# An Integrated, Systems-Based Approach to Authorisation of Actively-Controlled Running Dynamics

Roger GOODALL[2], Riccardo LICCIARDELLO[1], Sebastian STICHEL[3], Peter HUGHES[2]

[1] DICEA, La Sapienza, Rome, Italy
[2] Institute for Railway Research, University of Huddersfield, UK
[3] KTH, Stockholm, Sweden
Corresponding Author: Roger Goodall (r.m.goodall@hud.ac.uk)

## Abstract

A European Union funded research project called RUN2Rail is investigating a range of new technologies for railway rolling stock. The project includes a task on the use active of suspensions, and one of the subtasks is to propose a homologation or authorisation strategy. The incorporation of electronics and control into suspension systems is still at an early stage, so this paper provides a framework for a practical and efficient authorisation strategy based upon existing European regulations and standards.

Keywords: safety, suspensions, control, electronics

## 1. Introduction

It is well established that active or “mechatronic” suspensions offer performance improvements that cannot be achieved with purely passive solutions [1]. The principal requirement is now to develop safe, reliable active suspension systems. However, whereas failures of purely mechanical components or systems can be unambiguously avoided by a combination of conservative design and regular inspection and maintenance, this is not possible for active suspension systems that utilise sensors, actuators, electronics and software because such components can fail without warning. Also, even with conservative design, the combined failure rates of the components will sometimes not be sufficient to meet safety integrity requirements, which means that some form of redundancy may be needed. It is therefore essential to develop an approach that can provide the basis for future authorisation of advanced active suspension systems.

This paper presents an authorisation strategy that follows the existing regulations and standards in the European Union, but tailors it to the specific requirements of actively-controlled running dynamics, i.e. the suspension system. The paper: provides the background to what is available in the way of relevant standards, including the way in which these are relevant to active suspension systems; proposes a practical framework using a modular, reusable, hierarchical set of safety case documents; gives an illustrative example; and concludes with a summary of the project deliverables and limitations.

## 2. Background

### 2.1 Relevant standards

The existing framework for vehicle authorisation in Europe revolves around the Interoperability Directive [2] and the Safety Directive [3] The former defines the authorisation process and the Technical Standards for Interoperability, the latter introduces the Common Safety Methods (CSM) [4] which include the CSM for Risk Assessment (RA). Therefore risk-based analysis is included in the process, in the sense that any "significant change" to the railway system, such as the introduction of a new (and particularly novel) vehicle, must be assessed according to the CSM RA. The CSM is also a way of proving the safe integration of the vehicle in the network it is intended for, which is a key condition for the authorisation to be granted. This is a consequence of the safe integration of the active system into

the vehicle and of the safe integration of its components.

The CSM RA allows the acceptability of risks linked to the introduction of new rolling stock to be demonstrated using one of the following methods:

- demonstration of compliance with relevant codes of practice;
- comparison with a reference active suspension system that has an existing safety case;
- an explicit risk-based approach, e.g. compliant with EN50126 and EN50657; or
- a combination of the above approaches.

One important code of practice is EN14363 “Testing and Simulation for the acceptance of running characteristics of railway vehicles” [5] which is founded on experimental tests (fixed site and on-track tests), with an increasing contribution from virtual methods. If such tests are passed by a new vehicle, conformity with EN14363 "closes out" the risk related to the "running dynamic behaviour" and "safety against derailment on twisted track" requirements of the Technical Specification for Interoperability for the “Rolling Stock Subsystem - Locomotives and passenger rolling stock”, known as the LOC&PAS TSI [6].

The standard, however, is still not completely tailored to new vehicles with active secondary and/or primary suspension components. For secondary suspensions, each fault mode may require on-track tests to be performed again, leading to a high burden even if there is only one fault mode that needs to be tested. For primary suspensions the proliferation of test requirements could become even more burdensome.

EN50126, 50128 and 50129 deal with railway safety cases where electronics and software are a key part of the system, which therefore are very relevant to active suspension systems. These are focussed upon signalling applications, whereas EN50657 covers software assurance for rolling stock. EN50129 in particular supports the principles of establishing multiple related safety cases [7], stating that the following three different types of safety case can be considered:

- a Generic Product Safety Case (GPSC) provides evidence that a generic product is safe in a variety of applications;
- a Generic Application Safety Case (GASC) provides evidence that a generic product is safe in a specific class of applications;
- a Specific Application Safety Case (SASC) that is relevant to one specific application.

Fig. 1 is a diagram from European Standard EN50126-2:2007 [8] showing how they can be used together.

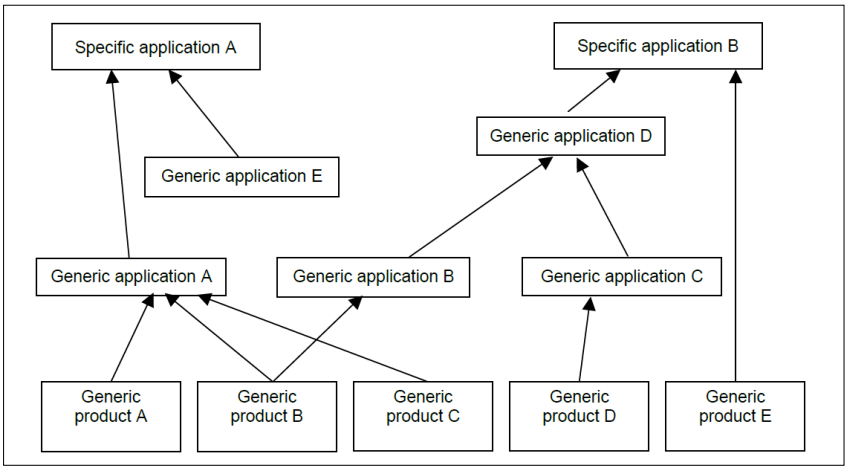


**Figure 1: The combination of numerous safety cases for different specific applications.**

## 2.2 Types of active suspension

From a number of discussions within the RUN2Rail project, three active suspension types have

emerged that are expected to be distinct in terms of their safety authorisation implications:

**Type 1 – Active Secondary Suspensions** It is expected that most active secondary suspensions (including tilting) could be authorised using existing standards (principally EN14363). This is because faults in either vertical or lateral active secondary suspensions are likely to degrade ride quality, but can readily be designed so as not cause unsafe instability, excessive wheel loads or derailment. An important issue may be the effect upon gauging.

**Type 2 – Active Primary Suspensions with mechanical constraints** In general active primary suspensions are expected be more difficult to authorise, but in principle could use the existing standards if safe operation in the event of an active system fault can be assured by means of a mechanical back-up, by limited force capability from the actuators, or a combination of the two. These mechanical constraints would need to be designed in order to assure against unsafe instability, excessive wheel loads or derailment.

**Type 3 – Active Primary Suspensions with functional redundancy** However, the constraints associated with a mechanical back-up and/or limited force capability from the actuators described as Type 2 are likely to limit the performance of an active primary suspension. Since the reliability of a single "channel" of active control will not be sufficient, some form of functional redundancy is required to decrease the probability of unsafe operation in the event of faults within the active system. Of course the existing standards for stability, derailment and wheel loads (EN14363) would still be directly relevant, but compliance would not prove the safe integration of the vehicle within the network. An explicit risk-based authorisation methodology will be needed to meet the specified integrity levels defined for the associated hazards.

## 2.3 Proposed authorisation framework

The RUN2Rail project has decided to adopt the GPSC, GASC and SASC approach, and Fig. 2 presents a modular framework of Safety Case documents: this is a re-drawing of the EN50126 diagram in Fig. 1 with the wording made directly relevant to active suspensions of different types (highlighted arrows show the possible relationship diagram for EMAs (Sect 3)). This shows how a particular actuation technology may be applied to a variety of active suspension applications.

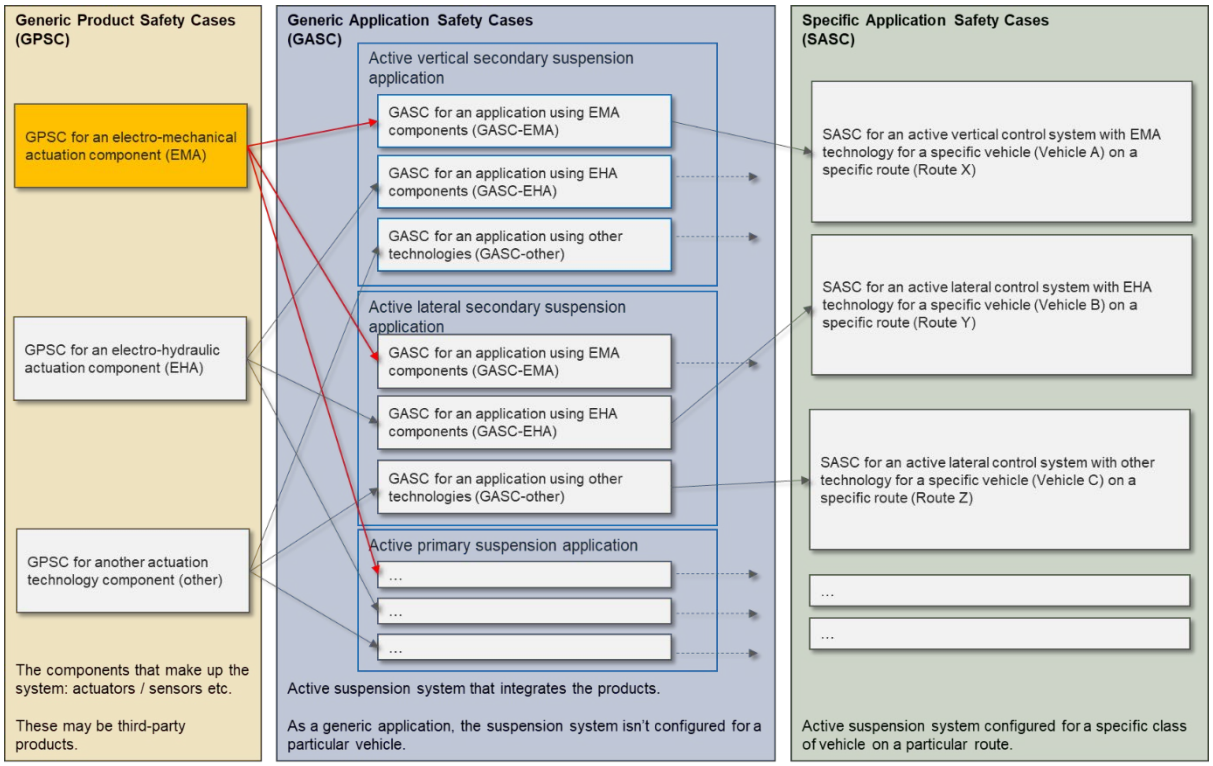


**Figure 2: Adaptation of European Standard EN 50126-2:2007.**

The left-hand panel of the figure illustrates safety cases for generic products (GPSCs), which are the components that have to be safely integrated to make up the system, in particular actuators and sensors. The components may implement different technologies, for example electro-mechanical actuation devices or electro-hydraulic actuation. A GPSC will provide a safety case for the product and will include descriptions of individual failure modes that may affect the operation within a particular application. In addition, the GPSC will describe specific safety requirements for the component such as the range of operating temperatures for which the safety case is valid, electrical or hydraulic safety, etc.

The centre panel illustrates generic application safety cases (GASCs). Generic applications can be considered to be the different types of active suspension systems, for example active secondary lateral suspension systems, or active primary suspension systems. A generic application may be made up of a number of components, any of which may have a GPSC. The GASC describes how the application is safely integrated with the components and how the overall application has been configured to ensure safety. The GASC will consider the safety-related effects of the GPSC failure modes upon the application. The GASC will also describe non-functional safety requirements such as procedures for maintenance of the application. There will therefore be a cluster of GASCs for a particular active solution (shown by the blue boxes In Fig. 2), and although these will not be identical there will be substantial commonality.

Specific application safety cases (SASCs) are illustrated in the right-hand panel: these describe how a generic application is configured for and safely integrated with a specific vehicle with given network characteristics. The SASC will show how the application conditions of the GASC have been met for a specific vehicle. As such, an SASC will normally contain a number of checklists showing that the application has been configured and installed correctly, for example an SASC will show that a specific installation of the application for a specific vehicle was fitted by a competent (named) fitter and show the licence details of the fitter. The SASC will also show that the process to fit and test the wiring was correctly followed and include the fitting and inspection checklists that were completed when the application was installed.

## 3. Templates and guidelines

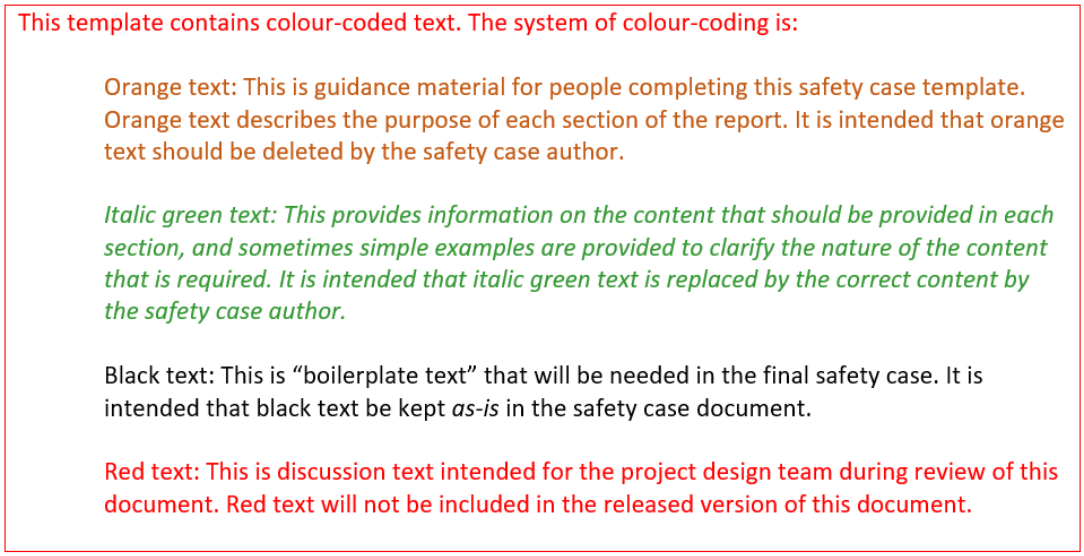


**Figure 3 Colour-coded guidelines for templates**

Three templates utilising colour-coded text shown in Fig. 3 have been written for the GPSC, GASC and SASC. Each SC has the section headings required by the CSM: Introduction, System Description, Quality Management Report, Safety Management Report (the safety process), Technical Safety Report

(the safety analysis), Conclusion plus relevant references and appendices. The guidance provided by the orange, green and black text is different for the GPSC, GASC and SASC templates.

## 4. Illustrative example

This example is intended to suggest how a Generic Product Safety Case for an electro-mechanical actuation product (EMA) could be used for a variety of active suspension applications, and specifically for an active lateral secondary suspension.

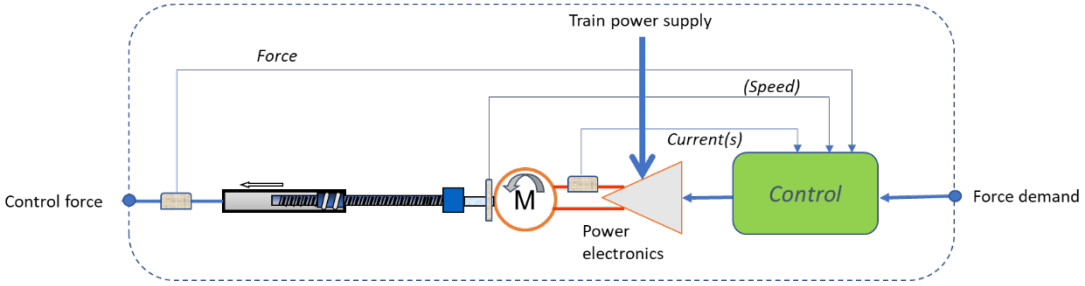


**Figure 4: EMA diagram.**

The EMA actuation system in Fig 4 shows an input force command (an electronic signal) and an output force that would be applied to the vehicle dynamic system in order to provide “active intervention”. There is an electrical motor driven by a power amplifier comprising high-frequency switched semiconductors giving high efficiency bi-directional control of the power supplied to and from the motor. A high efficiency lead screw and nut assembly converts rotary to linear motion, and because of the high efficiency, e.g. using a recirculatory ball nut, a reverse force will back-drive the motor. There are various internal feedback loops: a current command which is often included in the power electronic amplifier, a force feedback so that the input-output performance is enhanced, and the option to include motor speed feedback using an encoder fitted to the motor shaft. The GPSC will identify both general safety-related issues and fault modes that might affect functionality within an application.

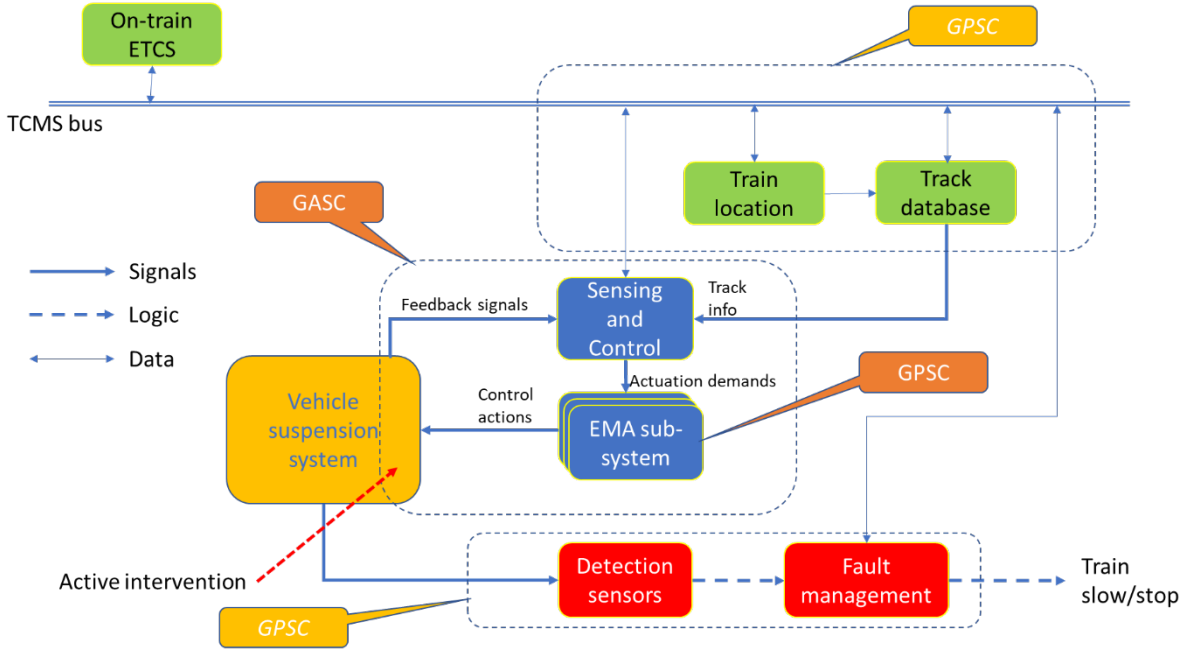


**Figure 5: Generic Active Suspension diagram.**

The overall system diagram for which the EMA might be used is shown in Fig 5, which also shows the interfaces to the EMA. This is generally applicable to various types of active suspension, both secondary

and primary. It includes the possibility of “feedforward” information from a track database system, for example design alignment data such as curvature – this would be described by a separate GPSC. As drawn, there is a detection sub-system which acts independently of the feedback sensors to monitor for incorrect/unsafe operation, including a fault management process that may command an operational change to the train: this may be a desirable approach which would be described by a separate GPSC, but is not an essential system requirement.

The GPSC describes the use of an EMA, which could be used in conjunction with other actuation technology, in order to provide an active suspension function. The system diagram indicates a multiplicity of actuation sub-systems: this may be a coordinated set of actuators providing the required functionality (e.g. two actuators to provide an active lateral secondary suspension), or a scheme involving functionally redundant EMAs, or a combination of the two. This GPSC is focussed upon the intrinsic safety of a single EMA sub-system, whereas coordination of a set of EMAs (or other actuator technologies), application-dependent effects of the GPSC fault modes and the provision of functional redundancy will be covered by the GASC.

A Generic Application Safety Case (GASC) for an active lateral secondary suspension application utilising EMAs would have a more specific version of Fig 5, as shown in Fig 6. It utilises two electro-mechanical actuators (EMAs) connected laterally (horizontally) in parallel with the secondary (airspring) suspension, one on each bogie. Active control is achieved by measuring lateral secondary suspension displacement and lateral body acceleration at each bogie and processing these signals in an appropriate manner to generate lateral force demands for the two actuators. The objective is to maximise the ride quality (measured by lateral accelerometers) whilst ensuring that the available “working space” of the lateral suspension is not exceeded (measured by lateral displacement sensors).

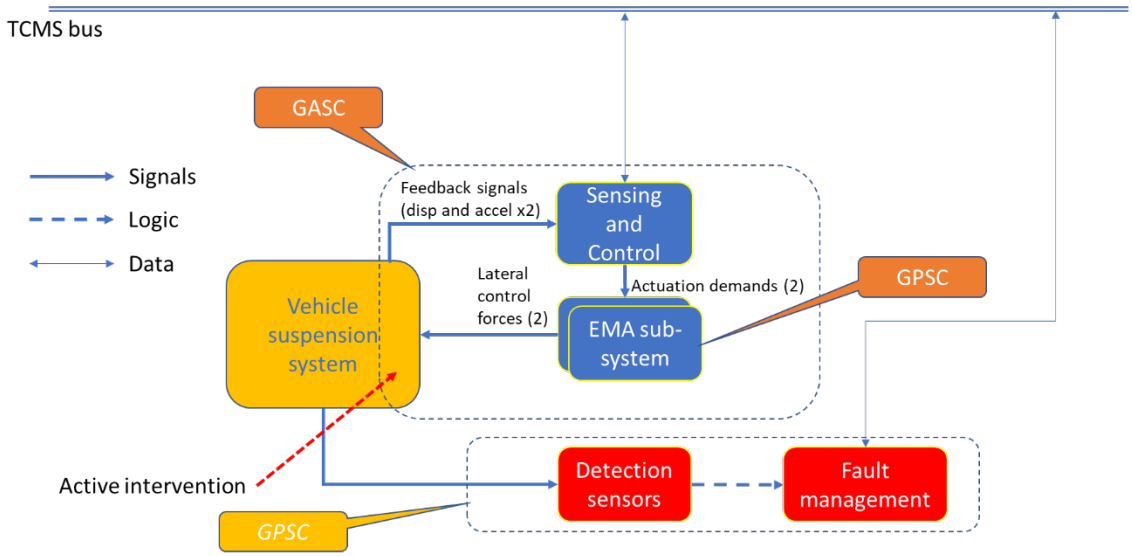


**Figure 6: Overall system diagram for active lateral secondary suspension using EMAs.**

The GASC would assess the effects of the EMA fault modes identified within the GPSC via simulation, laboratory and track tests to assure the safe integration of the EMAs within the active lateral suspension. This example includes a detection system which monitors the acceleration environment on the vehicle body using additional accelerometers in order to detect high levels of acceleration which could arise as a consequence of one of the GPSC fault modes which might otherwise create an unsafe condition. The functionality of this would be described in a “High Acceleration Detection” GPSC.

## 5. Conclusions

The Authorisation Strategy developed as part of the Run2Rail project will therefore consist of:

1. Proving safe integration at the different levels (components, active system, vehicle/network) by means of GPSC, GASC and SASC documents based upon EN50129, for which templates have been developed.
2. Guidelines incorporated into the templates which provide prompts and explanations of what would be needed for an industrial active suspension. Some illustrative examples are included in appendices to each template.
3. A number of GPSC and GASC examples using the templates. These will focus upon the technical aspects and are not expected to be complete.

This combination of documents will help to provide potential industry exploiters with a valuable starting point for a full safety case submission.

This is focussed only upon the Safety aspect of the RAMS process. In particular it does not deal with with operational reliability, and in practice some functional redundancy may be required to deliver the required level.

## Acknowledgment

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 777564.
The authors acknowledge support from all the members of the project partners who have provided advice.

## References

[1] Bruni, S, Goodall, RM, Mei, TX, Tsunashima, H (2007) Control and Monitoring for Railway Vehicle Dynamics, Vehicle System Dynamics, 45(7-8), pp.743-779, ISSN: 0042-3114. DOI: 10.1080/00423110701426690
[2] Directive (EU) 2016/797 of the European Parliament and Council, 11 May 2016, Interoperability of the rail system within the European Union
[3] Directive (EU) 2016/798 of the European Parliament and Council, 11 May 2016, Railway Safety
[4] Commission Implementing Regulation (EU) No 402/2013, Common Safety Method for Risk Evaluation and Assessment
[5] EN 14363:2016+A1:2018. Railway applications. Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests.
[6] Commission Regulation (EU) No 1302/2014, Nov 2014, technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union
[7] European Standard EN 50129:2018; Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling
[8] European Standard EN 50126-2:2007; Railway applications. The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Guide to the application of EN 50126-1 for safety