ERTMS/ETCS

UNISIG Causal Analysis Process

REF : SUBSET-077

ISSUE : 3.0.0

DATE : 2016-06-20

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
AZD		
BOMBARDIER		
CAF		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1. 10/12/00	All	Creation	WLH
0.0.2. 02/01/01		Update following comments from Alcatel, Ansaldo Invensys and Siemens	WLH
0.0.3. 11/01/01		Modification following a RAMS group review in Zurich 9/10-01-01	WLH
1.0.0. 17/01/01		Minor updates and release ‘for information’ to ESROG	WLH
1.0.1. 23/02/01		Updated for working group use with the description of Column 13 and clarification of the fault tree process	WLH
1.0.2. 18/02/02	3, 4, 5 & 6	Descriptions updated to reflect lessons learnt in the application of the process	WLH
1.0.3. 22-02-02		Tidying up	WLH
1.0.4 25-02-02		Minor comments ex Bombardier and Siemens	WLH
2.0.0. 26-02-01		Raised in issue for release to the EEIG	WLH
2.0.1. 01-10-02		Minor corrections. Sections 4 & 9 added	WLH
2.0.2. 03-12-02	3, 4, 5, 6, 7, 8, 9.	Amendments as required by Ansaldo, Bombardier and Siemens following review	WLH
2.0.3 15-01-03	4	Reference to subset 026 changed from Functional to System requirements following review meeting of 14-01-03	WLH
2.1.0. 31-01-03		Raised in issue for release to the Users Group.	WLH

2.2.2. 21-03-03		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	WLH
2.3.0 27-08-10		- Clarification of the FMEA process in chapter 7.2.2 - New document template - Minor corrections	DARI
2.3.1 14-09-10		Changes during RAMS-meeting	DARI
2.3.2 26-10-10		Minor correction during RAMS-meeting	DARI
3.0.0 2016-06-20	Front page	Baseline 3 2nd release and 1st maintenance release version	RAMS WP

2. TABLE OF CONTENTS

3. PURPOSE AND SCOPE OF THE CAUSAL PROCESS

3.1.1.1 The purpose of the causal process is to derive the minimum set of safety requirements for the ETCS equipment as bounded by the Unisig reference architecture. This reference architecture is defined in the Unisig System Requirements Specification (SRS), Subset-026.

3.1.1.2 The requirements will be the minimum necessary to ensure that technical interoperability can be achieved safely whilst allowing the maximum freedom of equipment implementation.

3.1.1.3 Tolerable hazard rates will be derived from an overall hazard rate for the reference architecture as agreed by the National Safety Authorities.

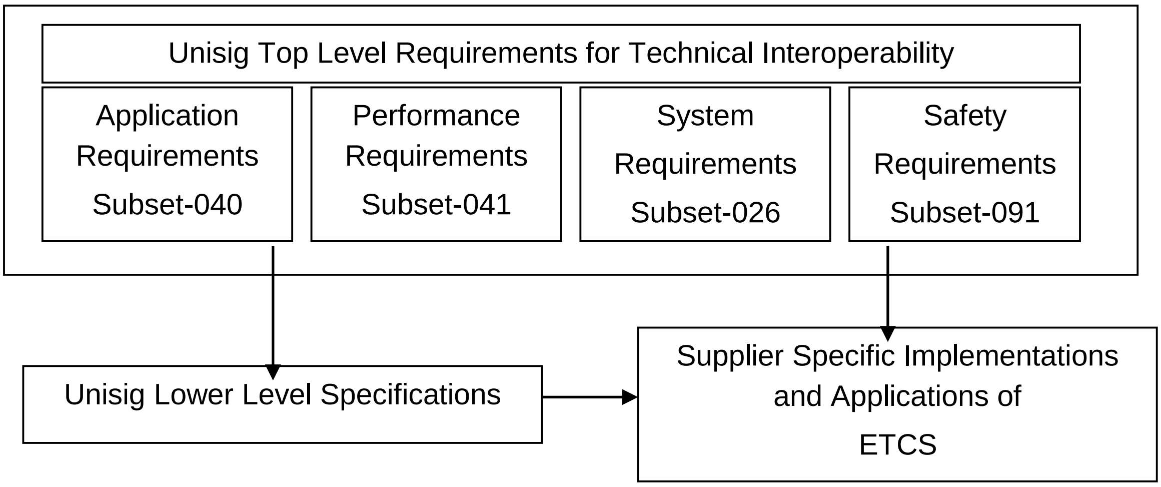
3.1.1.4 The mandatory safety requirements necessary for interoperability will be captured in Unisig document Subset – 091.

3.1.1.5 Compliance with the safety requirements for a specific implementation of the equipment will need to be demonstrated by a safety case prepared in accordance with the relevant European standards.

3.1.1.6 Supporting analysis documents that will be created as part of the causal process will not be mandatory but they will be available and may be used to assist suppliers in the preparation of safety cases demonstrating compliance with the Safety Requirements for their specific implementation of ETCS.

4. UNISIG DOCUMENT HIERARCHY

4.1.1.1 The following diagram indicates where the Safety Requirements Specification will sit in relation to other Unisig documents and how these documents might be used by a supplier when developing and applying the technically interoperable system.


Unisig Top Level Requirements for Technical Interoperability
Application Requirements Subset-040
Performance Requirements Subset-041
System Requirements Subset-026
Safety Requirements Subset-091
Unisig Lower Level Specifications
Supplier Specific Implementations and Applications of ETCS

5. INTRODUCTION TO THE CAUSAL PROCESS

5.1 Overview

5.1.1.1 The causal process is one of analysis of the design as defined in the Unisig System Requirements Specification Subset 026.

5.1.1.2 The analysis of the ETCS system design takes place in a series of clear steps.

- Identification of the core hazard(s) relating to ETCS
- Analysis of events at the boundary of the ETCS reference architecture to identify external events that may initiate a progression to ETCS entering a hazardous state. This will be undertaken in a series of Failure Mode and Effect Analyses (FMEAs).
- Analysis of how ETCS is intended to operate and to determine if there are internal barriers to the initiating events identified as potentially dangerous in the FMEAs. This functional view of ETCS will be captured in a Fault Tree (FT).
- A detailed analysis of the system operation in its various modes to formally assess all the events to determine the set of hazardous events. This step is required because of the difficulty in representing all modal variations in the fault tree.
- A top down apportionment of a tolerable Hazard Rate for ETCS that has been approved by the National Safety Authorities. This will be undertaken by assessing the performance of ETCS against a defined reference mission.
- Capturing all of the safety requirements and hazardous events together into a standalone document and defining the minimum set of tolerable hazard rates consistent with the reference architecture. The will also define the hazardous events that a supplier will need to control in order to meet the defined targets but such lower level apportionment of hazard rate will be private matter.

5.1.1.3 The package of work represents an independent assessment of ETCS and as such the work will be subject to review by the Unisig system Design Authority, the Super Group to ensure that their design intent has been fully respected.

5.2 Process Summary

5.2.1.1 The causal analysis will be focused on apportioning the tolerable hazard rate for the ETCS reference architecture to the Unisig grouping of constituents such as to ensure that technical interoperability can be achieved safely.

5.2.1.2 In addition the causal process will identify potential hazards within a constituent or grouping thereof that will need controlling within a particular implementation of ETCS.

5.2.1.3 The process to achieve the above will be a mixture of bottom up and top down analysis.

5.2.1.4 The initial step will be to identify the core hazard(s).

5.2.1.5 This will be followed by identifying by means of FMEAs the external initiating events that could occur at the boundary of ETCS and that would lead to an unsafe situation on the Railway and a possible unacceptable rate of occurrence of the core hazard.

5.2.1.6 This will be followed by a two-stage analysis of how these base events could migrate through the ETCS. This will result in a complete list of potential hazardous events within ETCS and the identification of all possible mitigations, both inherent in the design of ETCS and external to ETCS.

5.2.1.7 The final step will be the apportionment of the Tolerable Failure Rate (due to random failures) as decreed by the National Safety Authorities over the ETCS Constituents. This is undertaken against a mission profile representing both High Speed and Conventional applications, and will result in targets that may be assessed as part of a conformity process. The overall safety of a particular railway operation will remain dependent on how the system is utilised.

5.2.1.8 The analysis will be constrained by there being no mandated internal structure for the reference architecture. This is because as each manufacturer will implement the system in a manner that best suits the technology at his disposal and his own skill base. However, to ensure technical interoperability and a common acceptance process, each supplier will need to address the agreed set of hazardous events as identified by the causal process.

5.2.1.9 The application of the process could possibly drive out proposals for enhancements to ETCS and it could also identify possible areas of weakness in the application of ETCS. Any such findings will need to be discussed with the representatives of the European railways and may affect the analyses.

5.2.1.10 How such requirements will be satisfied will remain private to a specific manufacturer. However, demonstration of the adequacy of the mitigation measures taken will be demonstrated via an implementation specific safety case according to the relevant European standards.

6. RAILWAY OPERATIONAL ASSUMPTIONS

6.1 The Need for Assumptions

6.1.1.1 It will be necessary for the causal analysis to be conducted against a background of a general application. In the Unisig work the background will primarily be that of a European high-speed/conventional, interoperable and cross border network constructed and operated in accordance with the Technical Specification for Interoperability.

6.1.1.2 Only by having a representative application in mind in the form of a Mission Profile can assessments of the failure rates impinging on the ETCS be made with any confidence. It will be the role of the Railway Authorities to provide such a Mission Profile that can be related to standardised operational procedures and operational hazards that respect the Unisig functional allocation.

6.1.1.3 In considering the mission profile it will be assumed that the ETCS is deployed in accordance with the Unisig Dimensioning and Engineering Rules, Subset-040.

6.2 Summary of the Assumptions

6.2.1.1 The assumptions made, are that correct information is advised to,

- The ETCS equipment manufacturer
- The ETCS equipment from external interfaces
- The ETCS user responsible for the introduction of data.

6.2.1.2 The National Safety Authorities (NSA's) have indicated that the analysis will only consider harm to a passenger whilst travelling on the train. It remains the responsibility of the Railway Authorities to assess, by the analysis of possible consequences, that introduction of ETCS does not compromise a defined Tolerable Individual Risk of Fatality (TIRF) for the passenger on the train.

6.2.1.3 Operation in Level STM or Level 0 is considered to be a national issue and will not be analysed as part the Unisig work. Thus the work will be limited to consideration of Application Levels 1 and 2.

6.2.1.4 For the major part of its journey the high-speed train complete with its passengers, will operate with ETCS in the Full Supervision mode. Other driving modes / procedures that will be considered are;

- Start of Mission
- Staff Responsible
- Reversing
- Shunting

6.2.1.5 Consideration of Emergency operation, Temporary Speed Restrictions and Level transitions will occur as part of a bottom up macro function analysis

6.2.1.6 Consideration of the risks to railway staff and risks to non-travelling public (neighbours) using the railway infrastructure will be part of a national consequence analysis.

6.2.1.7 The starting point for the Causal Analysis work will be agreed core hazard(s) relating to the ETCS Reference architecture and an agreed maximum rate of occurrence for that hazard.

Unisig will identify the core hazard(s)

The Railways will approve the core hazard(s) and define the maximum Tolerable Rate of occurrence for the core hazard(s)

The defined tolerable rate of occurrence and the core hazard will be subject to approval by the National Safety Authorities

7. CAUSAL ANALYSIS

7.1 Core Hazard(s) and the Tolerable Hazard Rate(s)

7.1.1.1 Prior to the commencement of the Causal analyses, the definition of the role of the Unisig reference architecture will be agreed with representatives of the European Railways as appointed by the Users Group.

7.1.1.2 From the agreed definition, a core hazard (or set there of) that could ultimately lead to a passenger fatality will have been identified.

7.1.1.3 Derivation of a tolerable rate of occurrence for the core hazard(s) will be undertaken by the European Railway representatives and will be subject to approval by the National Safety Authorities.

7.2 Failure Modes & Effects Analysis (FMEA)

7.2.1.1 The FMEA will provide a means of rigorously assessing the effect of a functional failure at the boundary of the reference architecture assuming no mitigation by ETCS. The FMEA will be carried out on the interfaces to/from the Unisig Reference architecture at the detail of the mandatory macro functions.

7.2.1.2 The first step will be to identify the macro functions associated with each of the mandatory interfaces defined in the Unisig Reference architecture. The relevant interfaces are summarised as follows

1. On-board Assembly

    1.1 Interface to/from the Train Interface Unit (Subsets 080-1 & -2

    for Levels 1 & 2 respectively)

    1.2 Interface to/from the Man Machine Interface (Subsets 079-1 & -2

    for Levels 1 & 2 respectively)

2. Trackside Assembly

    2.1 Interface to/from an Adjacent RBC (Subset 078)

    2.2 The Transmission paths between trackside and train (Subsets 081-1 & -2 for Levels 1 & 2 respectively)

Note that the RBC interface to / from the interlocking and the interfaces to the power sources will be regarded as private interfaces subject to an application specific assessment. In addition, note that the interface to the JRU is not considered to be a safety-related interface and therefore, will not be analysed.

7.2.2 The FMEA Process

7.2.2.1 The FMEA will be used to systematically evaluate and document the potential impact of a failure of each of the mandatory ETCS macro functions that occur at the boundary of the reference architecture. Each defined functional failure will be assessed for its effects on the ETCS system and on train operation assuming that there are no other failures. The effects of each failure will be assigned a severity category based upon the potential impact of such a failure on the safety of a passenger on the train.

Mitigating effects due to any internal or external barriers of ETCS will not be taken into account at this stage, since the object with the FMEA is to actually identify the necessary barriers and their importance. To clarify this approach the effect column is denoted ‘Initial End Effect’, where ‘Initial’ thus refers to ‘before credit for barriers’.

7.2.2.2 A separate FMEA will be conducted for each ETCS application level, taking account of the various operational modes, as the differences in trackside infrastructure could result in a specific failure ending in a different end effect.

7.2.2.3 The FMEA will be documented on a standard worksheet which includes the following fields which must be considered for each ETCS interface macro function;

- Reference Identification
- ETCS Interface
- Macro Function
- Failure Mode(s)
- ETCS Failure Cause
- Operational Mode
- ETCS Failure Effects
  - ➢ Local Effects
  - ➢ Intermediate Effects
  - ➢ Initial End Effects
- ETCS External Protection / Mitigation / Barriers
- Severity (of Initial End Effect)
- Failure Rate
- Internal Barriers

7.2.2.4 The FMEA column fields to be filled in are explained in the following sections

7.2.3 Column 1: Reference Identification

7.2.3.1 A reference identification number will be assigned for traceability purposes and is entered onto the FMEA worksheet. The identification number shall be applied in accordance with the numbering system as shown in section 7.2.1.3. Additional levels of identification numbering will identify each macro function and its associated failure mode(s). This numbering convention will enable a clear and unique identification of interfaces, macro functions and failure modes throughout all of the FMEA's.

7.2.4 Column 2: ETCS Macro Function

7.2.4.1 The name of the ETCS interface and its macro function(s) to be analysed for failure modes will be included in this field; the name shall be consistent with those identified in section 7.2.1.3.

7.2.5 Column 3: Macro Function Data Item

7.2.5.1 For each macro interface function its inputs and outputs will be identified. These inputs and outputs are termed macro function data items and are the individual items for which the failure modes are to be determined.

7.2.5.2 For the purposes of traceability, cross referencing to the System Requirements Specification or its subordinate mandatory documents will be added.

7.2.6 Column 4: Failure Mode

7.2.6.1 Each macro function data item will be considered in turn and its failure modes determined by examination of its function and its stated requirements as defined by the reference architecture. Typical failure modes considered include failure to perform the function, incorrect performance of output function, incorrect timing of output function. Guidewords to be used to aid in the identification of the failure mode are listed below. These guide-words are as recommended in EN 50159-2, which also defines the meaning of the guide-words.

Failure Mode Guide-words for Data Transmission

Guide-words
Corruption
Deletion
Delay
Repetition
Insertion
Re-sequence
Masquerade

For discrete signals the following guide-words will be recommended

Guide-words
Incorrect
Absent
Timing
Insertion

Where the following meanings are assigned

Incorrect – The discrete signal is in the wrong state

Absent – The discrete signal is not present

Timing – The correct signal appears later than required

Insertion – A random change of state

7.2.7 Column 5: Failure Cause

7.2.7.1 For each failure mode a failure cause will be identified which relates the cause of the failure to the constituent most likely to be the source of the failure. Where the failure cause is identified as being from a separate constituent to that being assessed then a reference will be made to the unique FMEA reference identification number where the constituent item is assessed.

7.2.7.2 If the failure is caused by systems outside the ETCS reference architecture then this will be stated as such.

7.2.8 Column 6: Operational Mode

7.2.8.1 The effect of the failure will be assessed for each of the modes identified in 4.2.1.6. Where specific operational timing or location information is relevant to the failure, such information will be recorded.

7.2.9 Column 7: Local Effect

7.2.9.1 Local effects concentrate specifically on the impact the assumed failure mode has on the operation and function of the item under consideration assuming that no other failure is present. The consequences of each assumed failure on the operation of the ETCS function shall be described including any second order effects that result. It is possible for the local effect to be the failure mode.

7.2.10 Column 8: Intermediate Effect

7.2.10.1 Intermediate effects will define the impact that the assumed failure mode has on the operation of the ETCS and railway at an intermediate level. That is, between the failure mode itself and the resulting end effect on the ETCS systems and train as a whole. Again, the analysis will assume that no other failure is present.

7.2.11 Column 9: Initial End Effect

7.2.11.1 Initial End Effect will define the total effect the assumed single macro function failure has on the operation, function or status of the train. The end effects should be consistent with the core hazard(s).

As explained in chapter 7.2.2, evaluation of the initial end effects will **not** take into consideration any mitigation or protection measures inherent within the ETCS reference system that may either reduce the impact of such a failure or prevent it from occurring at all.

7.2.12 Column 10: ETCS External Protection / Mitigation / Barriers

7.2.12.1 This will, if possible, define measures external to the reference architecture that protect or mitigate against the effect of the failure. Such measures could include for example, specific protection features, redundant systems, operational rules, operator actions etc.

7.2.13 Column 11: Severity (of Initial End Effect)

7.2.13.1 A severity level will be assigned to each Initial End Effect, repeated for every failure mode associated with it. The categorisation system to be used will be as the example in EN 50126 for a passenger, part of which is repeated here for convenience, and also complemented with events without safety effect.

End Effect / Hazard Severity Level

Severity Level	Consequence to Passenger
Catastrophic	Single fatality and/or multiple injuries.
Critical	Single severe injury
Marginal	Minor injury
Insignificant	Possible minor injury
RAM Issue	Service impact, not safety related
No effect	None

7.2.14 Column 12: Failure Rate

7.2.14.1 If data is available, the failure rate for the failure mode under consideration will be recorded together with a reference to the source of the data.

7.2.14.2 Failure rate data will be obtained from the railway authorities, existing equipment designs e.g. EuroBalise. Failing either of these sources, figures from the original Esrog causal analysis may be used.

7.2.14.3 The failure rate referenced will take account of all external mitigation measures as identified in 5.2.12.

7.2.15 Column 13: Internal Barriers

7.2.15.1 Barriers internal to the Reference Architecture that are known to mitigate against the risk identified in columns 11 and 12 will if possible, be noted in this column. This information will be used in the development of the functional fault trees.

7.3 Analysis

7.3.1 Fault Tree

7.3.1.1 As indicated in the introduction, the work is that of analysing a well-documented design. The fault tree provides a convenient means of recording a functional hierarchy for the system to provide a means of assessing how the potentially hazardous events identified in the FMEA's could migrate through the system.

7.3.1.2 Fault Tree Analysis is a deductive technique so it will be used to decompose the agreed and approved core hazard(s) downward to meet the potentially hazardous events identified in the FMEA's. The decomposition will be through a hierarchy of internal ETCS macro function failures that will be combined by a series of logical OR or AND gates. A separate fault tree will be developed for each application level but no attempt will be made to portray different modes of operation.

7.3.1.3 The developed fault tree will represent a system view of ETCS without regard for a functional deployment to constituents.

7.3.2 Functional Analysis

7.3.2.1 The fault tree will lead to a fully documented analysis of the criticality of ETCS functionality in protecting against the boundary failures leading to the core hazard at an unacceptable rate.

7.3.2.2 This detailed 'bottom up' analysis will take account of the operational modes of ETCS as defined in 6.2.1.5 & 6 and will be documented to with all mitigation factors both external and the inherent protective features of ETCS, taken into account.

7.3.2.3 The analysis will lead to the completion of the hazard identification process

7.4 Top Down Apportionment of the ETCS THR

7.4.1.1 Following completion of the Fault Tree and the bottom up analysis will be the top down apportionment of the tolerable hazard rate for the core hazard over the approved grouping of constituents.

7.4.1.2 An initial trial apportionment will be undertaken based on a simple dividing down of targets over the constituent groupings. The feasibility of this trial apportionment will then be tested against an operational analysis of the role that constituent performs in ETCS.

7.4.1.3 The assumption will be made that all items and constituents external to the constituent under examination are working correctly

7.4.1.4 The frequency that an analysed role will be undertaken is a critical factor in the analysis and this rate of occurrence will be dictated by the approved mission profile. This in turn could lead to a modification of trial apportionment.

7.4.1.5 In determining the safety target, credit will be given to the inherent protective features of ETCS that have been identified earlier. Other possible mitigating factors such as driver vigilance will not be credited in deriving a tolerable failure rate for the constituent.

7.4.1.6 Assumptions about the failure rate of drivers will need to be made and such assumptions will be made clear, as ultimately they will need the approval of the railways.

7.4.1.7 Risks that cannot be successfully mitigated against in the reference architecture will be identified. Such risks may require, for example, additional protective features within ETCS, clarification of Operational Rules or amendments to the Unisig Engineering Rules.

7.4.1.8 A sensitivity analysis will be carried out on the THR apportionment to determine the criticality of key events and to determine if the derived targets will be suitable for a wide range of ETCS applications.

7.4.1.9 The resulting figures for the ETCS grouping of constituents will be as equipment failure rates which may be appropriate for conformity assessment but there is no simple relationship between these figures and the achieved safety on a railway network.

8. SAFETY REQUIREMENTS SPECIFICATION

8.1.1.1 The requirements will be developed in two passes. Requirements will be generated that are Application Level specific by consolidation of the respective ‘top down’ and ‘bottom up’ analyses.

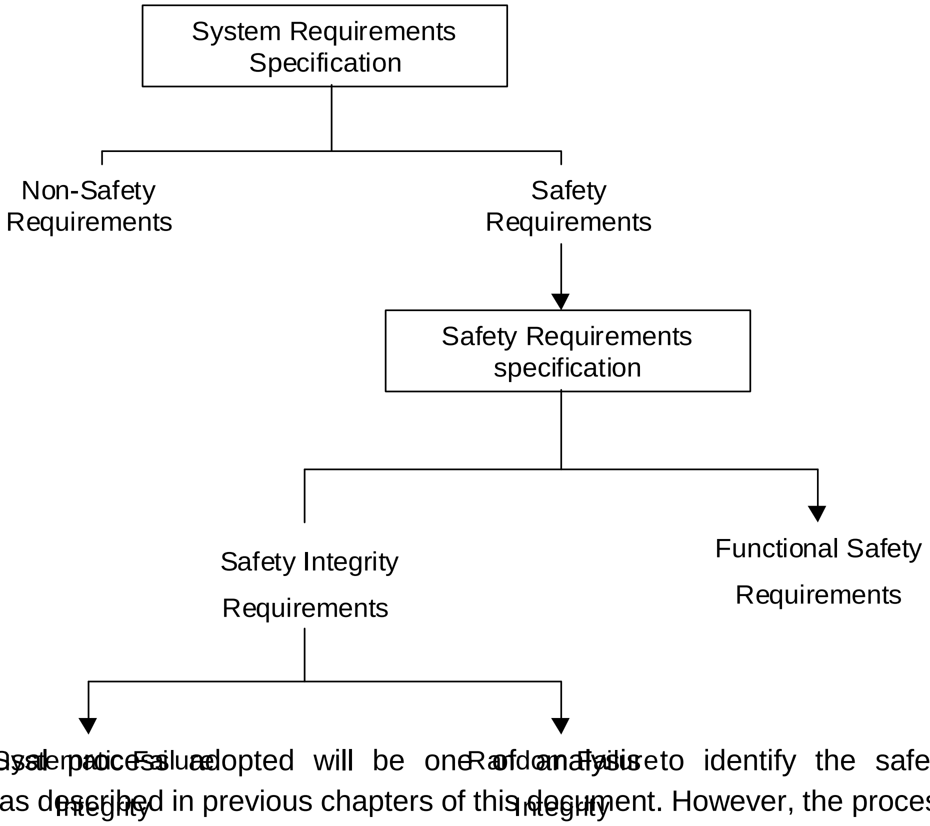
8.1.1.2 The consolidated set of safety requirements covering hazard rate targets for constituents with the identification of internal hazards, will represent the most onerous of Level 1 and Level 2 requirements

8.1.1.3 The requirements will also identify events external to ETCS that could influence the achieved operational safety. These events will be allocated an appropriate quality level designed to ensure that ETCS is not compromised.

9. PROCESS COMPLIANCE WITH APPLICABLE CENELEC STANDARDS

9.1.1.1 In assessing compliance against EN50129 it is important to remember that the causal process is primarily, an analysis of a fully documented design. This design, and its macro functionality, is defined in the Unisig System Requirements Specification Subset 026. In this document there is no distinction made between non-safety and safety requirements.

9.1.1.2 Considering Figure A.1 in Annex A of EN50129 which defines the hierarchy of requirements as follows,


System Requirements Specification
Non-Safety Requirements
Safety Requirements
Safety Requirements specification
Safety Integrity Requirements
Functional Safety Requirements
Systematic Failure Integrity
Random Failure Integrity

9.1.1.3 Thus the causal process adopted will be one of analysis to identify the safety requirements as described in previous chapters of this document. However, the process of apportioning safety integrity requirements is taken only to the level of the Unisig reference architecture. Since the implementation of internal features is not harmonised and will therefore be unique to a specific and private implementation of the functionality, no further allocation of safety integrity requirements will be made.

9.1.1.4 Where a hazard occurs at an interoperable boundary, then the hazard, its tolerable random failure integrity and tolerable systematic failure integrity will be defined.

9.1.1.5 Systematic integrity requirements will also be allocated to external processes upon which the rate of occurrence of the core hazard(s) of ETCS is dependent.