EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Report

"Safety Critical Components" in railways - The concept of "Safety Criticality" of the systems

	Drafted by	*Validated by*	*Approved by*
Name	Christina Kyriakopoulou		
Position	Trainee		
Date	24/05/2017	Enter a date.	Enter a date.
Signature			

Document History

Version	*Date*	*Comments*
0.1		First Version

Contents

The concept of "Safety Criticality"

In 2016, the 4th railway package[1] introduced the term "safety critical components".

EU railway legislation does not contain though any clear definition of which component can be characterised as safety critical. In 2016, the Agency conducted several informal and formal consultation[2] to define the state of play in the area. In general terms, the only output of the consultation conducted was that currently there is no list defining which components of the railway system are safety critical.

A harmonised list could vary among the different railway systems in the EU Member States (MSs), utterly considering potential diverse factors present in the different MSs, such as the environmental conditions including the geographical scope, the safety objectives, the km or the operational hours, the operational processes, the maintenance context, the time (lifecycle) and the design of each different railway system. Hence, depending on the situation, a harmonised list for all EU MSs could be either non-complete or too exhaustive, which could unavoidably result in non-sustainable increase of cost in design, use and maintenance of the technical systems.

In addition, it is better to refer to "systems", rather than to "components" given that "systems" pinpoint also the interactions between components.

For the aforementioned reasons, it is preferable at this stage to establish a harmonised "process approach". According to this approach, the RUs/ECMs in the MSs are those railway entities responsible for determining the maintenance levels of such systems, on the basis of the degree of risk arising from critical functions and/or component failures.

Following this process-approach principle, the aim of this report is:

A. To shortly go through safety criticality approaches already existing in

1. civil aviation
2. industry

B. To adjust some targeted points of the aforementioned approaches to the railway system.

[1] Regulation 2016/796: CHAPTER 4, Article 19, 1. (I); Directive 2016/797: Consideration (67), ANNEX III, 1.1.1; Directive 2016/798: CHAPTER VI, Article 29, ANNEX III, 10

[2] 1 meeting with the voluntary ECM in July 2016; 1 conference call with the voluntary IM in July 2016; 1 meeting with CEN/CENELEC in August 2016; 2 presentations in NSA network in September and November 2016; 1 presentation to Cooperation of ECM certification bodies in October 2016; 1 presentation in the Network of Representative Bodies in December 2016.

A.1. Civil Aviation Approach

The traditional approach of safety criticality in civil aviation dictated that *a component is safety critical if a single failure of the technical system in which it is integrated leads to a catastrophic accident*.

The aeroplane technical systems were in principle evaluated with use of i) exclusively the "single fault" criterion, or ii) exclusively the "fail-safe design" concept:

i) the "single fault" criterion

The single fault criterion is a requirement, according to which a system designed to carry out a defined safety function must be capable of carrying out its mission in spite of the failure of any single component within the system or in an associated system which supports its operation.

The compliance with this criterion should be considered in order to achieve high safety standards.

The main disadvantage of this assessment method is that it fails to consider the frequency of a failure. It would be valueless to characterise a technical system as safety critical if there is a low likelihood for a single failure of this system to lead directly to a catastrophic accident.

ii) the "fail-safe design" concept

This concept uses the following design principles or techniques to ensure a safe design: Designed Integrity and Quality, Redundancy or Backup Systems, Proven Reliability, Failure warning or Indication, Checkability, Designed Failure Effect Limits, Error-Tolerance, etc[3].

Regarding this concept, the combination of two or more principles or techniques is usually needed to provide a fail-safe design.

In other words, the system's non-compliance with at least two of them, renders it safety critical.

The new "CS-25" approach[4]

The development of new-generation aeroplanes resulted in a higher level complexity of systems' interaction (highly integrated systems). This led to the need for more complex safety-critical functions. The efficiency of already existing techniques for assessing safety aspects of highly integrated systems was put in question, particularly with the expansion of IT technology and software based techniques.

This led to the development of new approaches, both qualitative and quantitative, for determining safety requirements and establishing compliance with them.

The new approach, known as CS-25, concerning the airworthiness requirements for large aircraft, covers[5] the design and installation requirements for the aeroplane systems and their associated components, for them to function properly when installed and not to degrade safety.

These requirements are determined by considering both the likelihood and severity of the Failure Condition[6] Effects.

[3] CS-25 BOO2, AMC 25.1309, 6(b)2

[4] https://www.easa.europa.eu/system/files/dfu/CS-25%20Amendment%2018_0.pdf

[5] especially the AMC (Acceptable Means of Compliance), See AMC 25.1309 of CS-25

[6] A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering the flight phase and relevant adverse operational or environmental conditions.

A.2. Industry Approach

The concept of functional safety applies to every industrial sector. Fictional safety in industry identifies specific potentially dangerous conditions, situations or events that could result in an accident that could harm somebody or destroy something.

Fictional safety in industry is part of the overall safety of a system or piece of equipment and generally focuses on electronics and related software. For instance, when someone boards a train functional safety ensures that the doors close before the vehicle departs and that they don't open while it is in movement.

The aim of functional safety is to bring risk down to a tolerable level and reduce its negative impact; however, there is no such thing as zero risk. Functional safety measures risk on the basis of how likely it is that a given event will occur and how severe it would be; in other words: how harm it could cause.

The industrial standard IEC 61508[7]

Currently, this standard used in industry is already used also in railways (see also IEC 62279:2015).

This standard has its origins in the process control[8] industry and serves the purposes of development of new technical solutions applying to Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).

Standard IEC 61508 provides an effective benchmark system used by electro-mechanical technology or solid-state programmable electronics. IEC 61508 supports the assessment of risks to minimize these failures in all E/E/PE safety-related systems, irrespective of where and how they used and it is intended to be a basic functional safety standard for each and every industry.

The standard covers the complete safety life cycle[9], and may need interpretation to develop sector specific standards. For instance, IEC 62279:2015 provides a specific adaptation of IEC 61508 for railway applications which is intended to cover the development of software for railway control and protection including communications, signaling and processing systems.

Central to the standard are the concepts of risk and safety function. The risk is a function of frequency (or likelihood) of the Hazardous event and the event consequence severity. According to IEC 61508 risk is reduced to a tolerable level by applying safety functions which consist of E/E/PES. This risk assessment effort yields a target SIL[10], which thus becomes a requirement for the final system.

The Agency suggests that the procedure used by the industrial standard IEC 61508 expands to all components and it is not restricted to the Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) of railways.

[7] http://www.iec.ch/functionalsafety/explained/

[8] The active changing of the process based on the results of process monitoring.

[9] The series of phases from initiation and specifications of safety requirements, covering design and development of safety features in a safety-critical system, and ending in decommissioning of that system.

[10] A measure of safety system performance, in terms of probability of failure on demand (PFD).

B. Safety Criticality in railways, inspired by aviation CS-25 & industry IEC 61508 approaches

Purpose of this section is to adjust some targeted points to the railway system by:

a) adjusting in railways the **procedures** followed in CS-25 & IEC 61508

b) tracing all the safety critical events

c) filtering the safety critical significant events

d) taking into account arising considerations/constraints that apply.

For the following analysis, consider that the terms "Failure conditions" (in aviation) and "Hazardous events"(in industry) and " Safety critical events" (in railways) have a similar notion.

CS-25 approach

According to the civil aviation approach, in order to determine if a system is safety critical, you assess the failure conditions in the system.

The **criteria** for considering the failure conditions (and thus the system) are the severity and the frequency; mutatis mutandis for railways as following:

- ✓ **Severity**
  Failure Conditions may be classified in five "teams" according to the severity of their effects as follows:

  I. **No Safety Effect:** Failure Conditions which would have no effect on safety; *for example, Failure Conditions that would not affect the operational capability of the railway system or would not increase staff workload.*

  II. **Minor:** Failure Conditions which would not significantly reduce railway safety, and which involve staff action that are within their capabilities; *for example, a slight reduction in safety margins or functional capabilities, a slight increase in staff workload, such as routine plan changes, or some physical discomfort to passengers or staff*

  III. **Major:** Failure Conditions which would reduce the capability of the railway system or the ability of the staff to cope with adverse operating conditions; *for example, a significant reduction in safety margins of functional capabilities, a significant increase in staff workload or in conditions impairing staff efficiency, or discomfort to the railway staff, or physical distress to passengers or staff, possibly including injuries.*

  IV. **Hazardous:** Failure Conditions which would reduce the capability of the railway or the ability of the staff to cope with adverse operating; *for example, a large reduction in safety margins or functional capabilities, or physical distress or excessive workload such that the staff cannot be relied upon to perform their tasks accurately or completely or serious fatal injury to a relative small number of the occupants other than the staff.*

  V. **Catastrophic:** Failure Conditions which would prevent continued safe route of the train and result in multiple fatalities.

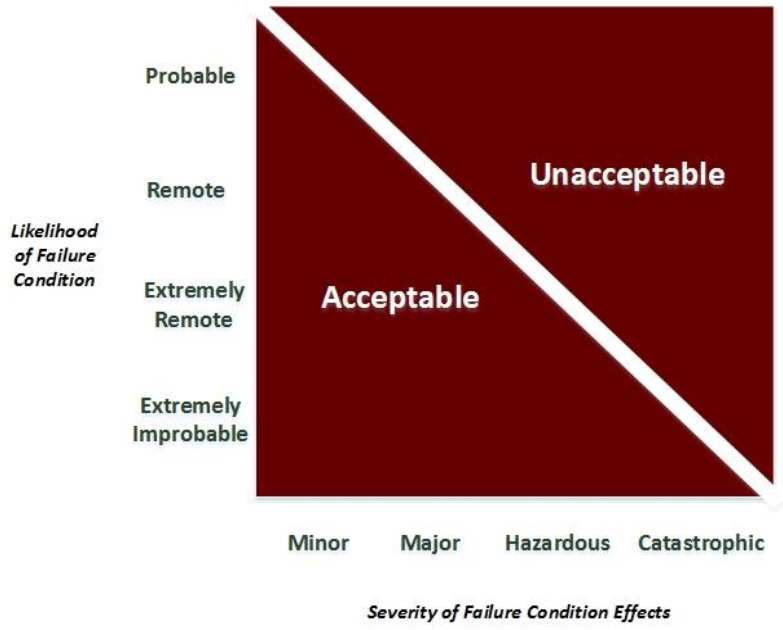
✓ **Frequency**

The following descriptions of the likelihood levels could be used

- **Probable Failure Conditions** are those anticipated to occur one or more times during the entire operational life of each system.
- **Remote Failure Conditions** are those unlikely to occur to each system during its total life, which may occur several times when considering the total operational life of a number of systems of one type.
- **Extremely Remote Failure Conditions** are those not anticipated to occur to each system during its total life but which may occur a few times when considering the total operational life of all systems of one type.
- **Extremely Improbable Failure Conditions** are those so unlikely that they are not anticipated to occur during the entire operational life of all systems of one type.

The general principle is that a logical and acceptable inverse relationship should exist between the likelihood of a Failure Condition and its effect, as shown in the Figure below:

Figure 1: Relationship between Likelihood and Severity of Failure Condition Effects



From this diagram we conclude that the following requirements are acceptable in aviation (for railways, see further in the text):

- ✓ Minor Failure Conditions that vary from extremely improbable to probable
- ✓ Major Failure Conditions must be no more frequent than Remote
- ✓ Hazardous Failure Conditions must be no more frequent than Extremely Remote
- ✓ Catastrophic Failure Conditions must be Extremely Improbable

Failure Conditions with No Safety Effect are not to be considered at all as safety critical.

The adaptation of CS-25 in railways follows an adverse approach in relation to aviation.

According to this adverse approach, what matters to identify the safety criticality for railways is to detect the unacceptable area of the graphics above, rather than to focus on the acceptable part meaning the compliance with the requirements.

According to this principle, regarding to these requirements, safety critical could be considered only those railway systems which are involved in **probable Major** Failure Conditions, **probable and remote Hazardous** Failure Conditions or **probable, remote and extremely remote Catastrophic** Failure Conditions.

The following matrix points out the safety critical Failure Conditions proposed for railways.

Figure 2: Safety Critical Failure Conditions

Frequency/Severity	Minor	Major	Hazardous	Catstrophic
Probable	?	X	X	X
Remote		?	X	X
Extremely Remote			?	X
Extremely Improbable				?

Industry IEC 61508 approach

As said above, please consider that the terms “Failure conditions” (in aviation) and “Hazardous events” (in industry) and “Safety critical events” (in railways) have a similar notion.

According to the industry approach, in order to determine if a system is safety critical, the hazardous events of that system should be considered.

The **criteria** for considering a Hazardous event of a system as safety critical for industry are the following:

- ✓ **Severity**
  Hazardous events may be classified in four “teams” according to the severity of their consequence as follows:
  - **I. Negligible:** Hazardous events which would result in minor injuries at worst
  - **II. Marginal:** Hazardous events which would result in major injuries to one or more persons.
  - **III. Critical:** Hazardous events which would result in loss of a single life.
  - **IV. Catastrophic:** Hazardous events which would result in multiple loss of life.

✓ **Frequency**

The following descriptions of the likelihood levels in industry could be used:

- **Frequent Hazardous Event** are those anticipated to occur many times in system lifetime.
- **Probable Hazardous Event** are those unlikely to occur several times in system lifetime.
- **Occasional Hazardous Event** are those not anticipated to occur once in system lifetime.
- **Remote Hazardous Event** are those so unlikely to occur in system lifetime.
- **Improbable Hazardous Event** are those very unlikely to occur.
- **Incredible Hazardous Event** are those cannot believe that it could occur.

These are typically combined into a risk class matrix for industry.

Figure 3: Safety Critical Hazardous Events

Frequency/Severity	Neligible	Marginal	Critical	Catstrophic
Frequent	II	I	I	I
Probable	III	II	I	I
Occasional	III	III	II	I
Remote	IV	III	III	II
Improbable	IV	IV	III	III
Incredible	IV	IV	IV	IV

Where:

- Class I: Unacceptable in any circumstance;
- Class II: Undesirable: tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained (ALARP principle);
- Class III: Tolerable if the cost of risk reduction would exceed the improvement;
- Class IV: Acceptable as it stands, though it may need to be monitored.

According to IEC 61508 applicable to industry, zero risk can never be reached.

By applying the adverse principle seen above for railways, according to which what matters to identify the safety criticality for railways is to detect the unacceptable area of the graphics above, rather than to focus on the acceptable part meaning the compliance with the requirements we conclude that

Safety critical could be considered only those railway systems which are involved in **frequent Marginal** Hazardous Events, **frequent and probable Critical** Hazardous Events or **frequent, probable and occasional Catastrophic** Hazardous Events.

Safety criticality in Railways

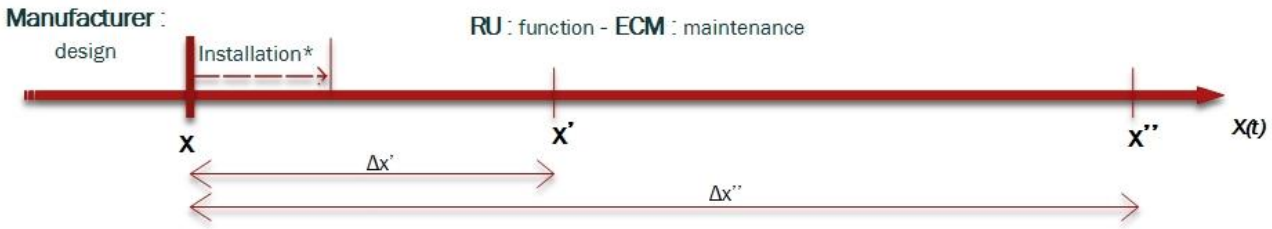
To sum up, the adaptation of CS-25 & IEC 61508 in railways follows an adverse approach in relation to aviation and industry.

What matters to identify the safety criticality for railways is to detect the unacceptable area of the graphics above, rather than to focus on the acceptable part meaning the compliance with the requirements.

The Failure Conditions according to CS-25 and the Hazardous Events according to IEC 61508 will be referred as Safety critical Events for the railways. The teams of classification and the quantitative and qualitative terms of the likelihood levels should be decided and be harmonized and clearly defined.

It should be mentioned that the arrows in the Figures 2, 3 above indicate that the criticality could vary during the operational life-cycle of a system. Hence, the appraisal of the Safety Critical Events should be a continuously repeated procedure and apparently not a standard list.

Figure 4: Appraisal of Safety critical Events of a system and/or component along its lifecycle



x(t): appraisal (frequency & severity) of Safety critical Events during the time
Δx(t): change of x(t)
x'= x + Δx'
x''= x + Δx''

*redefinition of the x

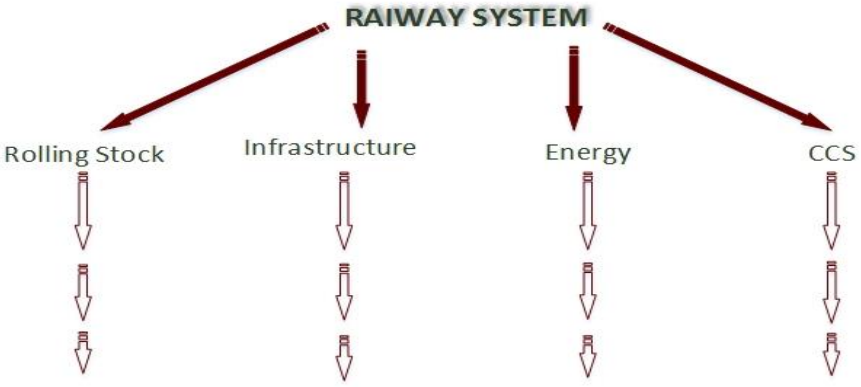
As it is shown in the Figure 4, the assessment procedure of the Safety critical Events should be conducted by the RU and the ECM operating or maintaining the system/component, since contrary with what happens civil aviation, the railway manufacturers are not responsible for the components' or systems' criticality. Of course at the time the system is supplied, the manufacturers must provide an appraisal of its Safety critical Event to ensure an acceptable safety level as installed in the railway network. This appraisal could be however even redefined during the installation period by experienced engineers.

B.a Procedure - Depth of analysis by the RU and the ECM to identify and classify Safety critical Events

The Safety critical Events should be identified by considering the potential effects of failures on the railway system and its users. These should be considered from two perspectives:

- by considering failures of function at the whole railway system level
- by considering failures of function at each sub-system

Figure 5: Level of Analysis



Depending on the extent of functions to be examined and the correlation between function and systems, different approaches may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interconnects are relatively simple, it may be feasible to conduct separate assessment for each system, providing any interface aspects are properly considered and are easily understood. However, where system and function interconnects more complex, a top down approach, from railway system level perspective, should be taken in planning and conducting assessments.

It should also be mentioned that a Safety critical Event might result from a combination of lower level events. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all Safety critical Events, which arise from multiple failures and combinations of lower level events, are properly identified and accounted for. The relevant combinations of failures and Safety critical Events should be determined by the whole safety assessment process that encompasses the railway system and sub-system level functional hazard assessments and common cause analyses. The overall effect on the railway system of a combination of sub-system Safety critical Event occurring as a result of a common or not failure, may be more severe than the individual system effect. For example, in the civil aviation Failure Conditions classified as Minor or Major by themselves may have Hazardous effects at a railway system level, when considered in combination.

As far as the division of the railway system in sub-systems is concerned, the best approach is to be based on the existing classification which is used in the ERA's safety alert IT system. This classification follows the EU TSIs and the EN 15380. ANNEX 1 contains the existing and proposed categorisation of the sub-systems (proposed by SAIT).

Apparently, there is no sense to create an alternative division of the sub-systems, which will probably result in confusion. The level of considering the failure of function should not be predetermined and each RU/ECM should be entitled to decide the depth of analysis.

B.b Assessment Methods by the RU and the ECM to identify and classify the Safety critical Events

Please, refer also to Annex 2.

The range of the acceptable probabilities for each likelihood level in order to define the frequency should be defined by experienced engineers.

An assessment of the likelihood of a Safety Critical events may be either qualitative or quantitative. On the other hand, an assessment to identify and classify the severity of a Safety critical Events is necessarily qualitative.

The quantitative methods of analysis are used with the help of analytical tools for determining numerical values should not in any case replace, qualitative methods based on engineering and operational judgement, but only supplement them. In some cases, the qualitative analyses of the frequency should be combined with quantitative analyses. In this way, the quantitative analyses provide guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes.

An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depend on:

- the types of functions performed by the system
- the severity of Safety critical Events
- whether or not the system is complex.

One of the assessment methods used in civil aviation and proposed also in railways is the the **Functional Hazard Assessment** (FHA).

What?

The FHA is an engineering tool, which should be performed early in the design stage and updated as necessary during the operational life-cycle of each system. FHA is a systematic, comprehensive examination of the severity of the failure.

How?

It could be used to define the safety objectives of high level railway systems or their individual sub-systems that must be considered in the proposed system architectures. It should also be used to assist in determining the development assurance levels for the systems.

FHA focuses primarily and targets only to identify potential Safety critical Events which may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors.

This assessment may be conducted using service experience, engineering and operational judgement, and/or a top-down deductive qualitative examination of each function.

Classification of Safety critical Events

In case FHA does not lead to an answer on safety criticality, there should be a further analysis also including the assessment of causes, severity, and likelihood of Safety critical Events and consequently the relative classification. The various types of analysis are based on either inductive or deductive approaches and the likelihood assessment may be qualitative or quantitative.

The additional analysis may be done using the following methods:

- **Design Appraisal**: This is a qualitative appraisal of the integrity and safety of the design system.
- **Installation Appraisal:** This a qualitative appraisal of the integrity and safety of installation. Any deviation from normal, industry accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into force.
- **Failure Modes and Effects Analysis** (FMEA): This a structured, inductive, bottom-up analysis, which is used to evaluate the effects on each sub-system and the whole railway system of each possible element or component failure. When properly formatted, it will aid in identifying latent failures and possible causes of each failure mode. A FMEA could be a Piece-Part FMEA (hardware) or a functional FMEA. For modern systems an exhaustive Piece-Part FMEA is not practically feasible with the present state of art. In that context a FMEA may be more functional than piece part oriented. A functional oriented FMEA can lead to uncertainties in the qualitative and quantitative aspects, which can be compensated for by more conservative assessment as such :
  - assuming all failure modes result in the events of interest,
  - careful choice of system architecture
  - taking into account the experience lessons learned on the use of similar technology
- **Fault Tree or Dependence Diagram Analysis**: This is a structured, deductive, top-down analyses that are used to identify the conditions, failures, and events that would cause each defined Failure Condition. They are graphical methods of identifying the logical relationship between each particular Safety critical Events and primary element or component failures, other events, or combinations that can cause it. A FMEA may be used as the source document for those primary failures or other events.
- **Markov Analysis:** A Markov model (chain) represents various system states and the relationships among them. The states can be either operational or no-operational. The transition from one state to another are a function of the failure and repair rates. Markov analysis can be used as a replacement for fault tree/dependence diagram analysis, but it often leads to more complex representation, especially when the system has many states. It is recommended that Markov analysis be used when fault tree or dependence diagrams are not easily usable, namely to take into account complex transition states of systems which are difficult to represent and handle with classical fault tree or dependence diagram analysis.
- **Common Cause Analysis**. The acceptance of adequate likelihood of Safety critical Event is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense and specific studies are necessary to ensure that independence can either be assumed or deemed acceptable.
  - ***Zonal Safety Analysis***. This analysis has the objective of ensuring that the equipment installations within each zone of the railway system are at an adequate safety standard with respect to design and installation standards, interference between systems, and maintenance errors. In those areas where multiple systems or components are installed in close proximity, it should be ensured that the zonal analysis would identify any failure or malfunction which by itself is considered sustainable but which could have more serious effects when adversely affecting adjacent systems or components.
  - ***Particular Risk Analysis***. Particular risks are defined those events or influences, which are outside the systems concerned. Examples are fire, leaking fluids, uncontained failure of high energy operating machines, adverse weather conditions, etc. Each risk should be the subject of a specific study to examine and document the simultaneous effects or influences, which may violate independence.

- ***Common Mode Analysis***. This analysis is performed to confirm the assumed independence of the events, which were considered in combination for a given Safety critical Event. The effects of specification, design, implementation, installation, maintenance, and manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered.

B.c Assessment Process by the RU and the ECM to identify and classify Safety critical Events

The safety assessment process is a methodical and systematic manner, which addresses the above methods and ensures that the whole process and its findings are visible and readily assimilated.

1. ***Define the system and its interfaces***, and identify the functions that the system is to perform. Determine whether or not the system is complex, similar to other systems used, or conventional. Where multiple systems and functions are to be evaluated, consider the relationships between multiple safety assessments.

2. ***Identify and classify Safety Critical Events.*** All relevant engineering organizations, such as systems, structures, and tests should be involved in this process. This identification and classification may be done by conducting a Functional Hazard Assessment, which is usually based on one of the following methods, as appropriate:

   - If the system is not complex and its relevant attributes are similar to other already used systems, the identification and classification may be derived from design and installation appraisals and the service experience of the comparable, previously approved systems.
   - If the system is complex, it is necessary to systematically postulate the effects on the safety of the railway system and its occupants resulting from any possible failures, considered both individually and in combination with other failures or events.

3. ***Choose the means***. As it is mentioned, the depth and scope of the analysis depends on the types of functions performed by the system, the severity of system events, and whether or not the system is complex. **For significant events, experienced engineering and operational judgement, design and installation appraisals and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For more severe events, a very thorough safety assessment is necessary.**

4. ***Conduct the analysis and produce the data***. A typical analysis should include the following information to the extent necessary to show compliance:

   - A statement of the functions, boundaries, and interfaces of the system.
   - A list of the parts and equipment of which the system is comprised, including their performance specifications or design standards and development assurance levels if applicable. This list may reference other documents, such as manufacturer's specifications, etc.
   - The conclusions, including a statement of the Safety critical Events and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that Safety critical Events.
   - A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each Safety critical Event. It should also include a description of precautions taken against common-cause failures, provide any data such as component failure rates and their sources and

applicability, support any assumptions made, and identify any required on-board staff or maintenance staff actions.

5. ***Assess the analyses and conclusions of multiple safety assessments***.
6. ***Prepare the safety critical systems list.***

B.d Considerations by the RU and the ECM during the Assessment Process

Many considerations could arise from each phase of the Assessment Process concerning the reliability and the adaptability of the proposed process.

a. *Considerations when Assessing Effects*

The Safety critical Events classification intends to ensure an orderly and thorough evaluation of the effects on safety of foreseeable failures, errors or external circumstances, separately or in combination, involving one or more system functions. The severity of the events should be evaluated according to the effects on:

- the railway system
- staff members
- occupants

The interactions of these factors within a system and among relevant systems should be considered. In assessing the effects, factors, which might alleviate or intensify the direct effects of the initial Failure Condition should also be considered.

Regardless of the types of assessment used, the classification of Safety critical Events should always be accomplished with consideration of all relevant factors; e.g., system, staff, performance, operational, external

When assessing the consequences of a given event, account should be taken of the failure information provided, the complexity of the staff action, and the relevant staff training.

b. *Single Failure Considerations*

An analysis should consider that a single failure includes all set of failures, which are not independent from each other.

c. *Common Cause Failure Considerations*

An analysis should consider the application of the fail-safe design concept and give special attention to ensure the effective use of design and installation techniques that would prevent single failures or other events from damaging or otherwise adversely affecting:

- more than one redundant system channel
- more than one system performing operationally similar functions, or
- any system and an associated safeguard.

d. *Analysis Considerations*

The maximum allowable probability of the occurrence of each event is determined from the event's effects, and when assessing the likelihood of event appropriate analysis considerations should be accounted for. Any analysis must consider:

(i) Possible Safety critical Events and their causes, modes of failure, and damage from sources external to the system.

(ii) The likelihood of multiple failures and undetected failures.

(iii) The likelihood of requirement, design and implementation errors.

(iv) The effect of reasonably anticipated staff errors after the occurrence of a failure or Safety critical Event.

(v) The effect of reasonably anticipated errors when performing maintenance actions.

(vi) The staff alerting cues, corrective action required, and the capability of detecting faults.

(vii) The resulting effects on the railway system and the occupants, considering the operating and environmental conditions.

e. *Calculation of Average Probability per Operational Hour (Quantitative Analysis).*

The Average Probability per Operational Hour is the probability of occurrence, normalized by the Operational time, of a Safety critical Event during the operation, which can be seen as an average over all operations of a system type. The calculation of the Average Probability per Operational Hour for a Safety critical Event should consider:

(i) the average operation duration and the average operation profile for the system type,

(ii) all combinations of failures and events that contribute to the Safety critical Event,

(iii) the conditional probability if a sequence of events is necessary to produce the Safety critical Event,

(iv) the relevant "at risk" time if an event is only relevant during certain phases,

(v) the average exposure time if the failure can persist for multiple times.

f. *Integrated Systems*

Interconnections between systems have been a feature of railway system design so it is recognized that requiring systems should be considered in relation to other systems.

Each system function should be examined with respect to other functions performed by the system, because the loss or malfunction of all functions performed by the system may result in a more severe events than the loss of a single function.

In addition, each system function should be examined with respect to functions performed by other railway sub-systems, because the loss or malfunction of different but related functions, provided by separate systems may affect the severity of events postulated for a particular system.

Providing the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be shown through a series of system safety assessments, each of which deals with a particular events (or more likely a group of events) associated with a system and, where necessary, takes account of failures arising at the interface with other systems.

However, where the systems and their interfaces become more complex and extensive, the task of identifying and classifying Safety critical Events may become more complex. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of test which must be accomplished. It is therefore essential that the means of compliance are considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy.

Experienced engineering and operational judgement should be applied when determining whether or not a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems attributes should be considered; however, the complexity of the software and hardware need not be a dominant factor in the determination of complexity at the system level, e.g., the design may be very complex, such as a satellite communication system, but its function may be fairly simple.

g. *Operational or Environmental Conditions*

A probability of one should usually be used for encountering a discrete condition (severe icing, lighting strike, high energy rejected, fire in engine, etc.) for which the system is designed. However, a guidance should be compiled which will contain allowable probabilities, which may be assigned to various operational and environmental conditions for use in computing the average probability per operational hour of events resulting from multiple independent failures, without further justification. This guidance is not intended to be exhaustive or prescriptive.

At this time, a number of items have no accepted standard statistical data from which to derive a probability figure. However, these items could be included for either future consideration or as items for which the NSA/railway actors may propose a probability figure supported by statistically valid data or supporting service experience. The NSA/railway actors should have the opportunity to propose additional conditions or different probabilities provided they are based on statistically valid data or supporting service experience. When combining the probability of such a random condition with that of a system failure, care should be taken to ensure that the condition and the system failure are independent of one another, or that any dependencies are properly accounted for.

General, the conditions under which the installed equipment will be operated should be equal to or less severe than the environment for which the equipment is qualified. The proper or not functioning of equipment, systems, and installations under the operating and environmental conditions approved for the railway system may be shown by test and/or analysis or reference to comparable service experience on other systems.

h. *Justification of Assumptions, Data Sources and Analytical Techniques*

Any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault in dependence, and limitation of analytical methods, processes, and assumptions.

The justification of the assumptions made with respect to the above items should be an integral part of the analysis. Assumptions can be validated by using experience with identical or similar systems or components with due allowance made for differences of design, duty cycle and environment. Where it is not possible to fully justify the adequacy of the safety analysis and where data or assumptions are critical to the acceptability of the event, extra conservatism should be built into either the analysis or the design. Alternatively any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions are insensitive to that uncertainty.

i. *Operational and Maintenance Considerations*

On-board staff and maintenance tasks should be appropriate and reasonable. However, quantitative assessments of staff errors are not considered feasible. Therefore, reasonable tasks are those for which full credit can be taken because they can realistically be anticipated to be performed correctly when they are required or scheduled. In addition, based on experienced engineering and operational judgement, the discovery of obvious failures during normal operation or maintenance of the system may be assumed, even though identification of such failures is not the primary purpose of the operational or maintenance actions.

Credits may be taken for both qualitative and quantitative assessments:

- ✓ if the evaluation indicates that a potential Safety critical Event can be alleviated or overcome without jeopardizing other safety related staff tasks and without requiring exceptional skill or strength
- ✓ for correct staff performance of the periodic checks required to demonstrate compliance, provided overall staff workload during the time available to perform them is not excessive and they do not require exceptional skill or strength (rational methods, which usually involve quantitative analysis, or relevant service experience should be used to determine check intervals).
- ✓ for correct accomplishment of reasonable maintenance tasks

In case of unsafe system operating conditions, information by installed supporting systems and controls must be provided to the crew to enable them to take appropriate corrective maintenance action. When assessing the ability of the staff to cope with a Safety critical Event, the information provided to the staff and the complexity of the required action should be considered.

C. Conclusions

In accordance to this report we could conclude that:

- Safety criticality could vary among the Member States.
- A harmonized safety critical component list throughout EU is not feasible.
- A process approach in the EU, based on identifying and classifying the severity and frequency of the safety critical events of the systems, conducted by RU and ECM is preferable.
- Harmonized terms of severity and frequency classification and the respective quantitative probabilities of each level of frequency should be proposed for the railways.
- The proposed taxonomy of the railway system is a suggestion of the level of analysis to consider the failures and then decide the classification of an event.
- After the completion of the process, a temporary safety critical components list could be proposed for each railway (sub) system as next step.
- This list could contribute to the preparation compliance statements, maintenance requirements, and manual requirements in order to minimize the Safety critical Events and improve the level of railway safety

Finally, taking everything into consideration it could be inferred that safety criticality approach is closely related not only with the systems but also with the human's performance. Multi-disciplinary teams should be assigned in order to identify and classify significant Safety critical Events by taking into account not only the probable failures but also the operational and maintenance procedures which contribute to the limitation of the failures.

Annex 1 Taxonomy of the railway systems proposed by ERA

ROLLING STOCK

Freight Wagons

- Running Gear
  - Wheel
  - Suspension
  - Axles boxes/bearing
  - Axles
  - Bogie frame
- Braking
- Buffing and draw gear
- Car body
- Wagon superstructure

Locomotives

- Car body
  - Car body shell
  - Crash energy absorption
  - Aerdynamic system
  - Windows
  - Windscreen
- Doors
  - Interior doors
  - Exterior doors
- Guidance
  - Running gear
  - Runnning gear connection
  - Running gear auxiliary components
- Interiors
  - Compartments
  - Toilet/Sanitary System
  - Heat-Ventilation-Air conditioning
  - Driver's cab
- Lighting
  - Interior lighting
  - Exterior lighting
- Energy supply
  - Main energy
  - Auxiliary energy
  - Energy storage system
- Propulsion and Braking
  - Propulsion
  - Braking
- Information and communication
  - On-board train communication
  - On-board train infromation
  - Train external communication
- Train control
  - Train Control and Monitoring System (TCMS)
  - Automatic Train Control (ATC)

- Coupling and interconnection
    - Consist coupling
    - Vehicle coupling

Passenger coaches

- Car body
    - Car body shell
    - Crash energy absorptio
    - Aerodynamic system
    - Windows
    - Windscreen
- Doors
    - Exterior doors
    - Interior doors
    - Boarding aids
- Guidance
    - Running gear
    - Running gear connection
    - Running gear auxiliary components
- Interiors
    - Floors and stairways, vestibules
    - Compartments
    - Toilet/ sanitary system
    - Ctering/ Gallery
    - Heat-Ventilation-Air conditioning
    - Driver's cab
- Lighting
    - Interior lighting
    - Exterior lighting
- Energy supply
    - Auxiliary energy
    - Energy storage system
- Braking
- Information and communication
    - On-board train communication
    - On-board train infromation
    - Train external communication
- Coupling and interconnection
    - Consist coupling
    - Vehicle coupling
    - Gangway

On-track machines

- Car body
    - Car body shell
    - Crash energy absorption
    - Aerdynamic system
    - Windows
    - Windscreen
- Doors
    - Interior doors

        - Exterior doors
        - Loadind system
    - Guidance
        - Running gear
        - Runnning gear connection
        - Running gear auxiliary components
    - Interiors
        - Floors and stairways, vestibules
        - Compartments
        - Toilet/Sanitary System
        - Heat-Ventilation-Air conditioning
        - Driver's cab
    - Lighting
        - Interior lighting
        - Exterior lighting
    - Energy supply
        - Main energy
        - Auxiliary energy
        - Energy storage system
    - Propulsion and Braking
        - Propulsion
        - Braking
    - Train control
        - Train Control and Monitoring System (TCMS)
        - Automatic Train Control (ATC)
    - Coupling and interconnection
        - Consist coupling
        - Vehicle coupling
        - Gangway

Multiple units

    - Car body
        - Car body shell
        - Crash energy absorption
        - Aerdynamic system
        - Windows
        - Windscreen
    - Doors
        - Interior doors
        - Exterior doors
        - Loadind system
    - Guidance
        - Running gear
        - Runnning gear connection
        - Running gear auxiliary components
    - Interiors
        - Floors and stairways, vestibules
        - Compartments
        - Toilet/Sanitary System
        - Heat-Ventilation-Air conditioning
        - Driver's cab

- Lighting
  - Interior lighting
  - Exterior lighting
- Energy supply
  - Main energy
  - Auxiliary energy
  - Energy storage system
- Propulsion and Braking
  - Propulsion
  - Braking
- Information and communication
  - On-board train communication
  - On-board train infromation
  - Train external communication
- Train control
  - Train Control and Monitoring System (TCMS)
  - Automatic Train Control (ATC)
- Coupling and interconnection
  - Consist coupling
  - Vehicle coupling
  - Gangway

INFRASTRUCTURE

- Rail
- Weldings
- Sleepers
- Fastening Systems
- Insulated Rail Joint
- Switches & Crossings
  - Switch Blade
  - Crossing
  - Point System
  - Bearers
- Expansion devices

ENERGY

- Overhad contact line (OCL0
  - Mast
  - Wire
  - Contact wire
  - Tensioning device
  - Cantilever
  - Registration tube
  - Steady arm
  - Insulator
  - Low voltage limiter
  - Clamp
- Power supply
  - Transformer
  - Main braker

- Disconnector
- Protection suystem
- Rectifier
- Converter
- Filter
- Battery
- Insulator
- Low voltage limiter
- Cable
- Surge arrester
- SCADA system

ON- BOARD CCS (CCS)

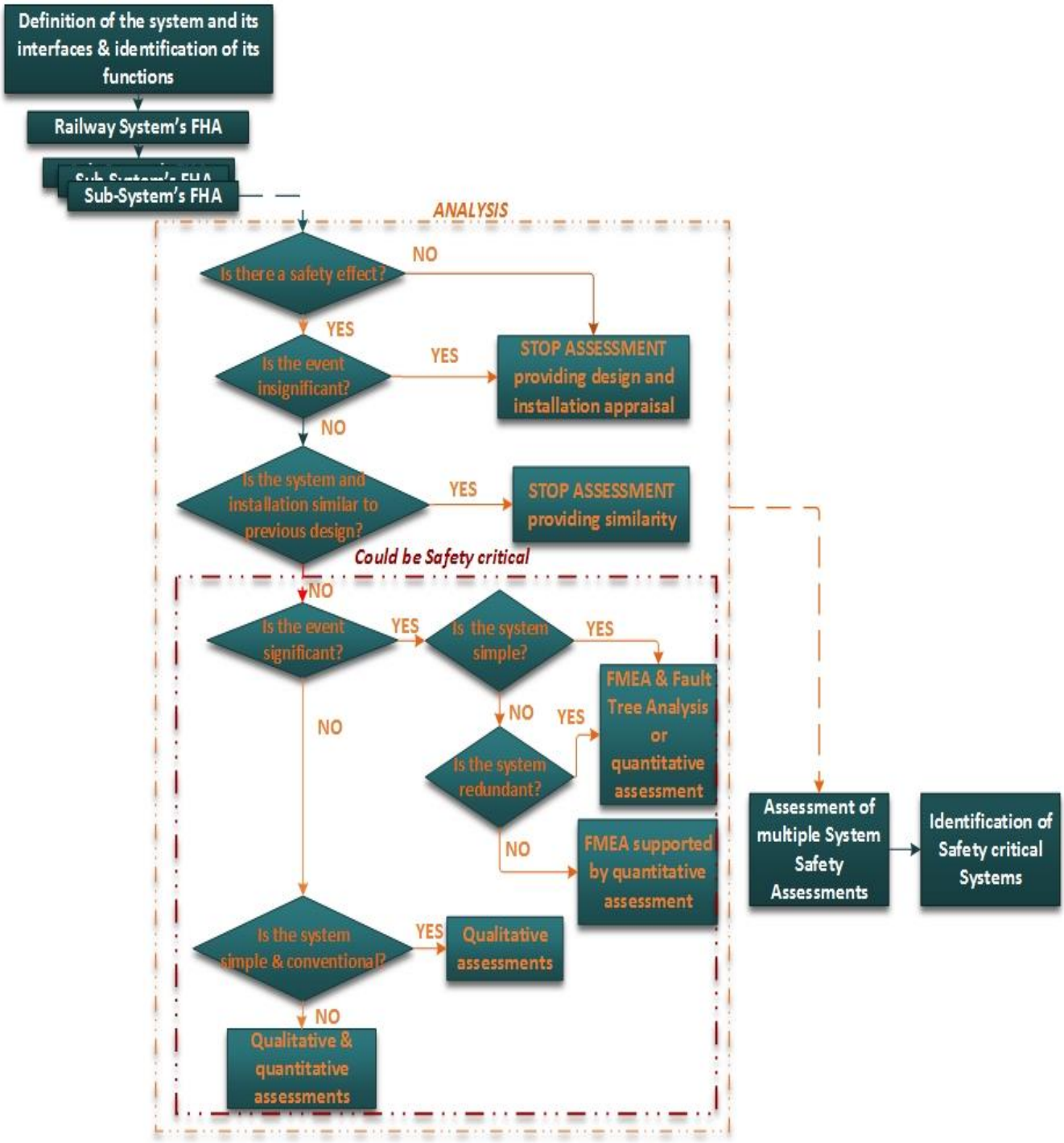
- GSM-R Onboard Voice
  - Antenna
  - Terminal
  - Driver Machine Intreface- DMI
- GSM-R Onboard Date
  - Antenna
  - ETCS Data Only Radio- EDOR
- ETCS Onboard
  - European Vital Computer – EVC
  - Diver Machine Interface – DMI
  - Balise Transmission Module – BTM
  - Loop Transmission Module – LTM
  - Specific Transmisiion Module – STM
  - Odometer

TRACKSIDE CCS (CCS)

- GSM-R Trackside Voice/Data
  - Dispatcher Terminl
  - Base Station (Base Tranceiver Station – BTS/ Base Station Controller- BSC)
  - Mobile Switching Centre- MSC
- ETCS Trackside
  - Eurobalise
  - Euroloop
  - Lineside Electronic Unit – LEU
  - Radio Block Center- RBC
- Train detection equipment
  - Axle Counter (Head/Comparator)
  - Track Circuit

Annex 2 Assessment Process Flowchart

The following identifies the depth of analysis expected based on the identification and classification of a Safety critical Event, in other words which assessment methods should be chosen.



Safety effect: any condition which has a negative effect on the railway system and/or its occupants caused by one or more failures or errors.

Redundant system: an additional independent system which accomplish a given function.

Conventional system: a system same or similar to another as far as its functionality, its technology and its intended usage.