S9.4.3.1 Annex EN5012x vs IEC61508

for the development of an STM ATB

Colophon	
Document ID	S9.4.3.1
Version	2.0
Revision	787346
Author	AVO
Reviewed	787346 ,STMA-82355
Approved	787346 ,STMA-82381
Archive	
Date:	2023/04/28 11:33

Authorization

Compiled by: JW Signature/E-sign: 787346 ,STMA-82273	Date: 2023/05/08 14:37
Reviewed by: HRi Signature/E-sign: 787346 ,STMA-82355	Date: 2023/05/09 07:54
Approved by: BvB Signature/E-sign: 787346 ,STMA-82381	Date: 2023/05/09 09:28

CONTENT

1 Preface

, STMA-72478 - The EN50129:2003 refers to the IEC61508-1 as a mandatory reference, where IEC61508-1 is referring to the IEC61508-2, however the standards are not completely compatible.
To investigate the issues when using components certified against the IEC61508-2 a comparison between requirements in EN50129:2003 and requirements in IEC61508-2 has been performed.

2 Deriving the safety integrity level

, STMA-72479 - EN50129: A5.1: a supplier may start development of generic products in a bottom-up fashion and may even achieve safety approval for a generic product safety case (without the results of any risk analysis being available), but in the end he shall ensure that the required tolerable hazard rates (application safety case) are fulfilled. The railway authority and/or the safety authority shall determine the base line for this process. ... During the next phases, the system requirements and apportionment of system requirements phases, the tolerable hazard rates are apportioned to system functions and sub-systems, respectively. Each of these functions shall have a qualitative safety target and a quantitative target attached to them. The qualitative target shall be in the form of a Safety Integrity Level, and shall cover systematic failure integrity. The quantitative target shall be in the form of a numerical failure rate, and shall cover random failure integrity.

, STMA-72481 - EN50129 differences compared to IEC61508:
NOTE In contrast to other standards the SIL table in this standard has only one column for frequencies (formerly called high
demand or continuous mode) and does not have a column for failure probabilities on demand (formerly called demand mode). The
reasons to restrict to one mode are
- less ambiguity in determination of SIL,
- all demand mode systems can be modelled as continuous mode systems,
- continuous control and command signalling systems are clearly the majority in modern railway signalling applications.
The SIL table has been constructed taking into account EN 61508-1.
The last bullit of the above text shows that the standard is primarily written for way-side signalling. On board signalling systems are mostly monitoring systems thus for a large part working on demand (a driver failure).
The allocation according to IEC61508 has to take into account both type of systems: "continuous"

and "on demand", therefore a hardware designed according to IEC61508 standards has to comply with requirements for both system types, thus is usable for systems which have to comply with EN50129.

3 Allocation of safety requirements

T, STMA-72482 - EN50129:2003:

Definition, STMA-27594 - Safety functional requirements are the actual safety-related functions which the system, sub-system or equipment is required to carry out.

Definition, STMA-27591 - Safety integrity requirements define the level of safety integrity required for each safety-related function.

Definition, STMA-27590 -

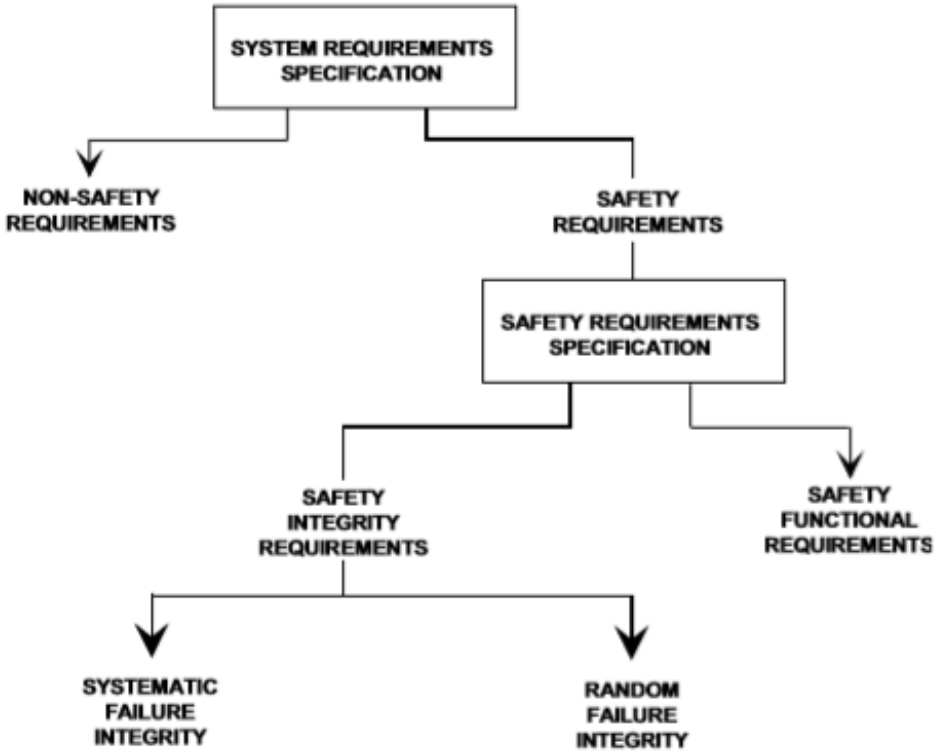


Figure A.1 – Safety requirements and safety integrity

T, STMA-72483 - IEC61508-2: Assigning the SIL level to sub systems

Elements are combined to give a maximum hardware safety integrity level for the safety function under

consideration, for subsystem X as follows:

a) Combining elements 1 and 2: The hardware fault tolerance and safe failure fraction achieved by the

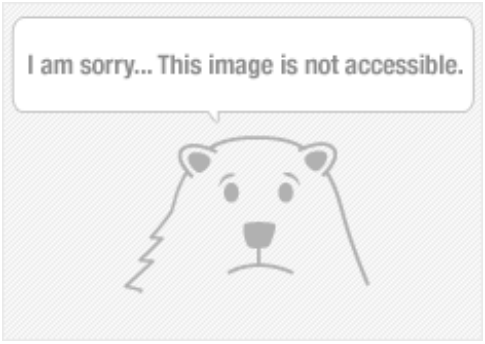
combination of elements 1 and 2 (each separately meeting the requirements for SIL 3 and SIL 2 respectively)
meets the requirements of SIL 2 (determined by element 2; see 7.4.4.2.3);
b) Combining elements 3 and 4: The hardware fault tolerance and safe failure fraction achieved by the
combination of elements 3 and 4 (each separately meeting the requirements for SIL 2 and SIL 1 respectively)
meets the requirements of SIL 1 (determined by element 4 see 7.4.4.2.3);
c) Further combining the combination of elements 1 and 2 with the combination of elements 3 and 4: the maximum safety integrity level that can be claimed for the safety function under consideration is determined by selecting the channel with the highest safety integrity level that has been achieved and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of elements. In this case the subsystem comprises two parallel channels with a hardware fault tolerance of 1. The channel with the highest safety integrity level, for the safety function under consideration was that comprising elements 1 and 2 which achieved the requirements for SIL 2. Therefore, the maximum safety integrity level for the subsystem for a hardware fault tolerance of 1 is (SIL 2 + 1) = SIL 3 (see 7.4.4.2.4).

T, STMA-72485 - The procedure of assigning safety requirements to subsystems and their required SIL is more precise described in the IEC61508-2. In praxis: two parallel SIL0 systems can, according to EN50129, form a SIL4 system provided that the SIL0 systems are independent. Based on IEC61508-2 the two subsystems shall at least have SIL3.

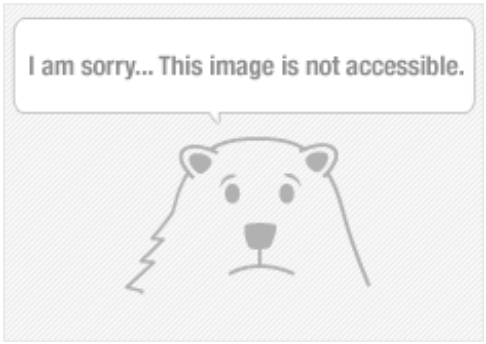
4 Life cycle

T, STMA-72509 - This comparison between EN50129 and IEC61508 concerns the aspects relevant for "programmable electronic devices". Therefore the phases concerning the application (deriving safety targets, customer requirements,..) are not taken into account. The comparison starts at compiling the requirements

Definition, STMA-72511 - Figure: RAMS management phases according to IEC61508-1:2010 paragraph 7.1.1.5.



Definition, STMA-72512 - Figure: RAMS management phases according to EN50126-1:2017 paragraph 6.2



, STMA-72522 - In the above figures STMA-72511 and STMA-72512 the phases are defined. Apart from the extra phases 6, 7, 8 and 11 in IEC61508-1 which are integrated in other phases in EN50126-1 the definition of the phases corresponds to eachother. A more detailed description of the phases is given in IEC61508-1:table 1 paragraph 7.1.2.2 and EN50126-1 table 1 paragraph 6.2.

5 Architectural requirements

, STMA-27523 - To reach SIL3 or SIL4 one of the following techniques is "highly recommended" (according to EN50129, table E.4):

- Dual electronic structure based on composite fail-safety with fail safe comparison
- Single electronic structure based on inherent fail safety
- Single electronic structure based on reactive fail safety
- Diverse electronic structure with fail-safe comparison

The RM48x choice corresponds to "Single electronic structure based on reactive fail safety". IEC61508-2 (7.4.4), choices made for the RM48x (see safety manual RM48x, SPNU577D):

- route 1H,
- SFF > 99%,

- HFT = 0,
- Type B

The RM48x is certified against SIL3 requirements with HFT=0. This corresponds with a "Single electronic structure based on reactive fail safety" as defined in the EN50129:2003. Therefore requirements concerning components characterized with [route 1H, SFF >99%, HFT=0, Type B] shall be compared to requirements as formulated concerning SIL3/4 in EN50129:2003.

T, STMA-42178 - - IEC61508-2 (7.4.5), effect of random failures items taken into account (items relevant for the RM48x are listed):

- architecture in terms of sub-systems (not applicable) and elements.
- diagnostic coverage, according to IEC61508-2, annex C (taking into account the "process safety time")
- common cause failures, according to IEC61508-6, annex D
- Test intervals: time needed to mitigate faults/repair times (7.4.5.3, IEC61508-4, 3.6.21/22 and IEC61508-6 annex B)
- Proof if tests are likely to be 100% effective.
- Available method.

5.1 Effect of single faults

T, STMA-42179 - - The approach between EN50129:2003 and IEC61508-2:2010 concerning the effect of single faults is different. The EN50129:2003 approach is qualitative: "assurance (= confidence) that no single random hardware component failure mode is hazardous..." versus the quantitative approach of IEC61508-2:2010. Concerning the RM48x and Artix FPGA as used in the STM ATB, the concept meets both approaches as the RM48x has a 100% coverage on the CPU and memory and in the Artix two functional faults are necessary before a hazardous situation can occur.

5.1.1 EN50129:2003, B3.1:

External Requirement, STMA-27422 -

- Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods. The component failure modes to be considered in the analysis shall be identified using the procedures defined in Annex C. NOTE A top-down failure analysis method should be used, such as Fault Tree Analysis (FTA). This should be supported, if necessary, by a bottom-up method such as Failure Modes and Effects Analysis (FMEA). See also guidance given in Table E.6. Failure analyses shall be qualitative, and quantitative where credible data is available. Random hardware failure rates, or probabilities of component failure, should be based on field data if possible. Apportionment of an overall component failure rate between its failure modes shall be justified in the analysis.
(EN50129:2003/C1:2020 - section B.3.1 effects of single faults)

5.1.2 IEC61508-2:2010, 7.4.5.1:

T, STMA-27749 - 7.4.5.1 For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10).

5.2 Common causes, analysis and independence

T, STMA-27750 - - According to both, EN50129:2003 and IEC61508-2:2010, a single implementation with diagnostic functions to monitor the single channel is an acceptable architecture. Such an architecture requires independence between the implementation of the functions and the implementation of the diagnostics. In this paragraph a comparison is made between requirements in EN50129:2003 and IEC61508-2:2010 concerning common causes, common cause analysis and independence of items.

5.2.1 Relevant requirements in the EN50129

5.2.1.1 B3.2 Independence of items

External Requirement, STMA-27404 - Measures shall be taken to avoid non-intentional physical internal influences. NOTE 2 D.2 contains a range of measures for the achievement of physical internal independence (protection against influences of Type A).

External Requirement, STMA-27405 - Measures shall be taken to avoid functional internal influences. This shall be achieved by means of functional internal independence (protection against influences of Type B). NOTE 3 A functional internal influence would allow faulty information in one item to influence another item in a hazardous manner

External Requirement, STMA-27410 - Measures shall be taken to avoid non-intentional physical external influences. B.4 contains requirements for external influences which shall be considered. NOTE 5 D.3 contains a range of measures for the achievement of physical external independence (protection against influences of Type C).

External Requirement, STMA-27411 - Measures shall be taken to avoid functional external influences. This shall be achieved by means of functional external independence (protection against influences of Type D). NOTE 6 A functional external influence would allow faulty information from an external source to influence the system in a hazardous manner.

5.2.1.2 B3.5 Effect of multiple faults

External Requirement, STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance that a multiple fault could only occur by means of a combination of random single faults, and not as the result of a common cause fault.

5.2.1.3 A.4.2.2 Common cause failure analysis

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.

5.2.2 Relevant requirements in the 61508-2

, STMA-27459 - 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.

NOTE 1 For systematic capability, with respect to hardware design, realisation, operation and maintenance, possible approaches to the achievement of sufficient independence include:

- *functional diversity: use of different approaches to achieve the same results;*
- *diverse technologies: use of different types of equipment to achieve the same results);*
- *common parts/services: ensuring that there are no common parts or services or support systems (for example*
  power supplies) whose failure could result in a dangerous mode of failure of all systems;
- *common procedures: ensuring that there are no common operational, maintenance or test procedures*

NOTE 2 Independence of application means that elements will not adversely interfere with each other's execution behaviour such that a dangerous failure would occur.

, STMA-79794 - Requirements concerning on-chip redundancy are provided in IEC61508-2 annex E.

5.2.3 Conclusion

, STMA-27460 - Multiple requirements in the EN50129:2003 intent to specify independence between multiple items whose simultaneous failure could lead to a hazard:

- Requirements stating that measures shall be taken to avoid functional and technical influences
- A requirement to perform common cause analysis in order to get confidence that common-cause faults will not lead to multiple (hazardous) faults
- It shall be ensured that sufficient independence exists. It's not clear what is meant by "If independence cannot be demonstrated completely", however a common cause analysis has to be performed anyway based on STMA-27497.

A common cause analysis is a means to prove that (sufficient) measures have been taken to avoid functional and technical influences. Therefore the mentioned requirements can be covered

with a common cause analysis which provides confidence that a common cause fault will not lead to multiple faults (which together cause a hazard) and which ensures that sufficient independence exists between parts implementing functions whose combined occurrence could lead to a hazard.
The requirements concerning independence are covered in the IEC61508-2 standard (a.o) by paragraph 7.4.3.4 (STMA-27459). For items which have positively been tested against 61508-2, it may therefore be assumed that independence is justified by a common cause failure analysis which shows 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, therefore "sufficient independence" has been shown.

5.3 Detection of single faults

5.3.1 Detection of single faults, requirements in EN50129:2003

External Requirement, STMA-27413 - 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 (i.e.: negated) in a time sufficiently short to fulfil the specified quantified safety target. Demonstration of this shall be achieved by a combination of Failure Modes and Effects Analysis (FMEA) and quantified assessment of Random Failure Integrity (see A.3).
In the case of Composite fail-safety, this requirement means that a first fault shall be detected, and a safe state enforced, in a time sufficiently short to ensure that the risk of a second fault occurring during the detection-plus-negation time is smaller than the specified probabilistic target.
In the case of Reactive fail-safety, this requirement means that the maximum total time taken for detection-plus-negation shall not exceed the specified limit for the duration of a transient, potentially-hazardous, condition.

, STMA-27666 - Requirement STMA-27413 (EN50129:2003, B3.3) concerning detection of single faults is covered in the IEC61508-2 standard (a.o.) by paragraph 7.4.5.1 and 7.4.8.3. If the safe state is enforced "in a time sufficiently short" is to be determined at application level, however for the generic product a safe state shall be possible in 1 clock cycle (<5ns), i.e. significantly faster than required from the STM ATB application.

, STMA-27674 - 7.4.5.1 For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10).

, STMA-27667 - 7.4.8.3 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case of a subsystem that is implementing any safety function(s) operating in the high demand or the continuous mode, result in a specified action to achieve or maintain a safe state (see Note).

, STMA-27672 - Requirement STMA-27417 (EN50129:2003, B3.3) concerning evidence of complying with STMA-27413 in relation to the mitigation time of detected faults is covered in the IEC61508-2 standard (a.o) by paragraph 7.4.5.3. This paragraph makes explicit that the response time shall be sufficiently short (<process safety time). For a generic product as the RM48x this is three clock cycles (<15ns).
For items which have positively been tested against 61508-2, it may therefore be assumed that sufficient proof has been provided to show that identified faults are mitigated within the permitted time.

, STMA-27673 - 7.4.5.3 When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if:

- the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or
- in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

5.3.2 Detection of single faults, requirements in IEC61508-2:2010

, STMA-27676 - 7.4.5.2 The estimate of the achieved failure measure for each safety function, as required by 7.4.5.1, shall take into account:

- a) the architecture of the E/E/PE safety-related system, in terms of its subsystems, as it relates to each safety function under consideration;
  NOTE 1 This involves deciding which failure modes of the elements of the subsystems are in a series configuration (i.e. any failure causes failure of the relevant safety function to be carried out) and which are in a parallel configuration (i.e. coincident failures are necessary for the relevant safety function to fail).
- b) the architecture of each subsystem of the E/E/PE safety-related system, in terms of its elements, as it relates to each safety function under consideration;
- c) the estimated failure rate of each subsystem and its elements in any modes that would cause a dangerous failure of the E/E/PE safety-related system but are detected by

diagnostic tests (see 7.4.9.4 to 7.4.9.5). Justification for the failure rates should be given considering the source of the data and its accuracy or tolerance. This may include consideration and the comparison of data from a number of sources and the selection of failure rates from systems most closely resembling that under consideration. Failure rates used for quantifying the effect of random hardware failures and calculating safe failure fraction or diagnostic coverage shall take into account the specified operating conditions.
NOTE 2 To take into account the operating conditions it will normally be necessary to adjust failure rates from data bases for example due to contact load or temperature.

- d) the susceptibility of the E/E/PE safety-related system and its subsystems to common cause failures (see Notes 3 and 4). There shall be a justification of the assumptions made;
  NOTE 3 Failures due to common cause effects may result from effects other than actual failures of hardware elements (e.g. electromagnetic interference, decoding errors, etc). However, such failures are considered, for the purposes of this standard, in the quantification of the effect of random hardware failures. Staggering the testing of elements decreases the likelihood of common cause failure. NOTE 4 In the case of common cause failures being identified between the E/E/PE safety–related systems and demand causes or other protection layers there will need to be confirmation that this has been taken into account when the safety integrity level and target failure measure requirements have been determined. For methods of determining common cause factors see IEC 61508-6, Annex D.
- e) the diagnostic coverage of the diagnostic tests (determined according to Annex C), the associated diagnostic test interval and the rate of dangerous unrevealed failure of the diagnostics due to random hardware failures of each subsystem. Where relevant, only those diagnostic tests that meet the requirements of 7.4.5.3 shall be considered. The 12 of 16 5.3.3 Conclusion 5.4 Action following detection 5.4.1 EN50129:2003: MTTR and MRT (see 3.6.21 and 3.6.22 of IEC 61508-4), shall be considered in the reliability model.
  NOTE 5 When establishing the diagnostic test interval, the intervals between all of the tests that contribute to the diagnostic coverage will need to be considered.
- f) the intervals at which proof tests are undertaken to reveal dangerous faults;
- g) whether the proof test is likely to be 100 % effective;
  NOTE 6 An imperfect proof test will result in a safety function that is not restored to 'as good as new' and therefore the probability of failure will increase. Justification should be given for the assumptions made, in particular, the renewable period of the elements or the effect on the risk reduction over the life of the safety function should be included. It will be necessary to consider the test duration if the item is tested off-line whilst testing is being undertaken.
- h) the repair times for detected failures;
  NOTE 7 The mean repair time (MRT) is one part of the mean time to restoration (MTTR), (see 3.6.22 and 3.6.21 of IEC 61508-4), which will also include the time taken to detect a failure and any time period during which repair is not possible (see Annex B of IEC 61508-6, for an example of how the MTTR and the MRT can be used to calculate the probability of failure). The repair can be considered to be instantaneous only when the EUC is shut-down or in a safe state during repair. For situations where the repair cannot be carried out whilst the EUC is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large. All relevant factors relating to repairs should be taken into account.
- i) the effect of random human error if a person is required to take action to achieve the

safety function.

NOTE 8 The random nature of human error should be considered in cases where a person is alerted to an unsafe condition and is required to take action and the probability of human error should be included in the overall calculation.

- j) the fact that a number of modelling methods are available and that the most appropriate method is a matter for the analyst and will depend on the circumstances. Available methods include cause consequence analysis (B.6.6.2 of IEC 61508-7;), fault tree analysis (B.6.6.5 of IEC 61508-7;), Markov models (Annex B of IEC 61508-6 and B.6.6.6 of IEC 61508-7), reliability block diagrams (Annex B of IEC 61508-6 and B.6.6.7 of IEC 61508-7;) and Petri nets (Annex B of IEC 61508-6 and B.2.3.3 of IEC 61508-7).

  NOTE 9 Annex B of IEC 61508-6 describes a simplified approach that may be used to estimate the average probability of a dangerous failure on demand of a safety function due to random hardware failures in order to determine that an architecture meets the required target failure measure. NOTE 10 Clause A.2 of IEC 61508-6 gives an overview of the necessary steps in achieving required hardware safety integrity, and shows how this subclause relates to other requirements of this standard. NOTE 11 It is necessary to quantify separately for each safety function the reliability of the E/E/PE safety-related systems because different element failure modes will apply and the architecture of the E/E/PE safety-related systems (in terms of redundancy) may also vary.

5.3.3 Conclusion

, STMA-27675 - Requirement STMA-27417 (EN50129:2003, B3.3) concerning evidence of complying with STMA-27413 in relation to the claimed failure rates is covered in the IEC61508-2 standard (a.o.) by paragraph 7.4.5.2.; STMA-27676 (especially point c.: "justification for the failure rates", d. "common cause failures", f. test intervals, h. repair times.

5.4 Action following detection

5.4.1 EN50129:2003:

External Requirement, STMA-27495 - After detection of a first fault, the system/sub-system/equipment shall enter, or continue in, a safe state. The safe state is generally (but not necessarily) more restrictive. The safe state shall be reached in a time sufficiently short that the combined detection-plus-negation time fulfills the specified safety target.

, STMA-27494 - NOTE The negation time is usually the time taken for the relevant part of the system to be shut down, either automatically or by human action. These requirements are illustrated in Figure B.2 (EN50129:2003).

External Requirement, STMA-27496 - After detection of a first fault, and having entered the safe state, further faults shall not cancel out the safe state. Cancellation of a restrictive safe state shall occur only in a controlled manner, as part of a corrective procedure.

External Requirement, STMA-27493 - The system/sub-system/equipment shall remain in a safe state if further faults occur during permissible delay-times-to-repair after occurrence of a first fault. Permissible delay-times-to-repair shall be sufficiently short to fulfill the specified safety target.

5.4.2 IEC61508-2:

, STMA-27878 - 7.4.5.3 When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if: the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100

, STMA-27888 - 7.4.8.3 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case of a subsystem that is implementing any safety function(s) operating in the high demand or the continuous mode, result in a specified action to achieve or maintain a safe state (see Note).
NOTE The specified action required to achieve or maintain a safe state will be specified in the E/E/PE system safety requirements (see IEC 61508-1, 7.10). It may consist, for example, of the safe shut-down of the EUC, or that part of the EUC that relies, for functional safety, on the faulty subsystem

, STMA-27889 - The approach of EN50129 is qualitative: after a first fault the system shall enter and stay in a safe state (B3.4, STMA-27495, STMA-27496 and STMA-27493).
The approach of IEC61508-2 is partly quantitative: the unsafe failure rate shall be calculated, taking into account the time period in which the system remains active but cannot be repaired (7.4.5.2 point h: STMA-27676 , note 7 and 7.4.5.3: STMA-27878).
However also IEC61508-2 requires to enter a safe state (in case of HFT=0, i.e. a 1oo1D architecture (see 7.4.8.3, STMA-27888).

Conclusion: the requirements concerning "action following detection" as stated in EN50129:2003 are covered by the requirements as state IEC61508-2:2010. In addition IEC61508-2:2010 includes quantitative requirements.

5.5 Effects of multiple faults

5.5.1 EN50129:2003:

External Requirement, STMA-27499 - 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 fulfill the specified safety target.

External Requirement, STMA-27500 - A suitable method, for example Fault Tree Analysis (FTA), shall be used to demonstrate the effects of multiple faults. The techniques used to achieve detection-plus-negation of multiple faults within the permitted time shall be shown, including supporting calculations.

5.5.2 IEC61508-2

, STMA-27880 - 7.4.5.4 The diagnostic test interval of any subsystem:

- having a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or
- which is implementing a safety function, or part of a safety function, operating in low demand mode of operation, shall be such that the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

5.5.3 Conclusion

, STMA-72532 - The first two requirements in B3.5 (STMA-27499 and STMA-27500) are focused at the remaining risk ("in a time sufficiently short to fulfill the specified safety target" and "...within the permitted time"). This is comparable to the approach in IEC61508-2:2010 which states: see STMA-27880 .

, STMA-72533 - The last requirement in B3.5 STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance... is more qualitative. Assurance (confidence) shall be provided that multiple faults (leading to a hazardous state) are not a result of a common cause fault.
Methods compliant with the IEC61508-2 can provide this confidence via a quantitative approach, i.e. by calculating the failure rate and showing that is sufficiently low for the targeted application. In addition a qualitative CCF analysis can also be used to meet STMA-27497 - A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance....

5.6 Requirements concerning components compliant with IEC61508-2

, STMA-72536 - To enable cross acceptance information shall be available concerning the components used. As the TI RM48x is assessed against IEC61508-2 the RM48 complies with the requirements listed below.

, STMA-72537 - 7.4.9.4 The following information shall be available for each safety-related element that is liable to random hardware failure (see also 7.4.9.3 and 7.4.9.5):

(NOTE 1 It will be necessary for a supplier of an element, claimed as being compliant with IEC 61508 series, to make this information available to the designer of a safety-related system in the element safety manual, see Annex D.)

1. a) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are not detected by diagnostic tests internal to the element or are not detectable by diagnostics external to the element (see 7.4.9.5);
2. b) for every failure mode in a), an estimated failure rate with respect to specified operating conditions
3. c) the failure modes of the element (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the safety function and that are detected by diagnostic tests internal to the element or are detectable by diagnostics external to the element (see 7.4.9.5);
4. d) for every failure mode in c), an estimated failure rate with respect to specified operating conditions;
5. e) any limits on the environment of the element that should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;
6. f) any limit on the lifetime of the element that should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;
7. g) any periodic proof test and/or maintenance requirements;
8. h) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic coverage derived according to Annex C (see Note 2);
9. i) for every failure mode in c) that is detected by diagnostics internal to the element, the diagnostic test interval (see Note 2); NOTE 2 The diagnostic coverage and diagnostic test interval is required to allow credit to be claimed for the action of the diagnostic tests performed in the element in the hardware safety integrity model of the E/E/PE safety related system (see 7.4.5.2, 7.4.5.3 and 7.4.5.4).
10. j) the failure rate of the diagnostics, due to random hardware failures;
11. k) any additional information (for example repair times) that is necessary to allow the derivation of the mean repair time (MRT), see 3.6.22 of IEC 61508-4,following detection of a fault by the diagnostics;
12. l) all information that is necessary to enable the derivation of the safe failure fraction (SFF) of the element as applied in the E/E/PE safety-related system, determined according to Annex C, including the classification as type A or type B according to 7.4.4;
13. m) the hardware fault tolerance of the element.

7.4.9.5 The estimated failure rates, due to random hardware failures, for elements (see 7.4.9.4 a) and c)) can be determined either
a) by a failure modes and effects analysis of the design using element failure data from a recognised industry source
b) from experience of the previous use of the element in a similar environment (see 7.4.10).

6 Conclusion

, STMA-79795 - -Below a generic conclusion, not focussed on the STM ATB development is included:

, STMA-79785 - The main objection from railway experts against the IEC61508 standard, compared to EN-5012X, is the acceptance of systems with “hardware fault tolerance” (HFT) =0, i.e. a single fault can lead directly to an unsafe state. The latter only with a chance with is sufficiently low to comply with the quantitative safety requirements of the EN5012x.

, STMA-79787 - In general HFT=0 doesn't imply that a single fault can lead to an unsafe state. Independent diagnostic measures which prevent the system from going into an unsafe state are taken into account in the "safe failure fraction" (SFF). I.e. a system with two independent circuits, one performing the function and the other one guarding the function is classified with HFT=0 while both the functional and the guarding sub-systems must fail before an unsafe state is reached. However certification against IEC61508 (SIL3) with HFT=0 doesn't guarantee that no single fault can lead to an unsafe state.

, STMA-79788 - Because of the acceptance of HFT=0 in specific cases with a very low probability, for each component for which certification against IEC61508 is to be cross accepted into an EN50126-129 product, it shall additionally be proven that no single fault can lead to an unsafe state, or that the concerning fault can be classified as incredible.

, STMA-79790 - The EN50129 provides examples (not requirements) to enhance independence which are primarily focussed on insulation between independent components. Insulation is an effective measure to achieve independence in case of digital (e.g. relay) circuits, however much less effective for electronic circuits. As EN50129 requires independence but doesn't provide concrete requirements for proving independence for on-chip redundancy there seems no formal objection to use the concrete requirements from IEC61508. Those requirements are included in IEC61508-2 annex E.