are implemented in the source code.

Linked Work Items	has parent: STMA-27550 - Assurance of correct software functionality , apportions: STMA-27576 - EN50129:2003/C1:2010 - section B.2.6 - Assurance of correct software functionali...