EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Report

<Safety critical components>

	Drafted by	*Validated by*	*Approved by*
Name	Jean-Marie DECHAMPS		Jean-Marie DECHAMPS
Position	HoS		HoS
Date	18/12/2017	Enter a date.	18/12/2017
Signature			

Document History

Version	*Date*	*Comments*
1.0	18/12/2017	Final

Content

1. Introduction and limitations

This report completes the preliminary report issued in 2016 (see annex II) and includes the results of Agency studies and discussions held with the National safety Authorities, Representative Bodies, the EU Commission and the working group 48 of CEN TC256.

Its scope includes Agency reflections and proposals related to:

- definition of safety critical components based on the effect of single failure ('approach by danger');
- maintenance principles related to role of designers/manufacturers and collaborative approach;
- feasibility of specific certification;
- a common EU list of safety critical components; and
- traceability and marking of safety critical components.

This report ends the 2017 Agency activities and aims to be submitted to a public consultation being part of an Agency proposal for an Implementing Act regarding the revision of ECM certification.
This consultation is intended to take place from December 2017 to February 2018.

This report concerns only the safety critical components on-board of railway vehicle (subsystems rolling-stock, CCS on-board and energy on-board). The Agency reflections will start by 2019-2020 for fixed installations (subsystems infrastructure, CCS fixed installations and energy)

2. Background

2.1. 4th railway package

Five references to 'safety critical components' have been found in the new legislation (4th railway package) Agency Regulation 2016/796 [1], Interoperability directive 216/797 [2] and Safety Directive 2016/798[3] (see also annex I):

The Agency Regulation 2016/796 [1] includes 1 reference:

REF1: "*CHAPTER 4: Tasks of the Agency relating to interoperability*
Article 19: Technical support in the field of railway interoperability
1. The Agency shall:…
(l) address, where appropriate, recommendations to the Commission in relation to safety-critical components."

Remark: The attention must be made on the difference but complementary with the art 19(k) related to Interchangeable Spare parts that states that:

> *"(k) address recommendations to the Commission in relation to harmonised standards to be developed by European standardisation bodies and standards relating to interchangeable spare parts which may improve the level of safety and interoperability of the Union rail system;"*

It is clear that both 'safety critical components' and 'interchangeable spare parts' are complementary in addressing safety. But one safety critical component may be at the same time an interchangeable spare part but it cannot be concluded that it is the case for all safety critical components and vice versa.

The duality safety critical component-interchangeable parts as well as the duality with interoperability constituents will not be discussed within this document.

The Interoperability Directive 2016/797 [2] includes 2 references:

REF2: "Consideration (67)…
The Commission should also report on actions taken regarding the identification and traceability of safety-critical components."

REF 3: "*ANNEX III: Essential requirements*
1. General requirements
1.1. Safety
1.1.1. The design, construction or assembly, maintenance and monitoring of safety-critical components, and more particularly of the components involved in train movements, must be such as to guarantee safety at the level corresponding to the aims laid down for the network, including those for specific degraded situations."

Finally the Safety directive 2016/798 includes also 2 references:

REF 4: "*CHAPTER VI: Transitional and final provisions*
Article 29: Report and further Union action
By 16 December 2017, the Commission shall report to the European Parliament and to the Council on the actions taken with a view to achieving the following objectives:
(a) the obligation for manufacturers to mark with an identification code the safety-critical components circulating on the European rail networks, ensuring that the identification code clearly identifies the component, the name of the manufacturer and the significant production data;
(b) the full traceability of the safety-critical components, the traceability of their maintenance activities and the identification of their operational life; and
(c) the identification of common mandatory principles for the maintenance of those components."

REF 5: "*ANNEX III Requirements and assessment criteria for organisations applying for an ECM certificate or for a certificate in respect of maintenance functions outsourced by an entity in charge of maintenance*
…
10. Maintenance activities — a structured approach to ensure:
— that all maintenance activities affecting safety and safety-critical components are identified and correctly managed and that all the necessary changes to those maintenance activities affecting safety are identified, properly managed based upon the return of experience and the application of Common Safety Methods for risk assessment in accordance with point (a) of Article 6(1) and properly documented;
…"

Following those 5 legal references, it is evident that there is no real clear definition or common understanding of safety critical components in the EU legislation.

However, REF3 specifies that safety critical components include but are not limited to components involved in train movements.

Therefore safety critical components may be as well components mounted on vehicles or on fixed infrastructure. Consequently safety critical components address all structural subsystems: Rolling stock, infrastructure, energy and CCS (on-board and fixed installations).

2.2. Mandate for revision of ECM certification

The European Commission addressed a mandate for the revision of ECM certification in 2015 completed by a letter received in 2016.

Regarding the safety critical components, the mandate addressed to the Agency requests in particular to:

- Identify common mandatory principles for the maintenance of the safety critical components (4th package);
- Examine the feasibility of the certification of entities and workshops specialised in the maintenance of specific critical components

3. Scope

This report, as part of the recommendation for an Implementing Act on the revision of ECM certification, address the following aspects

- Proposal of definition and common understanding of 'safety critical components' following the conclusion of section 2.1 here above (section 5).
- Proposal of common maintenance principles (section 6).
- Feasibility of certification of entities and workshops specialised in the maintenance of specific critical components (section 7).

In addition to that this report address also the following aspects that could not be dissociated from maintenance

- Establishment of a European common list of safety critical components (section 8).
- Issues with the traceability and marking of safety critical components (section 9).

Finally the Agency makes some proposals for further steps (section 10).

Limitation

The development in this document will only be related to safety critical components on board of railway vehicles so affecting only the subsystems rolling stock, energy and on-board CCS. The development for fixed installations will be the object of future Agency work starting in 2019-2020.

4. Activities performed by the Agency in 2017.

After the preliminary activities in 2016 concluded by a preliminary report "*Revision of the ECM certification Preliminary Phase …Part 2: Safety critical components* " of 20 December 2016 (ref 007 REC1004 v0.1 or see annex II of this report), the Agency continued to work on safety critical components within the project of issuing a recommendation on revision of ECM certification.

In particular the topic was discussed in 2 working party meetings on 23 May 2017 and 25 October 2017.

After the first meeting of the working party, the Agency received also inputs from 3 NSAs participating in the working party: Germany, Netherlands and Norway and 2 RBs participating in the working party: UIP and UNIFE.
After the second working party meeting, the Agency received a contribution of CEN TC256-WG48 on 01 December 2017.

The Agency issued two working papers:

- 24 June 2017, Report on "Safety Critical Components" in railways - The concept of "Safety Criticality" of the systems.
- 06 October 2017, working paper prior to the 2nd working party meeting on 25 October 2017. For this documents, the agency received 39 comments from 4 National Safety Authorities, 3 Representative Bodies and 1 ECM Certification Body.

The Agency got bilateral meetings with UNIFE on 08 September 2017 and CER on 08 December 2017.

The Agency participated also to several events where safety critical components were discussed:

- A meeting of OTIF WG TECH (technical working group- meeting 32) on 13 September 2017
- Several meeting with DG MOVE to coordinate the activities as the European Commission had to issue a report to the European Parliament in application of the article 29 of the Safety directive 216/798 (see REF 4 in section 2.1).
- the RISC meeting on 15 November 2017 (RISC Railway Interoperability and Safety Committee)
- The NRB meeting on 27 November 2017 (NRB Network of Representative Bodies)

5. Proposal of definition and common understanding of "safety critical components"

5.1. What is a component?

As it is evident that there is no real clear definition or common understanding of safety critical components (see section 2.1) in the EU legislation and following the report in the annex II of this report, the Agency confirms its approach to consider widely the term 'component'.

The functions ensured by vehicles such as traction, braking, guiding the vehicle or the train, doors management are materialised by technical systems for which their architecture is more or less complex, calling more or less to innovative solutions or new technologies.

The technical systems are composed on basic or elementary elements interconnected. Those basic or elementary elements are called components and connections.

The agency proposes in a large approach that the term 'component' in 'safety critical component' within the EU railway legal framework means:

- A technical system performing a function; or
- A technical subsystem performing a subfunction when the combination of subfunctions cover a function; or
- An individual (basic) component when it is convenient for systems with low complexity. Mainly for mechanical systems.
- Softwares should also be considered as component.
- Materials, tools and equipments used in maintenance

According to EN15380-2 (§3.10), a component is "uniquely identifiable product that is considered indivisible for particular planning or control purpose and/or which cannot be disassembled without it being destroyed". This definition, in the Agency approach, address the 'individual (basic) component as stated in preceding paragraph.

For the software, there are still discussions as the control of development and performance of software relies already on existing international standards. But a priori 'software' are kept in the definition.

5.2. Definition of "safety critical component"

The preliminary report of 2016 (annex II of this report) stated that there are many different approaches to define and evaluate the criticality of components and technical systems: as examples:

- Criticality based on danger.
- Criticality based on safety risks.
- Approach based on FMECA.
- Criticality associated to maintenance.

Therefore a choice for a common approach must be made.

5.2.1. Various approaches

There are various approaches in the industry including civil aviation. The Agency analysed more in detail the civil aviation as well as the French initiative for identification and management of safety critical components related to fixed installations.

5.2.1.1. Civil aviation

The specifications for large aeroplanes and their technical systems are compiled in the CS25 ('Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes')

The CS25.1309 Equipment, systems and installations (book 1 page 165) states that

"…

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that:

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) (ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote."

The AMC 25.1309 = Acceptable Means of Compliance completing the CS25.1309 (pages book 2 pages 679-709) states the definitions

- Major: Failure Conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

- Hazardous: Failure Conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating, conditions to the extent that there would be:
    - (i) A large reduction in safety margins or functional capabilities;
    - (ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
    - (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

- Catastrophic: Failure Conditions, which would result in multiple fatalities, usually with the loss of the aeroplane. (Note: A "Catastrophic" Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)

- Remote Failure Conditions are those unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type. (There is a link with probabilities book 2 page 687)

- Extremely Remote Failure Conditions are those not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type. (There is a link with probabilities book 2 page 687)

- Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type. (There is a link with probabilities book 2 page 687)

The AMC 25.1309 explained also the exceptions to which the CS 25.1309 do not apply:

- **Control systems** regulated by CS25.671: 25.671(c)(1) and CS 25.671(c)(3). Consideration of single failure regardless any probability. **= approach by danger**
-
- **CS25.735: Braking system**. The reason concerns the brake system requirement that limits the effect of a failure to doubling the brake stopping distance. This requirement has been shown to provide a satisfactory level of safety without the need to analyse the particular circumstances and conditions under which the single failure occurs. Mitigation measure to doubling stopping distance is considered as sufficient. **The level of degraded performance is fixed.**

- CS25.810 and 812: Egress and lighting for evacuation. The failure conditions associated with these cabin safety equipment installations are associated with varied evacuation scenarios for which the probability cannot be determined. It has not been proven possible to define appropriate scenarios under which compliance with CS 25.1309(b) can be demonstrated. It is therefore considered more practical to require particular design features or specific reliability demonstrations and except these items of equipment from the requirements of CS 25.1309(b). Traditionally, this approach has been found to be acceptable**. Rule-based approach**

Key aspects:

- Civil aviation approach is based on analysis of safety risks but:
    - For some technical systems, it is replaced by an approach by danger
    - For some technical systems, requirements are fixed on degraded performance (e.g. braking system) or design features (e.g. evacuation systems)

- Civil aviation does not consider only technical systems and components isolated but also in relation between each other.
- Civil aviation does not consider components on an isolated way as such but defines acceptability for technical systems and components.
- Civil aviation does not seem to impose the concept of safety critical components but have specific requirements for specific technical systems.

The Agency issued also a report on applicability of this method to railway. This report may be found in annex III of this report. In the mind of the Agency this method should be implemented within the railway system at middle term.

5.2.1.2. French approach for infrastructure

In France there are 16 infrastructure managers, some are new in the railway system and then have little experience and only access to too few data for performing risk analysis/assessment on the base of historical records.

There was a need identified for a common practical method to be implemented so that each Infrastructure Manager can adopt it according to its personal understanding and its specific environment.

To define this common method, the French National Safety Authority, EPSF, set up a working group beginning of 2017 to answer the following questions:

- Definition of a "safety-critical component"?
- Process to determine if a component is safety-critical or not?
- Need for a common safety-critical component list?
- Fields to be considered in the safety-criticality analysis? (environment, passengers, workers, others, …)

The adopted definition is "*A safety-critical Component is any component :*

- *for which single failure leads directly to a hazard which results in an accident with a seriousness ≥ 3 (EPSF scale of seriousness for safety events) in the hypothesis specified below; or*
- *for which contribution can be considered indisputable in the reduction of risks*.

  Note
  - Seriousness ≥ 3 means Event that might have had isolated human consequences (1 or 2 persons injured and hospitalised for less than 24 hours or 1 fatality)
  - The accident must affect passengers, environment, others (third parties), workers only if the danger is not considered as part of their mission (i.e. associated to occupational risk assessment regulated at national level)
  - « hazard » means '*a condition that could lead to an accident*' as defined in Regulation n°402/2013 on the common safety method for risk evaluation and assessment;
  - The probability of presence of a train is equal to 1 and other events can be considered with a probability equal to 1 depending on the environment
  - mitigation measures are not taken into account"

By application of a common process and a common definition to identify safety critical components, the Infrastructure Managers may have different safety-critical component lists depending on railway network specificities (design, environment, safety objectives,…), maintenance context, pattern of operations (type of trains, frequencies) and its monitoring return.

This do not cause any problem to the French NSA that considers that a list of components is not "an end in itself" as the most important is how safety-critical components are taken into account in the Safety Management System of the infrastructure Manager and more specifically in the projects' life cycle.

The complete method should be published by the French National Safety authority beginning of 2018 as an acceptable means of compliance.

5.2.2. Proposal of a definition

The Agency proposes to identify the safety critical components on the base of 'criticality by danger' as described in the previous Agency report (see annex II).

As common definition, the Agency proposes:
"*Safety critical components means any component for which single failure has a credible potential to lead directly to a catastrophic accident".*
Note 1: Accidents are derailment, collisions, and other accidents to persons caused by vehicles in motion, fire or other.
Note 2: Catastrophic is related to multiple fatalities. The most credible unsafe consequence of the failure must be taken into account
Note 3: The safety critical components are components meeting the definition here above and constituting of:

- For locomotives and passenger rolling stock, the elements of the rolling stock subsystem corresponding to the essential requirement related to safety in section 3.1. of COMMISSION REGULATION (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock— locomotives and passenger rolling stock' subsystem of the rail system in the European Union. Including amendments. I.e the 'Loc and Pas TSI'
- For freight wagons, the basic parameters corresponding to the essential requirement safety in table 1 of section 3. of REGULATION (EU) No 321/2013 of 13 March 2013 concerning the technical specification for interoperability relating to the subsystem 'rolling stock — freight wagons' of the rail system in the European Union and repealing Decision 2006/861/EC. Including amendments. I.e. the 'Freight wagon TSI'"

For instance to illustrate the definition, a suspension spring (running gear) may be considered, depending on the chosen suspension architecture, as safety critical or not. A broken spring may, under specific suspension design, lead to such instabilities that the vehicle derails while in other design, only a reduction of comfort may be identified. In the first case, the spring is safety critical, not in the second case.
In that analysis no consideration of probability/frequency of occurrences appears.

Justification of the proposal

Considering that:

- It has been observed that formal risk management, in particular risks assessment, remains a weak point within the EU railway system. For instance, in 2017, the Agency published a report on the evaluation of the implementation of the CSM on monitoring (Regulation 1078/2012) for the period 2013-2016 where it appears that only 30% of stakeholders have understood and implemented the method. In 2018, the Agency will perform an evaluation on the implementation of the CSM on risk assessment and evaluation (Regulation 402/2013).
- The process approach based on risk assessment in use in civil aviation seems to be particularly demanding in term of competence (see annex III of this report)

- Consequently, in a first step, adopting a risk-based definition grouping frequency of occurrences and gravity/severity of effects similar to what exists in civil aviation is premature and would only lead to endless discussions.
- The French experience as described in the section 5.2.1.2. here above.

The Agency considers then that, in a first step, the concept of safety critical components must be restrictive:

- To be understood by any railway interested actor.
- To provide an added value. It is reminded also that if every component is safety critical, nothing is safety critical. And
- To avoid unwanted economic effects i.e. avoid undue increase of costs for the railway sector.

Therefore the Agency proposes to start with the above definition focusing only on the gravity/severity of effects caused by failures of components.

However, as competence of railway actors in risk management should grow in the following years, a new reflection on the definition should take place to converge with other industry ways. The Agency does not expect the EU railway be ready before 2021 (to be confirmed by further evaluations).

6. Maintenance

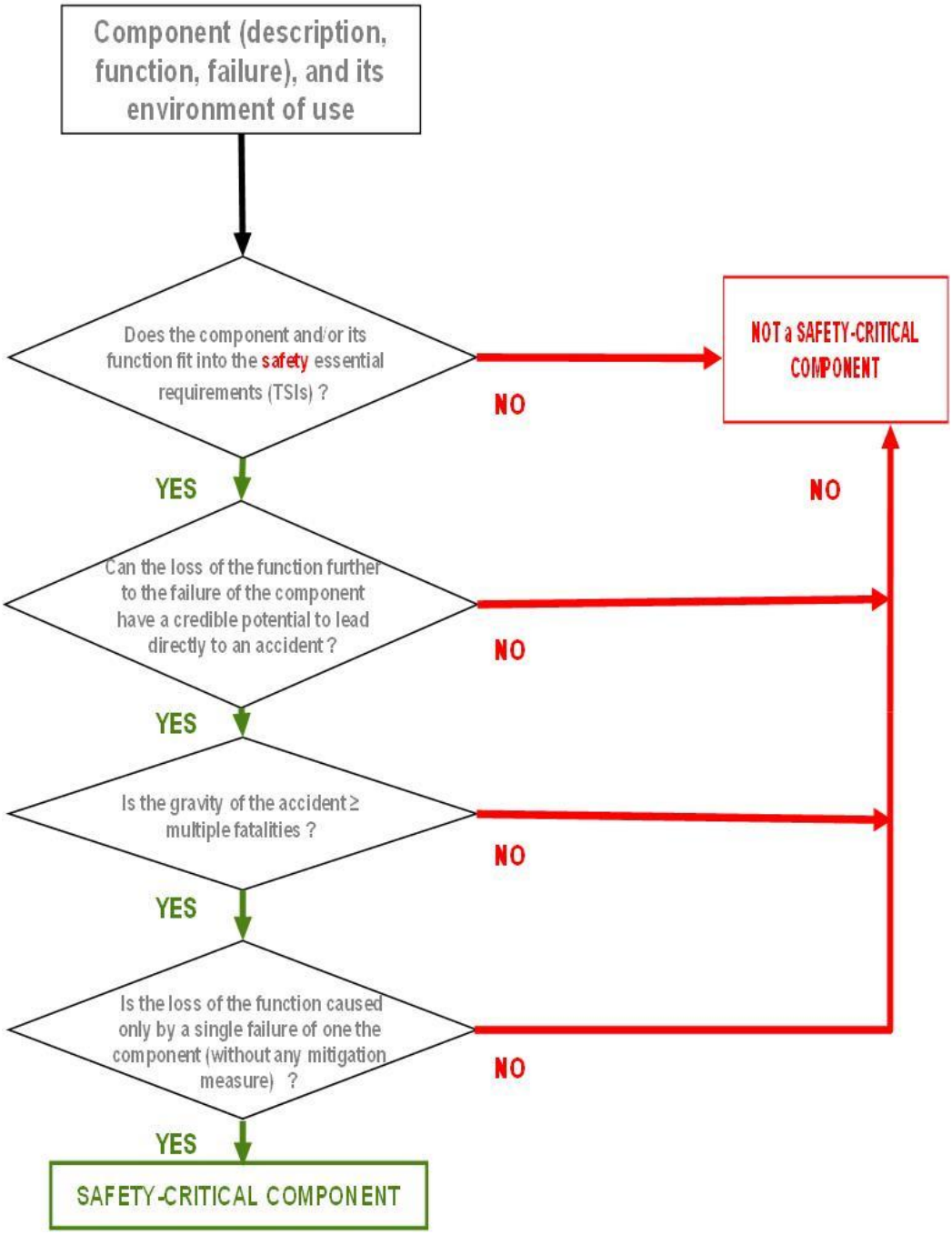
6.1. Initial identification of the safety critical components

As the criticality of a component depends on the design of the technical system in which it is incorporated and therefore of the design of the vehicle, the initial identification of safety critical components should start at the level of the design process and of the definition of manufacturing processes.

The designers/manufacturers should then have a process in place to identify the safety critical components in conformity with the above definition. This process should include a systematic risk analysis of all components in line with the annex I of the Commission Regulation 402/2013 and when applicable the relevant provisions related to (safety) requirements capture in the future adopted [1]*Implementing Regulation establishing practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process pursuant to Directive (EU) 2016/797 of the European Parliament and of the Council*.

The questions for the process for identification could also be summarized in the following flowchart:

[1] This implementing regulation has got a favourable opinion from Member States in November 2017 and will be formally adopted by the EU Commission in early 2018.



Remark: This flowchart can be added as new annex in the recommended Implementing Act for revision of ECM certification or in future guidance documents.

In the design and manufacturing of new or modified vehicles, the designers/manufacturers of the vehicles as well as any designers/manufacturers of the incorporated technical systems and components should collaborate.

For ensuring the level of safety of the railway system, it is crucial that the designers/manufacturers should also identify the control measures associated to the identified safety critical components and to communicate to RUs and ECMs those exported constraints related to maintenance and operations.
For the subsystem 'rolling stock', this communication should be performed by means of the documentation to be provided in accordance with:

- For locomotives and passenger rolling stock, sections 4.4 and 4.5 of COMMISSION REGULATION (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock— locomotives and passenger rolling stock' subsystem of the rail system in the European Union. Including amendments. I.e the 'Loc and Pas TSI'
- For freight wagons, sections 4.4 and 4.5 of the REGULATION (EU) No 321/2013 of 13 March 2013 concerning the technical specification for interoperability relating to the subsystem 'rolling stock — freight wagons' of the rail system in the European Union and repealing Decision 2006/861/EC. Including amendments. I.e. the 'Freight wagon TSI'

The designers/manufacturers should explain/justify in the provided documentation the credible potential to lead directly to a catastrophic accident of single failures of the identified safety critical component.

However in the working party meeting on 25 October 2017, it was highlighted that the documentation provided by designers/manufacturers could be strongly improved. The Agency is sensitive to this aspect also considering that documentation improvements can support also the collaboration between RUs, ECMs and designers/manufacturers. The Agency would then propose to set up a specific working group composed of railway sector experts under the umbrella of the Joint Network Secretariat and in collaboration with the CEN TC 256 WG 48.

6.2. Continuous identification all along the lifecycle of the vehicle.

6.2.1. General case

Because the designers/manufacturers can make mistakes or omissions in initial design due to insufficient knowledge of long term behavior of components in particular for innovative solutions or use of new technologies, they should also be able to revise the identified safety critical components

To this end the manufacturers should get information on how the vehicles are operated and maintained. It includes the reporting of occurrences of failures.
There is then a duty to ECMs and RUs to communicate, to the designers/manufacturers, the occurrences of failures and operational/maintenance measures that have been taken by them.

The designers/manufacturers, ECMs and RUs have therefore to implement the following processes:

- Designers/Manufacturers identify safety critical components all along the lifecycle (from initial design/manufacturing to end-of-life) and communicate in providing relevant operational/maintenance documentation. This is proposed to be stated in the implementing act revising the Commission Regulation 445/2011 or in further guidance document.

- ECMs develop maintenance files on the base of provided documentation as it is stated in the article 14 and annex III of Directive 2016/798 and in the annex III of Regulation 445/2011. I.e. the activities under the function called Maintenance Development.

- RUs implement internal operational rules on the base of provided documentation through the application of their SMS.

- RUs report to ECMs on in-operation detected failures and implemented operation control measures in application of the article 5 of the Regulation 445/2011. As this regulation address only freight wagons, this is proposed to be stated in the implementing act revising the Commission Regulation 445/2011 for all vehicles or in further guidance document.

- ECMs report to designers/manufacturers on detected failures, operational and maintenance control measures that have been taken. I.e. the Return on Experience. It is proposed to be stated in the implementing act revising the Commission Regulation 445/2011 for all vehicles

- Designers/manufacturers support ECMs and RUs on technical and engineering aspects. This is crucial for complex technical systems and application of new technologies to ensure clear and effective understanding by ECMs and RUs. It is proposed to be stated in the implementing act revising the Commission Regulation 445/2011 for all vehicles or in further guidance document

Remark. Similar to the previous section, the designers/manufacturers of the vehicles as well as any designers/manufacturers of the incorporated technical systems and components should collaborate.

6.2.2. Modification of vehicles

In case of modification of vehicles, the entity that will be entitled to manage the modification:
- is the designer/manufacturer or will assign the designer/manufacturer; and
- has to ensure the update of the identified safety critical components.

This process should be aligned to what is described in section 6.1. here above.

The collaboration with RUs and ECMs as described in the previous section 6.2.1. will have to be ensured by the entity that will be entitled to manage the modification and the assigned designer/manufacturer.

6.3. Specific requirements for Entities in Charge of Maintenance

The annex III of the Regulation 445/2011 have addressed the identification and management of safety critical components since 2011 in the following requirement:

> *"II.* ***Requirements and assessment criteria for the maintenance development function***
> *1. The organisation must have a procedure to identify and manage all maintenance activities affecting safety and* ***safety- critical components****."*

This requirement has been made applicable to all vehicles within the annex III of the Directive 2016/798. See REF 5 in section 2.1. of this report.

The concept of safety critical components have never been detailed as the common approach was that the ECM has to identify criticalities by observing and analysing the detected failures on the maintained vehicles. Following this identification, the ECM has to develop and implement maintenance control measures to ensure that the vehicle may be continuously used safely. For instance maintenance control measures may be additional inspections, change in inspection scheme, anticipation of replacement of components,…

In addition to that the Agency proposes also that those requirements applies to all components responding to the proposed definition in section 5.2.2. of this document.

The Agency proposes also to develop a specific guide addressing the ECM requirements stated in this section as well in preceding section 6.2. after the adoption of the Implementing Act revising the certification of ECMs.

7. Feasibility of certification of entities and workshops specialised in the maintenance of specific critical components

As seen its modular approach already expressed in the Commission Regulation 445/2011 and its applicability to certify maintenance workshops as well as any provider of maintenance services (to ECMs), the existing certification framework can be extended easily to providers specialised in maintenance of any component and in particular to safety critical components.

Easily the ECMs may require to their contractors/partners specialised in the maintenance of components to be certified against the EU harmonised certification framework.

In case of specific needs, the Agency may support the development and implementation of adequate accreditation and related certification schemes.

At this point the Agency considers that no urgent development is needed but clarifying the modular approach within the recommendation for an Implementing Act on the revision of ECM certification.

8. Establishment of a European Union common list of safety critical components

Several authorities are in favor of having an EU list of safety critical components while other authorities and railway actors do not see any added value to have it.

To try to get out of this, the Agency reflected to a SWOT[2] analysis for which the results are presented here below:

Strengths:

What is the added value of a list of Safety Critical Components?

The Agency identified two aspects for which an interest may be demonstrated:

- **Education**
  Managing safety is a crucial railway aspect. Having a common list may be useful to train railway staff including all levels of management by attracting the attention on key safety issues.
  In addition it may help all actors and in particular the smallest ones only acting at local level to understand the main concerns related to the safety of the railway system.

- **Interoperability**.
  National mandatory lists must be excluded as they will impair interoperability of vehicles by raising new barriers or add costs by the intermediate of maintenance.

Opportunities

The Agency identified two opportunities:

- **Collaborative approach**
  Even if collaboration within the railway sector is growing, for instance through the issue of EN standards by CEN/CENELEC, it remains low between operational actors such as ECMs and RUs.
  To issue an EU list of safety critical components, railway actors should have to collaborate by putting in common their information on reported failures of components and developing a common view. Also analysis of accidents, on recurrent failures and safety performances should have an added value. This exercise may support the need of more transparency and more collaboration within the railway sector.

[2] SWOT = Strengths, Weaknesses, Opportunities, Threats

- **Development of railway sector skills related to risk management**
  It has been observed that formal risk management remains a weak point within the EU railway system. For instance, in 2017, the Agency published a report on the evaluation of the implementation of the CSM on monitoring (Regulation 1078/2012) for the period 2013-2016 where it appears that only 30% of stakeholders have understood and implemented the method. For information, in 2018, the Agency will perform a new evaluation on the implementation of the CSM on risk assessment and evaluation (Regulation 402/2013).
  The process to issue an EU list will imply to define and discuss elements of the system under assessment i.e. system definition, hazard identification, failures and gravity/severity of effects of those failures. This could help to train railway actors to those first steps of an effective risk management.

- **Developing future designed targets related to components**
  The railway system may need additional harmonized design targets for a better efficiency. Frequencies of failures as well as gravity/severity of effects should also be considered in the process of identification and management of components. The experience gained in issuing a list of safety critical components in consistency with the definition of section 5.2.2. of this document could be a first step to move to a more efficient risk-based approach similar to other industries.

Weaknesses and Threats:

However the Agency have identified important issues related to a common EU list of safety critical components:

- **Safety culture issue**: Railway actors will focus only on the existing list and will not proceed to systematic identification and management of all hazards and failures. This could particularly be the case for the smallest actors acting at local level. Therefore the risk management in consistency with the CSMs will not be functioning at optimal level.
- **Additional costs** for the railway system if the list is too demanding. Therefore there is a need of continuous monitoring and optimization. In particular those railway actors having developed a smart risk management system may see this list as an additional administrative burden without any added value.
- **No value if the list is not enough demanding**. Railway actors will have anyway to proceed to systematic identification and management of all hazards and failures. The cost for issuing and maintaining a list will be lost while the resources could be used for other activities or reducing the total cost of railway transport.
- **Reduction of the consideration on differences** in design, age, environment in which vehicles are used, pattern of operation and pattern of maintenance. This may strongly impair the development of new railway services that are in the heart of the EU railway legal framework.
- **Additional burden in case of innovation** for instance regarding permanent on-board continuous automatized monitoring system (digitalization) or failsafe components.
- **Divergence from the approach in other modes of transport** such as aviation or maritime and other industries leading to an “isolation” of railway. Consequently railway will not profit of some industrial improvements and advances (e.g. synergies, harmonisation of practices, harmonisation of common products and manufacturing processes) having the potential to decrease the railway costs.

Those aspects must be carefully taken into account in the development and revision of a list. This necessitates:

- The EU List must be based on robust evaluation where failures and effects are deeply described and justified;
- a robust impact assessment justifying the economic **added value** for the railway system;

- collaborative approach; and
- regular revision/optimisation.

If a consensus is achieved to attempt to develop a first list, the Agency proposes to use
- Either the CEN TC 256 WG 48.
- Either the Joint Network Secretariat to set up Task Forces of experts under the umbrella of the JNS normal procedure.

9. Issues with the traceability and marking of safety critical components

The ECMs has to record all analysis and decisions related to modification of maintenance plans when affecting the identified safety critical components. This should be done in the vehicle configuration file as defined in the annex III of the regulation 445/2011 or the annex III of the Directive 2016/798 (details in annex IV).

It can be understood that the ECMs has to ensure for safety critical components as well as for all components:
- The traceability of maintenance records and all reported failures.
- The traceability of the configuration of the vehicle i.e. the list of identified components on vehicle. It implies that the ECMs must have a system to identify which components are installed on which technical systems and on which vehicles. To do that they use in general serial numbers and sometimes specific markings.

Even if the Commission Regulation 445/2011 address only freight wagons, this maintenance good practise should apply to all vehicles. The Agency agrees to explicitly state this in the recommendation for an Implementing Act for revising the ECM certification or to explain in the guidance documents.

To ensure this traceability, there are:
- ECM internal systems for identifying and marking components
- Harmonised system as per for the wheelsets.

Today the Agency does not see any need to mark physically the safety critical components in addition to what exists because the configuration files of vehicles is maintained by the ECMs and that ECMs are clearly identified, at least within the national vehicle Registers maintained by MS authorities (in many cases the NSA). I
Therefore, in case of raised safety issue, the authorities may have access to those configuration files upon request.
Even if this access is not explicit in the legislation, the Agency agrees to complete, in the recommendation of an Implementing Act for revising the ECM certification, the article 9 ***Role of the supervision regime.***

Having seen in many occasions, inefficiency of ECMs to answer to authorities in reasonable delays, sometimes it may takes several days or weeks, the Agency considers that the ECMs should improve to be able to answer to authorities' requests in short delays, for instance in maximum 12 or 24 hours. The Agency proposes to fix this delay for answering any authorities' request within the article 9 ***Role of the supervision regime*** in the recommendation of an Implementing Act for revising the ECM certification

It may also be questioned if the physical marking is still useful today when many developments on digitalisation including interconnections of databases require investments from the railway actors.

Nevertheless as the subject of traceability and physical marking remains sensitive and that it remains that several MS, but not all of them, support physical markings for the safety critical components, the Agency would propose to proceed to an identification of the today practices and an economic and safety impact assessment in 2018-2019 as support to a further recommendation on traceability and marking of safety critical components.
The impact assessment should analyse:

- the State of the Art;
- the needs for additional physical markings on the base of:
  - risk based approach (justification only though transparent risk assessment); and
  - the economic benefits;
- the sustainability of additional costs and the economic and safety added values of any new proposal for harmonisation.

10. Further steps

Public consultation December 2017-February 2018

As stated in the introduction of this report, it aims to be submitted to a public consultation.
For a large public consultation, the Agency invites the Member States by intermediate of representatives in RISC, the National Safety Authorities, the Representative bodies, the National Investigation Bodies, the railway actors, OTIF, CEN TC 256 WG 48, the social partners and every citizen of the European Union to communicate their contributions related to their positions, comments and proposals of improvements on this report and in particular on the Agency proposals.

Management of public contributions

In 2018, the Agency will analyse those contributions answering to all of them.

Recommendation on safety critical components

In 2018, based on the analysis of the contributions and views of the European Commission, the Agency will issue a relevant recommendation to the European Commission regarding:

- Proposals for completing the recommendation on an implementing act revising the ECM certification.
- Proposals of further actions in consistency with Agency priorities.

Annex I References

[Ref. N°]	Title	Reference	Version
[1]	Regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Railways and repealing Regulation (EC) No 881/2004 (Hereafter called "Agency regulation")	2016/796 (OJ L 138 of 26 May 2016)	11/05/16
[2]	Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (recast) (Hereafter called "Interoperability directive")	2016/797 (OJ L 138 of 26 May 2016)	11/05/16
[3]	Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (recast) (Hereafter called "Safety directive")	2016/798 (OJ L 138 of 26 May 2016)	11/05/16
[4]	Implementation of Commission Regulation (EU) No 445/2011 of 10 May 2011 on a system of certification of entities in charge of maintenance for freight wagons and amending Regulation (EC) No 653/2077	ERA-REP-125 V 1.0	23/02/2015

Glossary/Abbreviations

'Agency' means the European Union Agency for Railways regulated by the Regulation 2016/796 [1]
'ECM' means Entity in Charge of Maintenance as defined in the Directive 2016/798 [3]
'IM' means Infrastructure Manager
'RU' means Railway Undertaking
'ECM' means Entities in Charge of Maintenance

Annex II Preliminary report 2016 007REC1004

This preliminary report was published by the Agency in 2016 as support for further discussions held in 2017. It is partly reproduced here only for information.

…

4 Part 2: Safety critical components

4.1 Introduction

A new concept addressing 'safety critical components' was introduced in the new railway legislation, meaning the Regulation 2016/796 and the directives 2016/797 and 2016/798. This follows the discussions held since the accident of Viareggio in 2009 in particular the Task Force on maintenance of freight wagons (2009-2010) and discussions in the Freight Focus Group between 2013 and 2015.

The new legislation introduces the concept but without defining clearly without any confusion what a safety critical component is. Nevertheless the concept is used in definition of requirements for ECM system of maintenance stated in the annex III of Safety Directive 2016/798.

Therefore the Agency considers then that the first priority is to propose a unique EU definition of 'safety critical components' or at least achieve a common understanding.

To this end there was an interest to collect information of what is existing that could be assimilated to definitions of 'safety critical components'.
The Agency made in 2016 several informal and formal consultations:

- CEN/CENELEC;
- NSA network;
- 1 voluntary ECM;
- 1 voluntary Infrastructure Manager.

The Agency concentrated mainly on vehicles because of the needs expressed for the revision of ECM certification (article 14 and annex II of Directive 2016/798). Therefore this part is not containing developments specific to infrastructure. Such development will be performed in a further step.

The objective of this part of the report is to present the first results of Agency reflections.
In the future, this part will be used as input in the project of revision and extension of ECM certification.

4.2 Legal background

Five references to 'safety critical components' have been found in the new legislation [1], [2] and [3]:

- Agency regulation [1] contains 1 reference:

REF1: "*CHAPTER 4: Tasks of the Agency relating to interoperability*
Article 19: Technical support in the field of railway interoperability
1. The Agency shall:…

(l) address, where appropriate, recommendations to the Commission in relation to safety-critical components."

Remark: The attention must be made on the difference but complementary with the art 19(k) related to Interchangeable Spare parts that states that:
"(k) *address recommendations to the Commission in relation to harmonised standards to be developed by European standardisation bodies and standards relating to interchangeable spare parts which may improve the level of safety and interoperability of the Union rail system;"*

It is clear that both 'safety critical components' and 'interchangeable spare parts' are complementary in addressing safety. But one safety critical component may be in the same time an interchangeable spare part but it cannot be concluded now that it is the case for all safety critical components and vice versa.
The duality safety critical component-interchangeable parts will not be discussed within this part but in further steps.

› Interoperability directive [2] contains 2 references:

REF2: "*Consideration (67)… The Commission should also report on actions taken regarding the identification and traceability of safety-critical components."*

REF 3: "*ANNEX III: Essential requirements*
1. General requirements
1.1. Safety
1.1.1. The design, construction or assembly, maintenance and monitoring of safety-critical components, and more particularly of the components involved in train movements, must be such as to guarantee safety at the level corresponding to the aims laid down for the network, including those for specific degraded situations."

› Safety directive contains 2 references:

REF 4: "*CHAPTER VI: Transitional and final provisions*
Article 29: Report and further Union action

By 16 December 2017, the Commission shall report to the European Parliament and to the Council on the actions taken with a view to achieving the following objectives:

(a) the obligation for manufacturers to mark with an identification code the safety-critical components circulating on the European rail networks, ensuring that the identification code clearly identifies the component, the name of the manufacturer and the significant production data;
(b) the full traceability of the safety-critical components, the traceability of their maintenance activities and the identification of their operational life; and
(c) the identification of common mandatory principles for the maintenance of those components."

REF 5: "*ANNEX III*

Requirements and assessment criteria for organisations applying for an ECM certificate or for a certificate in respect of maintenance functions outsourced by an entity in charge of maintenance

10. Maintenance activities — a structured approach to ensure:
— that all maintenance activities affecting safety and safety-critical components are identified and correctly managed and that all the necessary changes to those maintenance activities affecting safety are identified, properly managed based upon the return of experience and the application of Common Safety Methods for risk assessment in accordance with point (a) of Article 6(1) and properly documented;
…"

4.3 Why defining 'safety critical components'?

According to those 5 references, it is evident that there is no real clear definition or common understanding of safety critical components in the EU legislation.

However, REF3 here above, specifies that safety critical components include but are not limited to components involved in train movements.
It has already been understood:

- That safety critical components may be as well components mounted on vehicles or on fixed infrastructure.
- Safety critical components may be components mounted in following structural subsystems: rolling stock, infrastructure, energy and CCS equipments.

In addition to that, there is no criteria stated in the legislation [1], [2] and [3] for defining and evaluating the criticality.

Therefore this justifies the first priority to define:

- Which components may be concerned or which requirements or criteria have to be used to identify those potential concerned components.
- What does criticality regarding safety mean?

4.4 Contributions

The Agency organised:

- 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 where it was requested to the NSAs to provide by 30 November 2016:
    - Information on any national rules/standards/practices containing elements that could help to define safety critical components? For instance elements could be:
        - (predefined) List of components having a role in safety or even a specific criticality for safety. How is this list defined and maintained?
        - Existing definitions
        - Criteria to define the critical risks for safety associated to technical components.

Contributions from 9 NSAs were received: Netherlands, UK, Germany, Ireland, Spain, Sweden, Italy, Romania and Poland.

- 1 presentation to Cooperation of ECM certification bodies in October 2016. A contribution from 1 Austrian accredited certification body was received.
- 1 presentation in the Network of Representative Bodies in December 2016.

All the contributions could not be analysed in December 2016 but the main results may be summarised for:

- Components

1. Each time CEN/CENELEC working groups tried to deal with safety critical components in railway, no conclusion could be achieved because of endless discussions in working group or during inquiries.List of existing components with safety issues is in the standards. But they must be considered as 'safety related' and not 'safety critical'

2. A list of obvious components like wheelsets for which there is no discussion would remain very limited.

3. Components should also include materials, tools and equipments used for maintenance

4. Components used in the functions: 'Guiding the train', 'transmit the breaking', 'doors management' seem to be good candidates to the status safety critical.

5. For infrastructure the focus should be put on installations rather on individual technical systems or individual components.

- Criticality

6. Components should be categorised as safety critical as output of a common process applied to all train and infrastructure components. This process must still be defined and be risk-based.

7. Safety criticality = function(design, operational context, environment, safety targets, maintenance context) therefore an exhaustive list is impossible to achieve. A good approach could be to impose to RUs and ECMs to implement a process of identifying those components responding to the function here above but attention must be made to avoid administrative burden.

8. For maintainers criticality of components depends also of the necessary skills for technicians/workers to inspect, check and take decisions for continuing use or replacing. For instance, NDTs impose specific skills and a hierarchical control of continuous suitability of the testing methods and process.

9. Economic aspects. Criticality should also be linked to economic aspects. In railway a train is considered as safe if it is stopped (except in winter conditions or hot summer when it is stopped for a long time in the middle of nowhere), delays in traffic should also be considered as element of criticality

10. PrEN 50126:2015 parts 1 and 2 (RAMS analysis), civil aviation approach (CS 25[3]), other industrial standards such as IEC 61508:2010 [4] , methodology such as FMECA[5] should be considered. Approach used in nuclear and chemical industrial sector may also be considered.

11. Any development related to safety critical components should not lead to undue additional costs for railway services.

[3] CS25 = Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (EASA Amendment 18 of 22 June 2016)

[4] IEC 61058:2010: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).

[5] FMECA : Failure Mode, Effects, and Criticality Analysis

12. In some MS, there are predefined lists of safety critical components in national rules or in national standards or in national technical documents. Generally, those lists are considered as non-exhaustive by national authorities.

13. Statistics of incidents and accidents and more generally safety performance may also be used for defining criticality. In one MS, those statistics have been used by authorities to justify a non-exhaustive list of safety critical components.

4.5 What is a component?

From the available documentation, the functions ensured by vehicles such as traction, braking, guiding the vehicle or the train, doors management are materialised by technical systems for which the architecture is more or less complex.

The technical systems are composed on basic or elementary elements interconnected. Those basic or elementary elements are called components and connections.

Remark: For making easy the understanding of a complex architecture, technical systems are sometimes expressed as interconnected sub-systems themselves composed on elementary interconnected elements = components and connections.

For E/E/PE technical systems: Components may be chips (themselves composed of transistors), electrical devices (e.g. switch), other electronic components (e.g. condensators), wires, cardboard and … software. To assemble all those basic components: Complex architecture. In many cases it would not be relevant to consider those components themselves in the concept of 'safety critical components' in the EU legislation but the technical systems themselves.

We should also take into account, at this level, the contribution **3** mentioned in the preceding section. As detailed analysis of this contribution will be performed in the framework of revision of ECM certification, the Agency proposes to include Materials, tools and equipments used in maintenance.

Therefore the Agency makes the following proposal:
The term 'components' in 'safety critical components' within the EU railway legal framework means:

- A technical system performing a function; or
- A technical subsystem performing a subfunction when the combination of subfunctions cover a function; or
- An individual (basic) component when it is convenient for systems with low complexity. Mainly mechanical systems.
- Softwares should also be considered as component.
- Materials, tools and equipments used in maintenance

4.6 What could criticality mean?

There are many different approaches to criticality. Here below the reader may find several non-exhaustive ones that have the potential to be used for addressing the EU railway *legal framework* regarding the concept of 'safety critical components'. In general criticality is expressed as a combination of different approaches.
The approaches presented here below are:

- Criticality based on danger.
- Criticality based on safety risks.
- Approach based on FMECA.
- Criticality associated to maintenance.

Economic aspects are not formally introduced in those approaches here described but they are crucial for future development. Consequently the Agency will have to assure that cost-efficiency and competitive aspects of the railway system are not impaired by any common approach of criticality that would be agreed by stakeholders and authorities.

4.6.1 Criticality based on danger.

Criticality is often expressed by for instance *"a component is safety critical if a single failure of this technical system leads to a catastrophic accident".*
This way is applied in civil aviation (CS25) stating that a single failure of a technical system can never lead to the loss of an aeroplane.
The main disadvantage of this approach is that it does not take care of the frequency of the failure. Even if a failure having the potential to lead directly to a catastrophic accident is unlikely, it has no influence on characterizing the technical system as safety critical therefore it can lead to non-sustainable increase of cost in design, use and maintenance of the technical system.

4.6.2 Criticality based on safety risks

An evolution of the preceding approach results in taking into account the frequency of occurrences of failures that can lead to unwanted effect (e.g. catastrophic accident or serious accident).

Criticality is then a combination of frequency of occurrence of failure and gravity of effect.

There could be many expressions related to this approach.

- For instance in 5.14 of EN 13306:2010 'Maintenance – Maintenance terminology ': '5.14 Criticality (of a failure or a fault) = numerical index of the severity of a failure or a fault combined with the probability or frequency of its occurrence'
- In annex E (informative) of this standards, a criticality matrix is proposed.

- Among the contributions that the Agency has received, at least one NSA justifies a list of safety critical components on measured frequencies of occurrences of failure based on statistics of incidents and accidents.

4.6.3 Approach based on FMECA[6]

Approach FMECA (Failure Mode, Effects and Criticality Analysis) used, among other, in EN IEC 61508 and CS 25 (civil aviation) introduces a third level compared to preceding approach to characterise the criticality.

Criticality is defined as a combination of detection possibility (D), Frequency of occurrence of failure (F), gravity of effects (G). For example: Criticality = D * F * G

[6] FMECA : Failure Mode, Effects, and Criticality Analysis

with
D: Detection possibility of failure or precursors to failure,
F: Frequency of occurrence of a failure mode,
G: Gravity of the effects (consequences)

For understanding, the Agency proposes, by analogy with other application of FMECA, that detection possibility may be defined in 4 levels as:

- **1 evident**: Automatic alarm or information system sent to driver
- **2 possible**: Need intervention of a person (technical inspection, visual inspection by maintenance staff or driver or on-board staff)
- **3 Probable**: Needs a dismounting or a specific testing system (for instance NDTs on axle in maintenance)
- **4 impossible**: No possibility of any detection before failure.

The Agency could observe that this approach has been used at least by two ECMs for freight wagons as well by one designer/manufacturer of wheelsets in a publication[7] related to maintenance in 2016. Nevertheless, no in-depth analysis has ever been performed by the Agency about the effectiveness of those developments.

4.6.4 Criticality associated to maintenance

In received contributions, an ECM developed the concept of criticality on the base of its relations with customers. In particular the criticality of components, from an ECM point of view, depends also:

- on the need for high expertise for performing specific tasks and taking decision of suitability for use such regarding for instance brake testing, NDTs.
- on use of tools kept under control (e.g. calibration needed)

Maintainers consider always, in addition to risk based approach, other requirements such as availability and reliability of vehicles and on-board technical systems to define criticality and from criticality, define their strategy for maintenance including the priorities for investments and management of human resources (e.g. trainings, qualification, and recruitment).

4.7 Conclusions and further steps

From the analysis made in this part, there are many ways to define a component and criticality. Therefore one priority for 2017 will be to issue a common definition or common understanding of what the concept ‘safety critical components’ in the EU railway framework would mean while ensuring that:

- safety is maintained or improved when it is reasonable; and
- cost-efficiency and competitive aspects of railway are at least not impaired.

The Agency proposes to continue the work in priority within the framework of revision and extension of ECM certification.
This part is one input for further collaborations with EC, NSAs and RBs.

[7] « A modern approach to wheelset maintenance plan optimisation » Collana LRS TECH Volume 9 ISBN 9788890624087

Annex IV

Legal Base for traceability of components

Directive 2016/798 annex III 7. et 8.

Annex III. REQUIREMENTS AND ASSESSMENT CRITERIA FOR ORGANISATIONS APPLYING FOR AN ECM CERTIFICATE OR FOR A CERTIFICATE IN RESPECT OF MAINTENANCE FUNCTIONS OUTSOURCED BY AN ENTITY IN CHARGE OF MAINTENANCE

…

The following basic requirements shall be applied to the four functions of an entity in charge of maintenance (ECM) to be covered by the organisation itself or through contracting arrangements:

…

7. Information — a structured approach to ensure that important information is available to those making judgments and decisions at all levels of the organisation and to ensure the completeness and appropriateness of the information;

8. Documentation — a structured approach to ensure the traceability of all relevant information;

Commission Regulation 445/2011 annex III I. 7. et 8.

'7. Information — a structured approach to ensure that important information is available to those making judgments and decisions at all levels of the organisation

…

8. Documentation — a structured approach to ensure the traceability of all relevant information

…'

Text not fully reproduced

Commission Regulation 445/2011 annex III II. 7. (b)

'7. When the documentation process is applied to the maintenance development function, the traceability of at least the following elements needs to be guaranteed:

…

(b) the configuration of vehicles, including, but not limited to, components related to safety'.