Workshop #08
Safety critical components: issues and methodology

Mrs Nathalie Duquenne

Project Officer
nathalie.duquenne@era.europa.eu

Mr Giuseppe Ragusa

Maintenance Engineering Project Officer at:
CEN-TC256-WG48 Representative
g.ragusa@trenitalia.it

CEN-TC256 Railway Applications

Safety Critical Components

Legislation and standards

Agency regulation

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,

Safety directive

Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (recast)

Interoperability directive

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)

TSIs revision

Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 amending Commission Regulations (EU) No 321/2013, (EU) No 1299/2014, (EU) No 1301/2014, (EU) No 1302/2014, (EU) No 1303/2014 and (EU) 2016/919 and Commission Implementing Decision 2011/665/EU as regards the alignment with Directive (EU) 2016/797 of the European Parliament and of the Council and the implementation of specific objectives set out in Commission Delegated Decision (EU) 2017/1474

ECM Regulation

Commission Implementing Regulation (EU) 2019/779 of 16 May 2019 laying down detailed provisions on a system of certification of entities in charge of maintenance of vehicles pursuant to Directive (EU) 2016/798 of the European Parliament and of the Council and repealing Commission Regulation (EU) No 445/2011

CEN/TR 17696

Vehicle Maintenance Guide for identification and management of Safety Critical Components for railway vehicles

TECHNICAL REPORT
RAPPORT TECHNIQUE
TECHNISCHER BERICHT

FINAL DRAFT
FprCEN/TR 17696

May 2021

ICS 45.060.01

English Version

Railway applications - Vehicle Maintenance - Guide for identification and management of Safety Critical Components for railway vehicles

Applications Ferroviaires - Maintenance des véhicules - Guide pour l'identification et le management des Composants Critiques de Sécurité pour les véhicules ferroviaires

Bahnanwendungen - Instandhaltung von Eisenbahnfahrzeugen - Sicherheits-kritische Bauteile

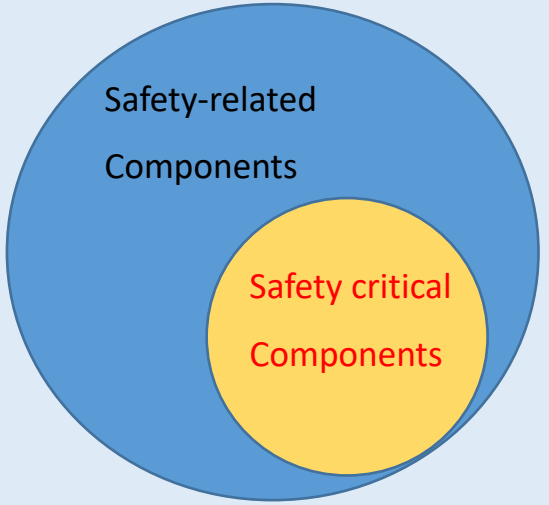
This draft Technical Report is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 256.

Safety Critical Components Definition

Safety critical components *are components for which a single failure has a credible potential to lead directly to a serious accident resulting in stated consequences*

CEN/TR 17696 "*Vehicle Maintenance - Guide for identification and management of Safety Critical Components for railway vehicles*" – Section 7.3.1

SCCs are a sub-set of the **safety-related components**, where these are defined as components performing safety relevant functions keeping the vehicle in a safe state and preventing a safety hazard occurring (see EN 17023-2018-ANNEX B).



Safety Critical Components Keywords

Safety critical components *are components for which a single failure has a credible potential to lead directly to a serious accident resulting in stated consequences*

- Components
- Single failure
- Credible potential to lead directly
- Serious accident
- Consequences

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

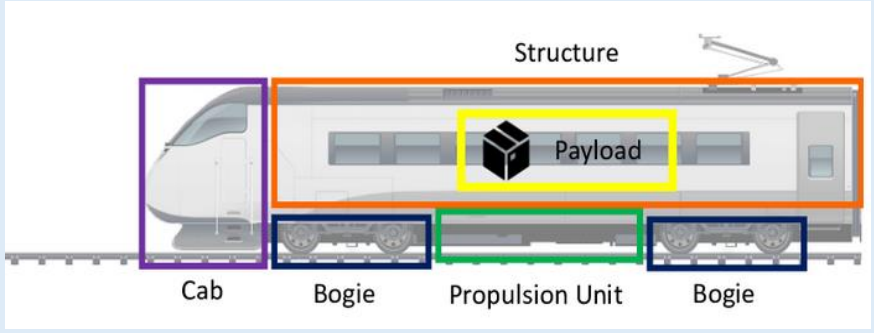
Serious accident

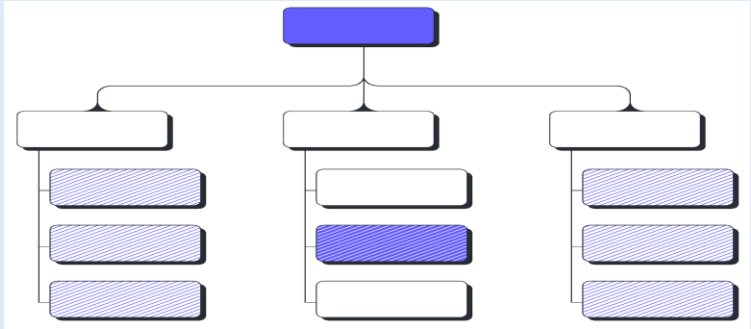
Consequences

The components of the vehicle can be defined and identified by starting with the definition as in 3.11 of **EN 15380-2:2006**:
'3.11 component
uniquely identifiable product that is considered indivisible for a particular planning or control purpose and/or which cannot be disassembled without it being destroyed
NOTE A component for one organizational group may be the final assembly of another group, e.g. an electric motor.

Components identification:

Breakdown structure of the vehicle starting from a functional and product level approach using EN 15380-2





MPG designation[a]	Name of the MPG
B	Vehicle body
C	Vehicle fitting out
D	Interior appointments
E	Running gear
F	Power system, drive unit
G	Control apparatus for train operations
H	Auxiliary operating equipment

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

Serious accident

Consequences

single failure: it means that when the failure of the component occurs, it is the unique event causing the partial/complete loss of the function performed by the component. No other failure or combination of failures is considered. All the other vehicle's components have to be considered in good state for performing their functions;

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

Serious accident

Consequences

credible: it addresses a judgement about the realistic possibility to have the accident (if it is considered not credible, it will not be considered). Credible means that it must be plausible that the failure of the component can result in an accident with the severity consequences specified. Hypothetical and not reasonable scenarios need not to be considered;

potential: it means that when the failure of the component occurs, it is quite possible that it results in an accident with the severity consequences specified. This assumption leads to consider the scenario in which the failure occurs (i.e. in terms of "persons exposed to the risk");

Directly: it means that the accident is the direct effect of the failure. No other additional failures are needed to cause the accident. In terms of Fault Tree Analysis, it means that the considered Minimal Cut Sets to have the Top Event (i.e. one of the accidents specified) need to have order 1.

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

Serious accident

Consequences

from Safety Directive Art. 3 Definitions

(12) 'serious accident' means any train collision or derailment of trains resulting in the death of at least one person or serious injuries to five or more persons or extensive damage to rolling stock, the infrastructure or the environment, and any other accident with the same consequences which has an obvious impact on railway safety regulation or the management of safety; 'extensive damage' means damage that can be immediately assessed by the investigating body to cost at least EUR 2 million in total;

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

Consequences

Table 1 — SCCs - List of accidents (non-exhaustive) from CEN/TR 17696

derailment		
collision	collision of train with obstacle	collision of train with rail vehicle
level crossing accident		
accident to persons involving rolling stock in motion	persons falling from trains persons hit by a railway vehicle or by an object attached to, or that has become detached from, the vehicle	passengers in station hurt by train
fire/explosion	fires in an area inside or outside the railway premises	
dangerous goods release during transport	pollution of an area by liquid, solid or gas release of goods	
objects detached from trains		
electrocution		
other accidents causing damage	material damage to an area (e.g. trees pulled down by rolling stock in motion, infrastructure damage, railway premises, …)	damage to rolling stocks

Safety Critical Components – Keywords

Components

Single failure

Credible potential to lead directly

Serious accident

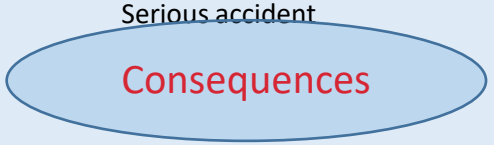


Table 2 — SCCs – List of consequences from CEN/TR 17696

death of at least one person
serious injuries to five or more persons
damage to rolling stock, the infrastructure or the environment assessed to cost at least 2 million EUR in total

Safety Critical Components – Who is involved

Commission

Manufacturer

Railway Undertaking

ERA

ECM

Keeper

Safety Critical Components – Who is involved
Actions requested

Commission

ERA

Manufacturer

ECM

Railway Undertaking

Keeper

Requirements

To report to the European Parliament and to the Council on:

- the obligation for manufacturers to mark with an identification code the SCCs
- the traceability of SCCs, their maintenance activities and identification of their operational life
- the identification of common mandatory principles for the maintenance of the SCCs

Safety Critical Components – Who is involved
Actions requested

Commission

ERA

Manufacturer

ECM

Railway Undertaking

Keeper

Requirements

address, where appropriate, recommendations to the Commission in relation to SCCs

Safety Critical Components – Who is involved Actions requested

Commission

Manufacturer

Railway Undertaking

ERA

ECM

Keeper

Requirements (from Table 5 of CEN/TR 17696)

Vehicle Phase	Requirement
Design	carrying out design, construction or assembly of SCCs, and more particularly of the components involved in train movements, in such a way to guarantee the corresponding safety level of the network in normal and degraded situations
Design	inserting a SCCs list into the technical file
Design	inserting a SCCs list into the maintenance description file together with specific servicing, maintenance and servicing/maintenance traceability requirements
Design	inserting a SCCs list into the operation documentation together with specific operational and operational traceability requirements
Design	specifying precedents, principles and methods used to identify SCCs and their specific operational, servicing, maintenance and traceability requirements inside the Maintenance Design Justification File
Design	developing specific operational and operational traceability requirements during the design phase
Design	identifying specific servicing, maintenance and maintenance traceability requirements during the design phase
Operation	collaborating with the RU/Keeper to develop specific operational and operational traceability requirements after the vehicles have entered into operation
Operation	collaborating with the ECM to identify SCCs and their specific servicing, maintenance and maintenance traceability requirements after the vehicles have entered into operation
Design/Operation	considering the SCCs definition during design and in the service life of the vehicle to identify new SCC or manage its changes
Design/Operation	managing information and maintenance instructions of SCCs in the technical file
Operation	confirming if new SCC identified by the ECM is safety-critical through a risk assessment taking into account the use and environment of the component
Operation	providing technical and engineering support about SCCs and their safe integration, when the ECM or Keeper address a request

Safety Critical Components – Who is involved Actions requested

Commission

Manufacturer

Railway Undertaking

ERA

ECM

Keeper

Requirements (from Table 6 of CEN/TR 17696)

carrying out the maintenance and monitoring of SCCs, and more particularly of the components involved in train movements, in such a way to guarantee the corresponding safety level of the network in normal and degraded situations
[maintenance development function] having a procedure to identify and manage SCCs
[maintenance development function] having a procedure for the competence management process taking into account maintenance activities on SCCs
[maintenance development function] having a procedure to guarantee traceability of the vehicle's configuration documentation related to SCCs
[maintenance delivery function] having a procedure for the competence management process taking into account maintenance activities on SCCs
taking into account the initial Manufacturer SCCs list and the specific maintenance instructions recorded into the technical file
identifying and correctly managing the maintenance activities affecting safety and SCCs and identifying and properly managing their changes through REX and the application of the Common Safety Method for risk assessment
meeting SCCs management requirements specified inside ECM Regulation
consider the SCCs definition in the service life of the vehicle to identify new SCC or manage its changes
inform without delay Manufacturer, the holder of the vehicle type and the holder of the vehicle authorisation (if these parties can be identified), when it becomes aware of evidence about a new SCC is identified
inform the rail sector and the rail support industry about new or unexpected safety relevant findings when the related risks are relevant for more actors and are likely to be poorly controlled. To do this, the ECM is required to use SAIT or other informatics tool provided by the Agency for that information
providing, directly or via the Keeper, information about SCCs to railway undertakings and infrastructure managers operating the vehicles, keepers, manufacturers, holders of vehicles authorisations and holders of the type authorisation of vehicles, subsystems or components, as most appropriate, and inform them of exceptional maintenance findings beyond wear and tear
as appropriate, adjusting procedures to ensure monitoring and safe maintenance of the component when a new SCC is identified
managing safety critical components and appropriate maintenance instructions as well as relevant maintenance activities in the maintenance file or documentation referred to in Article 14 of the Safety Directive
where necessary, addressing a request to the Manufacturer, directly or via the Keeper, for technical and engineering support about SCCs and their safe integration
collaborating with the Manufacturer to develop specific servicing, maintenance and maintenance traceability requirements after the vehicles have entered into operation

Safety Critical Components – Who is involved
Actions requested

Commission

Manufacturer

ERA

ECM

Railway Undertaking

Keeper

Requirements (from Table 7 of CEN/TR 17696)

carrying out monitoring of SCCs, and more particularly of the components involved in train movements, in such a way to guarantee the corresponding safety level of the network in normal and degraded situations
where necessary, addressing a request to the Manufacturer for technical and engineering support about SCCs and their safe integration
collaborating with the Manufacturer to develop specific operational and operational traceability requirements after vehicles have entered into operation

Safety Critical Components – What is involved

New vehicle

a vehicle for which an applicant has requested from the authorising entity the vehicle type authorisation for placing on the market under the new legislation (complying with Regulation 2018/545 and using the One-Stop-Shop of Agency).

Safety Critical Components – What is involved

Existing vehicle

a vehicle that does not meet the criteria of a new vehicle

Entity managing the change

SCCs identification in case of change to the vehicle **only** for the parts of the vehicle related to engineering change renewal/upgrading/refurbishment

ECM

Identification of potential SCCs during maintenance

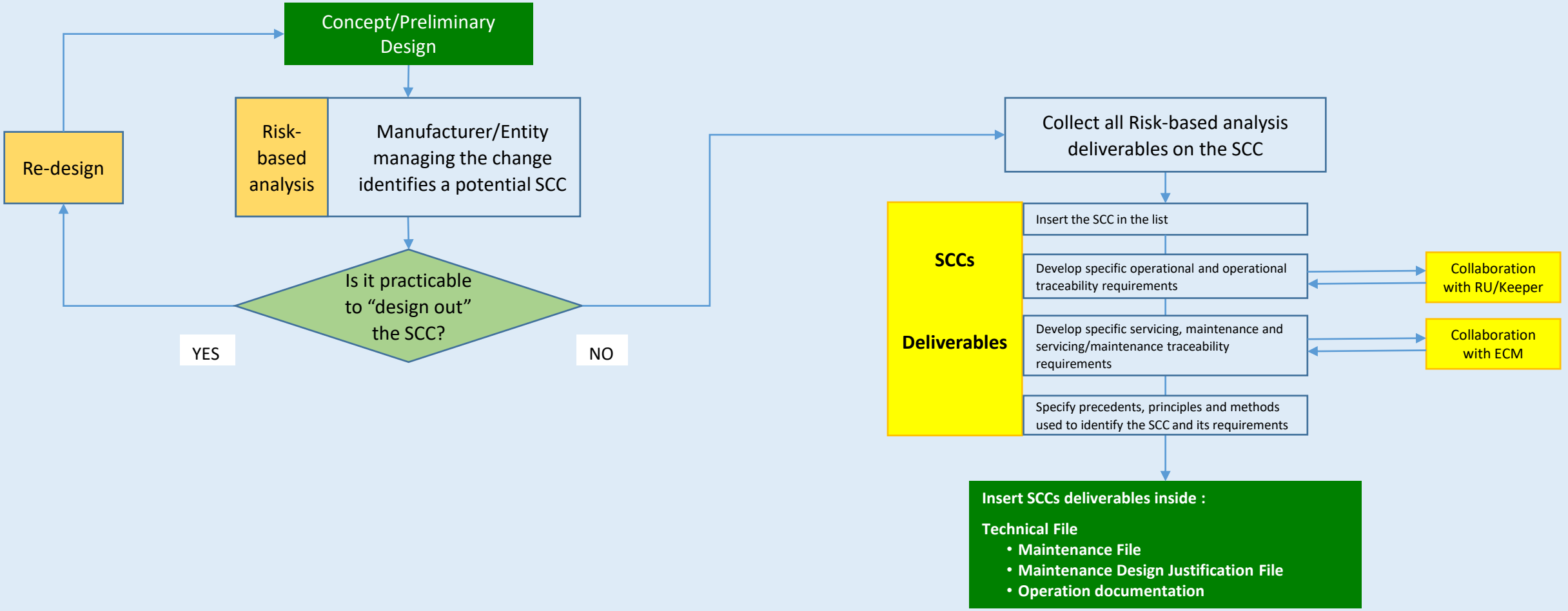
- **changes to the maintenance file**
- **monitoring activities**
- **continuous improvement**

NOTE:

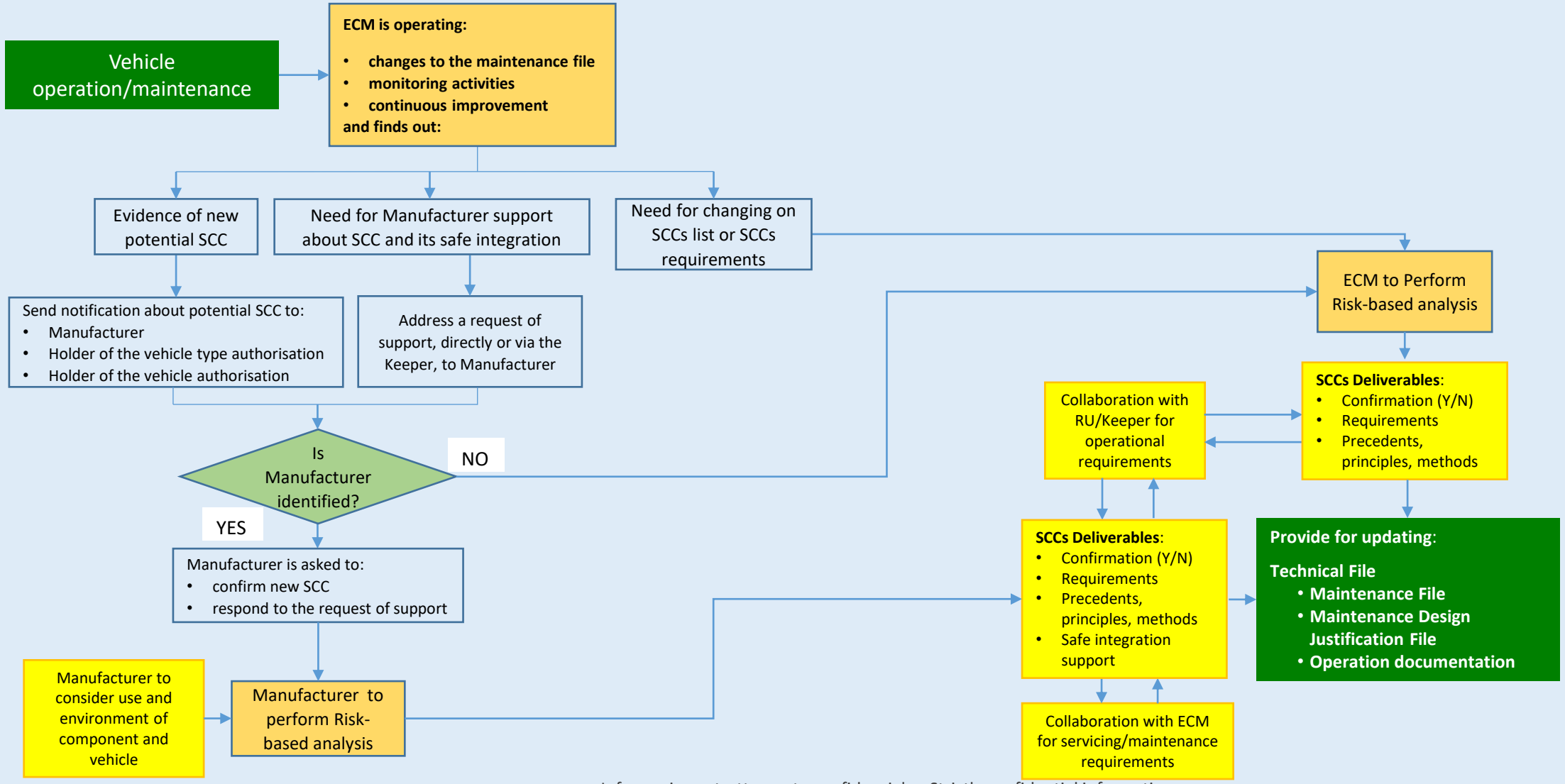
neither Manufacturers/Entities managing the change nor ECMs are obliged to identify retrospectively SCCs for existing vehicles except in the case of engineering change/renewal/upgrading/refurbishment

Safety Critical Components – Identification process
Perspective from Manufacturer/Entity managing the change

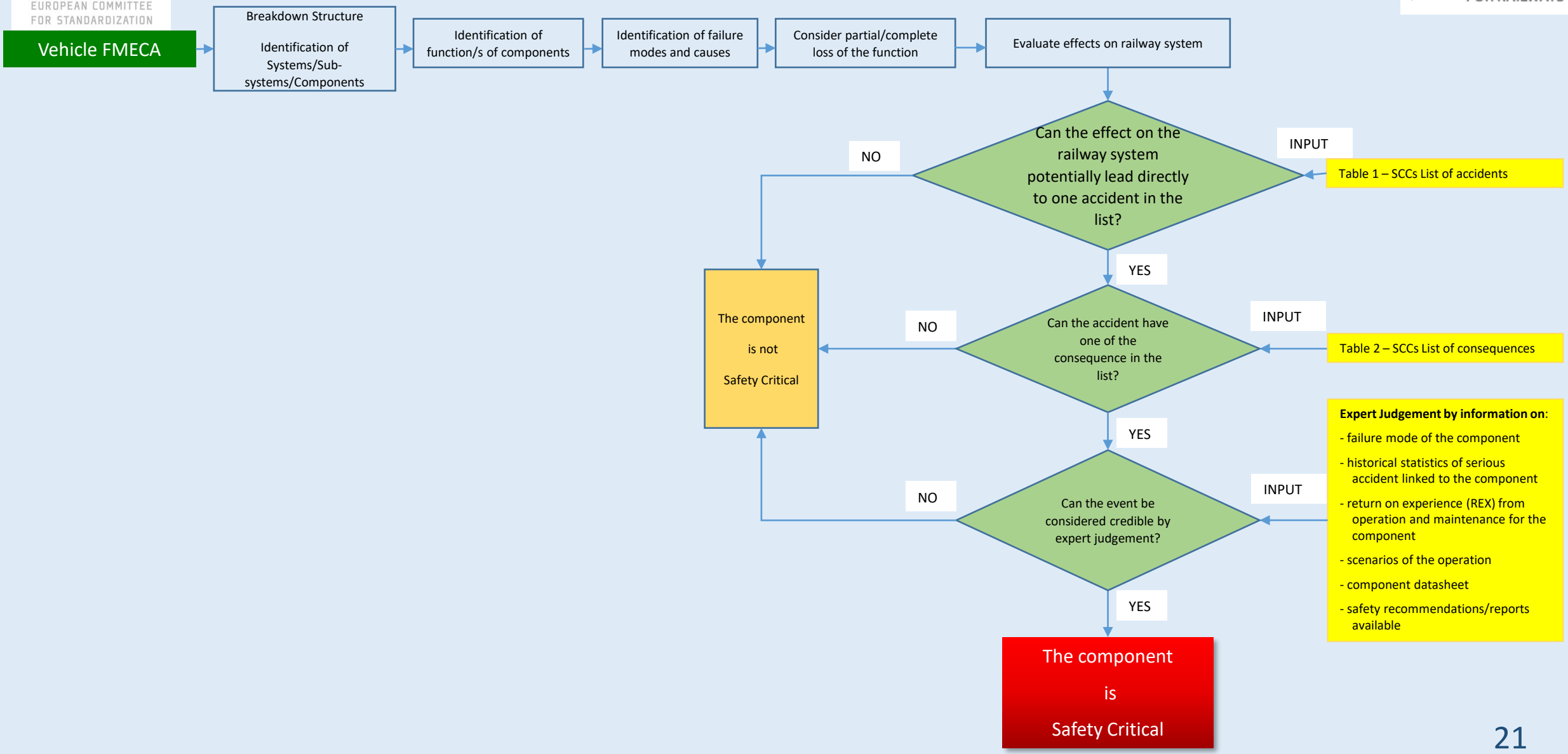
New vehicle or engineering change/ renewal/upgrading/refurbishment of existing vehicles



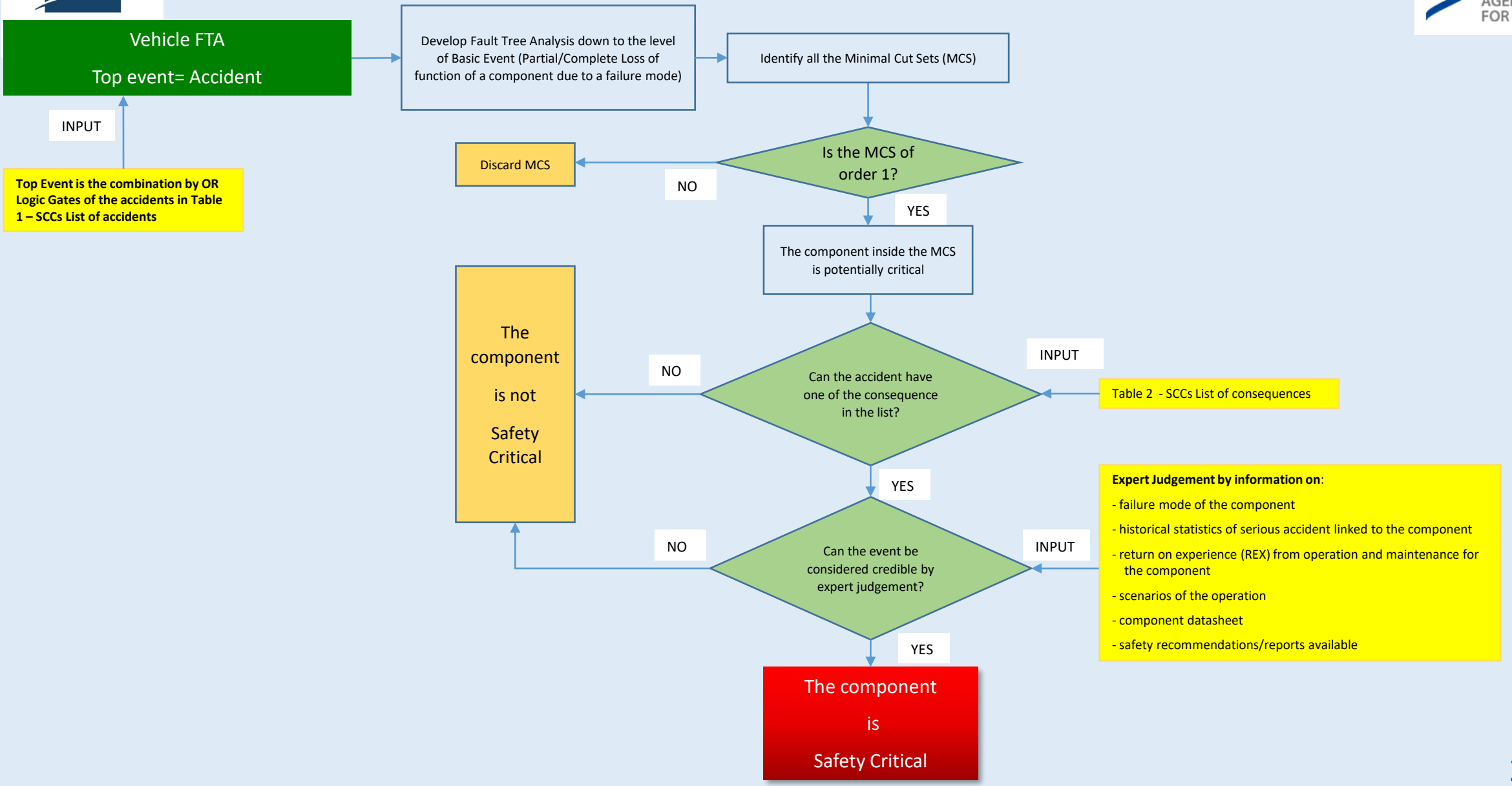
Safety Critical Components – Identification process
Perspective from ECM



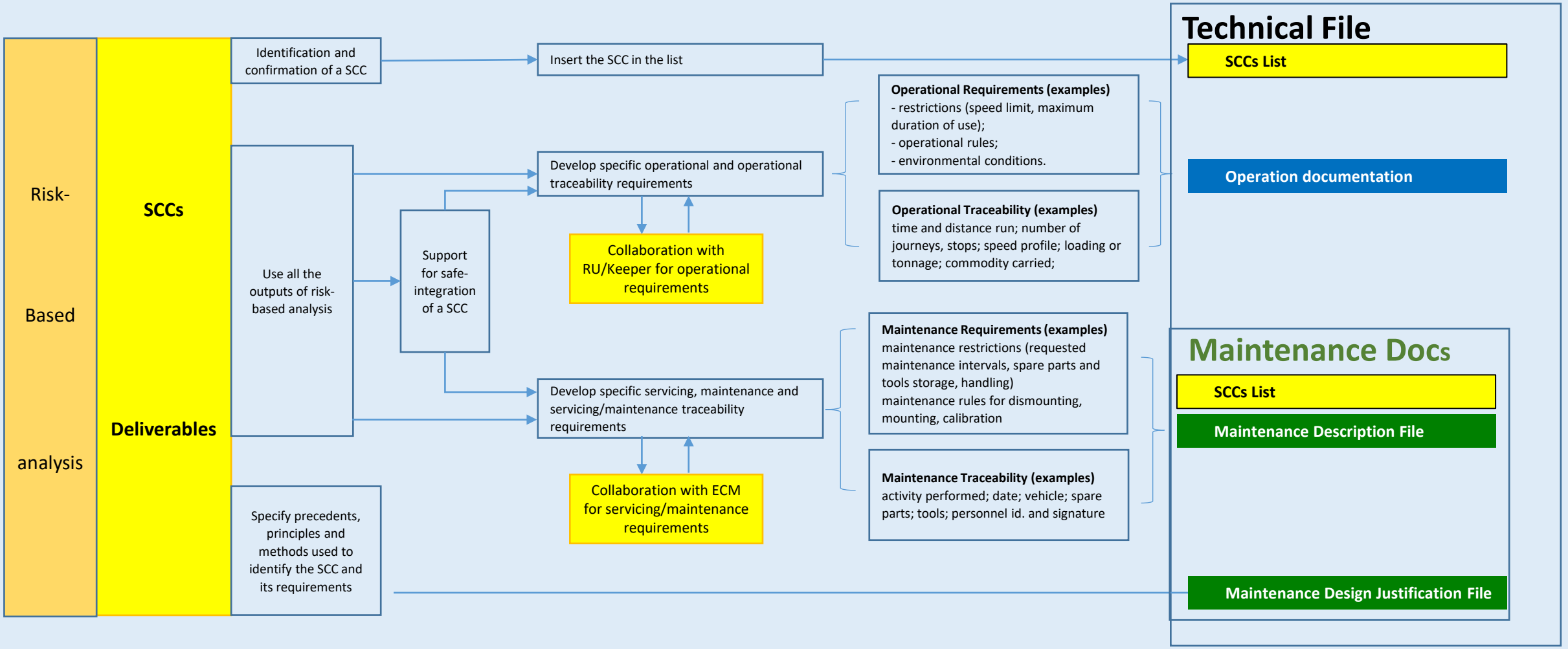
Safety Critical Components – SCCs – Identification method - 1



Safety Critical Components – SCCs – Identification method - 2



Safety Critical Components SCCs Deliverables



Safety Critical Components
Example of SCCs List
Early experience from European stakeholders

Basic List of components related to train movement

- Wheels
- Axles
- Axles boxes
- Wheelset bearings
- Bogie frame
- …….

Partial list extracted from an EMU Train project

Item no.	Safety Critical Components
1	Cabin Shell Connection
2	Anti-Yaw Intercar Dampers
3	Pitch Intercar Dampers
4	Lateral Curve Stop Supports
5	Body-Body Damper Supports 1) Mounting Roll Damper Support Male 2) Mounting Roll Damper Support Female e
6	Windscreen
7	Front End Fairings 1) Cab End Optical Panel Without Glass 2) Cab End Window Mask Without Opening
8	Front End Fairings 1) Cab End Hatch 2) Cab End Roof Panel 3) Cab End Side Panels Installation 4) Skirt Installation
9	Roof Fairings
10	External Boxes 1) Box Blocking Device 2) Cover Installation for the Ladder FRP

List from a representative body for Freight Wagons

- Wheelset
- Wheel
- Axle

Safety Critical Components
Example of SCCs List
Early experience from European stakeholders

Volunteers ?

- Brakes
- Buffer and draw gear
- Control-command and signalling
- Doors
- Tanks, valves (on freight wagons)
- ……

EUROPEAN COMMITTEE FOR STANDARDIZATION

EUROPEAN UNION AGENCY FOR RAILWAYS | EUROPEAN RAIL SAFETY DAYS 2021 Porto 3 - 5 November

Committed to Safety!

EUROPEAN UNION AGENCY FOR RAILWAYS

Workshop #08
Safety critical components: issues and methodology

Thanks for joining the workshop

Questions ?