Contract No. 777564

INNOVATIVE RUNNING GEAR SOLUTIONS FOR NEW DEPENDABLE, SUSTAINABLE, INTELLIGENT AND COMFORTABLE RAIL VEHICLES

Task 3.3 – Proposals for Authorisation Strategy for rail vehicles with active suspensions

Deliverable D3.3

Due date of deliverable: 31/08/2019

Actual submission date: 04/10/2019

Leader/Responsible of this Deliverable: Roger Goodall, HUD

Reviewed: Y

Document status		
Revision	Date	Description
1	27/08/2019	Draft Final issue
2	04/10/2019	Final issue
3	13/03/2020	Version incorporating changes in response to the comments from PO

This project has received funding from Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 777564.

Dissemination Level

PU	Public	✓
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of task: 01/03/2018 Duration: 18 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Roger Goodall/Peter Hughes	HUD	Overall editing plus Sections 1, 2, 3, 4 and 6
Rickard Persson	KTH	Section 4
Stefano Bruni / Francesco Braghin	POLIMI	Section 4.2
Riccardo Licciardello	DICEA	Sections 2.2 and Sect 5

EXECUTIVE SUMMARY

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 task provides a framework for a practical and efficient authorisation strategy based upon existing European regulations and standards.

The declared objectives of Authorisation Strategy task 3.3 are to propose an authorisation strategy for active suspensions, taking into account all reasonably foreseeable failure modes, and to assess them with regard to their likelihood and impact:

- identification of limits to actuation capability that will both deliver the required performance but restrict the impact of failures. Possible methods that can be used include Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA).
- Review of acceptance processes in other industries to check whether they can be adapted to rail vehicles

Despite these ambitious objectives, it should be emphasised that the total Run2Rail resource allocated to this task is 9 man-months, so there is clearly a limit to what can be achieved.

It is well established that active or “mechatronic” suspensions offer performance improvements that cannot be achieved with purely passive solutions. 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.

An assessment of methods used in other relevant industries, i.e. aerospace and automotive, has revealed that they have faced or are facing the same problems as railways. It’s probable that their systems will be more complex than active railway suspensions; also railways have a very different operating environment and they carry large numbers of people, which means that the solutions will inevitably be different.

Existing standards for running dynamics and gauging mandate limit values that still need to be recognised, even with an active system. Therefore, the possible effects of active system faults need

to be assessed and if necessary redundancy techniques should employed to reduce the probability of unsafe failures to an acceptable level.

Since railways already have standards for critical systems with electronics and software, principally written for signalling and train control functions, and the Run2Rail task has taken advantage of these, in particular the idea of using a set of distinct Safety Cases for Generic Products, Generic Applications and Specific Applications (GPSC, GASC and SASC, respectively). A set of templates with guidelines oriented towards active suspension systems has been prepared, and these are supported by four examples, two GPSCs and two GASCs. (The SASC is too specific for an example arising from a research project.) This structured approach provides a modular, reusable set of safety-related documents.

The project team took a decision at an early stage not to deal with the safety assurance of the electronic controller (hardware and software), instead to assume that this can be guaranteed separately. The focus has therefore been at the vehicle system level, within which the controller is identified as a sub-system which would need a Generic Product Safety Case.

The task has also reviewed the implications in terms of possible changes to existing standards, and in particular suggests an authorisation process based upon the GPSC, GASC and SASC and aimed towards a harmonised risk acceptance criterion (now called a Design Target).

ABBREVIATIONS AND ACRONYMS

ASIL	Automotive Safety Integrity Level
CSM	Common Safety Methods
DT	Design Target
EHA	Electro-hydraulic Actuation
EMA	Electro-mechanical Actuation
ERA	European Rail Agency
ETCS	European Train Control System
FBW	Fly-by-wire
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
FTC	Fault Tolerant Control
GASC	Generic Application Safety Case
GPSC	Generic Product Safety Case
LRU	Line replaceable unit
MTBF	Mean time between failures
OEM	Original Equipment Manufacturers
PFCAS	Primary Flight Control Actuation System
RA	Risk Assessment
RAT	Ram Air Turbine
RPN	Risk Priority Number
SASC	Specific Application Safety Case
SC	Safety Case
SIL	Safety Integrity Level
TCMS	Train Control and Management System
TSI	Technical Standard for Interoperability

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Task 3.3 falls within WP3 “Active Suspension & Control Strategy” and the aim is to propose a homologation or authorisation strategy for active suspensions. It is a key part of WP3 and relates principally to Task 3.2 “Implementation of active technology on conventional bogie vehicles and a two-axle vehicle”, but also has input from T3.1 “State of the art of Actuator Technology”. Some impacts are assessed within this report, but in addition T3.4 “Impact assessment support” is linked. The initial proposal stated that T3.3 should:

> “take into account all reasonably foreseeable failure modes, and assess them with regard to their likelihood and impact. This will include identification of technical solutions (e.g. to actuation capability) that will both deliver the required performance and restrict the impact of failures. Possible methods that can be used here are Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Acceptance processes in other industries are reviewed to check whether they can be adapted to rail vehicles."

This a key aspect of Run2Rail’s work: although failures of purely mechanical components or systems can be unambiguously avoided by a combination of conservative design, regular inspection and maintenance, this is not possible for active suspension systems that utilise sensors, actuators, electronics and software which can develop faults without warning. Even with conservative design, the combined failure rates of the components will almost inevitably not be sufficient to meet safety integrity requirements, and no amount of regular inspection and maintenance can mitigate this. This implies the need for either some form of mechanical back-up that maintains safe operation in the case of an active system failure, or functional and/or analytical redundancy within the active system to ensure a sufficient level of safe operation.

A strategy is proposed that is strongly based upon existing European Standards and Regulations, and that will provide a starting point for future preparation of safety cases for active suspensions. It was decided not to deal with the safety assurance of the electronic controller (hardware and software), instead to assume that this can be guaranteed separately. The focus has therefore been at the vehicle system level, within which the controller is identified as a sub-system. This would need a Generic Product Safety Case which would have to demonstrate compliance with EN 50155.

2. BACKGROUND

There has been a significant amount of work on safety principles aimed towards transportation systems, and this section provides a review of other industries' approaches, summarises what the project partners have researched, identifies the relevant standards and proposes an authorisation strategy framework for the Run2Rail project.

2.1 CERTIFICATION FOR OTHER INDUSTRIES

In many senses other industries are ahead of railways in authorisation of their systems or products that involve active control, and so it's useful to study how these industries approach the issue. A number of industries have safety critical requirements, but the survey is restricted to transportation technologies, in particular aircraft and automotive which are the most relevant to railways.

2.1.1 Aircraft certification

The introduction of fly-by-wire (FBW) flight control systems was a watershed development in aircraft evolution because the mechanical or hydro-mechanical controls of the various flight control surfaces were replaced by electrical command signalling and software, and it enabled technical advances to be made which were not possible before [1]. For example, a FBW system can exploit aircraft configurations which provide increased aerodynamic efficiency, especially more lift and lower drag. Generally, these benefits are at the cost of reduced natural stability, including negative stability in which an aircraft is aerodynamically unstable over part its flight envelope but where the FBW system provides stability.

The probability of a catastrophic failure in the FBW system must not exceed $1x10^{-7}$/hour for a military aircraft or $1x10^{-9}$/hour for a civil aircraft [2]. The statistical level of civil aircraft safety, derived from the total number of civil aircraft crashes occurring in a year from all causes divided by the total number of aircraft flying and their annual operating hours, corresponds to $1x10^{-6}$/hour. Typically, the mean time between failures (MTBF) of a single channel FBW system is quoted to be about 3,000 hours. Consequently, the system must incorporate redundancy with multiple parallel channels so that it is able to survive at least two failures. FBW systems are therefore fundamentally based upon the provision and management of redundancy with a variety of architectures for the computing and control hardware.

A quadruplex system is composed of four totally independent channels of sensors and computers in a parallel arrangement to give the required failure survival capability. They are configured such that the system of interconnected sensors, computers and actuators can survive any two failures from whatever cause. The incorporation of a monitoring system to check the correct functioning of a channel by an acceptance test allows the system to identify the failed channel. This is the basis for an alternative failure survival configuration known as monitored triplex[1] composed of three independent parallel channels. Each channel is monitored by a dissimilar system to detect a failure. If this monitoring has a high degree of integrity and confidence level, this configuration can also survive two failures [2].

Aircraft flight controls involve both primary controls (ailerons, flaperons, inboard and outboard spoilers, elevator and rudder) and secondary controls (flaps, spoilers, trim, etc.). These are usually kept separate and in the event of loss of the primary controls the secondary controls can maintain flight, albeit with reduced performance. Servo-hydraulic, electro-hydraulic and electro-mechanical actuators are all used to move the control surfaces, often in combination to provide dissimilar technology thereby avoiding common-mode failures. Duplicated hydraulic and/or electrical power supplies are invariably provided

from more than one engine, and in the case of loss of both power supplies a Ram Air Turbine (RAT) is enabled to supply the auxiliary power for the flight controls.

At some point the multiple actions from the parallel channels must be brought together or "consolidated". In the early days of military aircraft, the quadraplex actuators [1] were connected to the control surface shaft, i.e. mechanical consolidation; later multiple servo-valves fed into a single actuator providing hydraulic consolidation; another option has been a single servo-valve with multiple coils, i.e. electrical or magnetic consolidation. Nowadays, particularly for civil aircraft, there are separate portions of the control surfaces, each with a separate actuator, thereby implementing aerodynamic consolidation.

Modern civil aircraft examples:

1. The Airbus A380 has modal control of yaw, roll and pitch using a multiplicity of actuators and control surfaces (more than 20) [3], which has gravitated from simple functional redundancy on early Airbus FBW systems [4].
2. The Boeing 787 PFCAS System controls 21 flight surfaces and includes a mix of electrohydraulic (EH) and electro-mechanical (EM) servo-actuators with their associated control electronics.

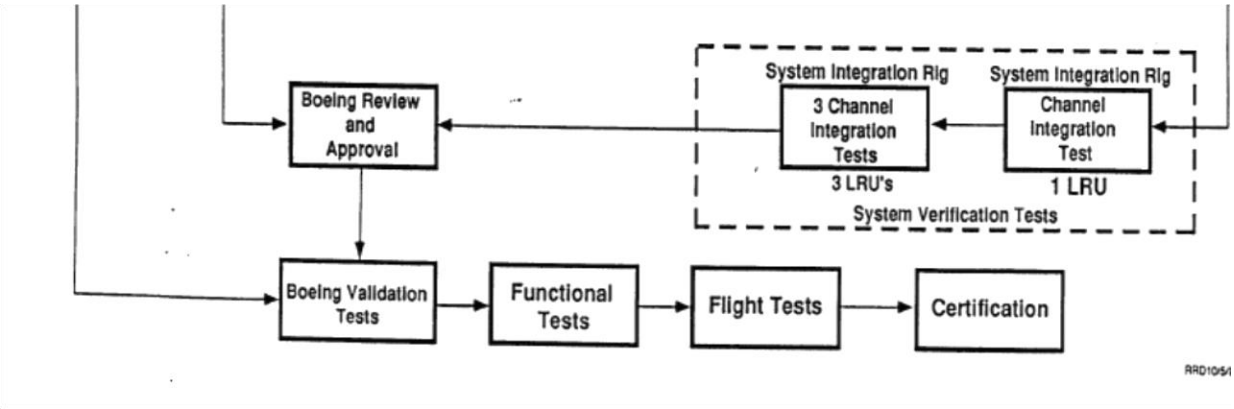


Figure 1: Aircraft certification process

There seems to be limited publicly-available information which is explicitly about certification or authorisation, but part of a diagram from one of the Boeing papers is shown by Figure 1 which illustrates the importance of a Systems Integration Rig as part of the process [5]. A Boeing Design Review which is related to Certification is available [6].

[1] The Solid-State Interlocking used (for example) in UK for signalling/train control is an example of a monitored triplex system, although it works on a 2 out of 3 voting principle and locks out the failed channel. If there is a second failure it reverts to a safe state, i.e. signals at red.

2.1.2 Automotive certification

Electronic systems are increasingly becoming part of modern automotive technology, with things like Cruise Control, Dynamic Yaw Control, Steer-by-Wire, Brake-by-Wire etc., and in the longer term fully autonomous vehicles.

The Automotive Safety Integrity Level (ASIL) [7] is a risk classification scheme defined by the ISO 26262 standard "Functional Safety for Road Vehicles" [8]. This is an adaptation for the automotive industry of the Safety Integrity Level used in IEC 61508 and is an international standard for functional safety of electrical and/or electronic systems in production automobiles. This ASIL classification helps defining the safety requirements necessary to be in line with the ISO 26262 standard.

The standard defines different levels of Severity, Exposure and Controllability[2]. In terms of these classifications an "Automotive Safety Integrity Level D" hazardous event (abbreviated "ASIL D") is defined as an event having reasonable possibility of causing a life-threatening (survival uncertain) or fatal injury (Severity classification S3), with the injury being physically possible in most operating conditions (Exposure classification E4), and with little chance the driver can do something to prevent the injury (Controllability classification C3) . ASIL is stated to be equivalent to SIL3 for railways [7]. For each single reduction in any one classification from its maximum value (excluding reduction of C1 to C0), there is a single level reduction in the ASIL from D. For example, a hypothetical uncontrollable (C3) fatal injury (S3) hazard could be classified as ASIL A if the hazard has a very low probability (E1). The ASIL level below A is the lowest level, QM. QM refers to the standard's consideration that, below ASIL A, there is no safety relevance and only standard Quality Management processes are required.

Electrical Steering is ASIL D, whereas Cruise Control will normally be ASIL A. An interesting statement is that it is generally accepted that each level of ASIL causes a ten-fold increase in cost due to the extra design effort and rigorous validation.

Most Automotive Original Equipment Manufacturers (OEMs) are starting to require ISO 26262 for the New Vehicles they are designing. ISO 26262, which is the Functional Safety Analysis standard comprised of 10 parts, will be released shortly; but even before its release, it is widely being used by European and US Automotive companies. It is being adopted by many Tier One automotive organizations who are finding ISO 26262 conformance a requirement in their Request for Quotes. The expectation is that it's only a matter of time before this permeates to lower tier suppliers such Semiconductor Organizations and Software companies.

The European Directive addressing this topic is 2007/46/EC (dated 5 September 2007), which defines responsibilities to be borne by the different parties involved in the process of approval:

- The manufacturer is responsible to the approval authority for all aspects of the approval process and for ensuring conformity of production, whether or not the manufacturer is directly involved in all stages of the construction of a vehicle, system, component or separate technical unit.
- In the case of multi-stage type-approval, each manufacturer is responsible for the approval and conformity of production of the systems, components or separate technical units added at the stage of vehicle completion handled by him

- The manufacturer who modifies components or systems already approved at earlier stages shall be responsible for the approval and conformity of production of those components and systems.

In contrast with the previously-mentioned ISO 26262, the EU Directive's only use of the word "active" is in the context of active protection systems. "Electronic Control" is mentioned but there seems to be no direct reference, including in the testing requirements, to emerging active technologies such as those mentioned in the first paragraph of this sub-section.

2.1.3 Summary of other industries' certification approaches

It's clear that aircraft FBW systems have evolved a long way from where they started, and certification of today's systems is entirely risk-based exploiting functional and analytical redundancy. The architectures are complex, almost certainly much more complicated than would be needed for rail vehicles, but they are designed to very similar integrity levels [9]. Availability requirements are also probably similar because Delays and Cancellations are a critical performance requirement demanded by aircraft operators, although the maintenance regime is very different.

There is much more information that is publicly available regarding aircraft, but it's clear that the automotive industry is starting to grapple with certification. Various organisations are able to provide an independent safety assurance, but it seems that this is still ultimately the responsibility of the manufacturers. The automotive industry's ASIL measure has many commonalities with those for railway, but has the added dimension of Controllability by the driver. Railways however have the probability of a large number of people involved when something goes wrong, and this must be factored into the safety assessment.

It seems therefore that, while there may be useful lessons to be taken from other industries, there is not an actual process that can be directly copied for use by railways.

[2] Controllability is "avoidance of the specified harm or damage through the timely reactions of the persons involved", and is therefore generally not relevant to railway rolling stock

2.2 BACKGROUND INFORMATION

The research partners have some pre-existing expertise in the area of system safety assessment.
A KTH paper [10] maintained a strong link to EN14363 safe running criteria and proposed a methodology based primarily on FMEA using Risk Priority Number (RPN). It included a definition of 7 generalised failure modes and presented a flowchart which was supported by Fault Tree Analysis (FTA). A Case Study using Simpack simulation of failure mode effects was included.
The Mechatronic Train project [11] included a substantial task concerned with safety and reliability. The approach assumed that functional redundancy would be required and therefore was strongly based upon Fault Tolerant Control (FTC) concepts, aimed towards requirements defined by one of the partners (Deutsche Bahn) for both Fail-to-Safe operation and operational reliability. An operational failure was defined as when one more fault would cause an unsafe condition, in which case the train would have to either slow down or stop. The study developed a database of active system components with well-defined fault states and probabilities.

2.3 RELEVANT REGULATORY & STANDARDISATION (R&S) FRAMEWORK

The existing framework for vehicle authorisation in Europe revolves around the Interoperability Directive (Dir. 2016/797, formerly 2008/57 which is gradually being replaced) and the Safety Directive (Dir. 2016/798, formerly 2004/49, similarly under gradual replacement). The former defines the authorisation process and the TSIs, in particular the TSI Loc&Pas [12] which is valid for locomotives and passenger rolling stock. The latter is intended to cover railway operations rather than vehicle authorisation, but introduces the Common Safety Methods (CSM), including in particular the CSM Risk Assessment (CSM RA) [13], which is relevant for vehicle authorisation. Appendix 1 includes some definitions from the CSM documentation.) TSI Loc&Pas clause 4.2.3.4.2 (running dynamic behaviour) points to an ERA technical document [14] and standard EN 14363 [15] for the assessment conditions, and EN 14363/EN 15686 for the running safety limit values. In the same TSI clause, for active systems there are additional requirements when it is not possible to comply with the limit values for running safety, which require the use of the CSM RA with specified harmonised design target probabilities for the electrical, electronic and programmable electronic part. The design target probability is “highly improbable” for the above active systems which do not lead to compliance with running safety limits.
The CSM RA regulation provides for three risk acceptance principles: the application of codes of practice, a comparison with similar parts of the railway system, or an explicit risk estimation. For active suspensions, this translates to

- demonstration of compliance to existing standard(s), mainly EN 14363;
- comparison with a reference active suspension system that has an existing safety case;
- a risk-based approach compliant with other railway approaches; or

- a combination of the above approaches.

In summary, in order for vehicles with active systems in the running gear to be authorised (e.g. active steering systems), two possibilities, to be used as alternatives or in combination, are:

- "EN 14363 route": the EN 14363 / EN 15686 running safety limits are always complied with, even in the presence of faults (possible e.g. with active systems relying on mechanical backups such as passive springs in parallel to the actuators), but this would likely require on-track testing for every possible fault mode and such systems have a relatively low performance;
- "TSI active systems route": it is acknowledged that the fault modes would cause running safety limits to be exceeded, and the assessment is focussed on demonstrating that they are "highly improbable".

Regarding the first option, EN 14363 [15] is referred to by the TSI to assess running dynamic behaviour. However the TSI does not explicitly "call" EN 14363 for active systems, it is indicated as mandatory specification in clause §4.2.3.4 for running dynamics in general. The relevant clause of the standard is §5.2.2 fault modes. The reference here is to the 2016 version which is not yet indicated in the TSI. The most relevant clause that is an opening to the RUN2Rail authorisation strategy is:

"If running safety cannot be demonstrated for a relevant fault mode, limiting criteria for a safe operation shall be determined and possible measures for supervision and/or mitigation shall be defined to reduce the criticality of the fault mode."

As it stands the standard requires the assessment of running safety for any fault mode in which the vehicle might have to operate. On the other hand the RUN2Rail process would not require running safety assessment if the design is such to comply with the TSI requirements above, for which however a harmonised design target is missing for the "purely mechanical part".

The European Railway Agency technical document [14] concerns the application of EN 14363 within the framework of the TSI. Regarding fault modes, in which those of active systems are included, the document modified the text existing in the 2005 version including the following relevant provisions. "*The criticality (the combination of probability and consequence) of fault modes shall be analysed. The assumptions and results shall be reported. For each critical fault mode identified it shall be clearly stated what the consequences in terms of the safety aspects within the scope of this document would be and what, if anything, is required to be done in terms of testing or other analysis. If there is a low probability of occurrence of the considered fault mode based on the results of the analysis, the safety margin included in the limit values of the assessment quantities may be reduced."…. "It is allowed to use specific limit values depending on the type of the fault mode characteristics and their effects.*"

Regarding the second option, in RUN2Rail reference is made to the EN 50126-1/2 (2017) series of standards [16], as also suggested in the ERA Guide on possible tools supporting the CSM Regulation (12).
https://www.era.europa.eu/sites/default/files/activities/docs/collection_of_ra_ex_and_some_tools_for_csm_en.pdf

The authorisation strategy proposed in RUN2Rail refers to both the above possibilities, and develops GPSC and GASC according to EN 50126-1/2 which include, in the safety case, assessment of conformity with EN 14363.

As mentioned previously the electronic systems have not been covered in this research, it should be noted that the electronic controller has to meet EN 50155, and all other on-board systems containing electronics need to be compliant with this standard and must pass the type tests defined in this standard (e.g. EMC, environmental conditions (heat, cold, humidity), vibration and shock etc.) This also applies to sensors and actuators which usually contain electronics.

2.4 PROPOSED STRATEGY FRAMEWORK

2.4.1 Active suspension types

Three active suspension types have been identified that are expected to be distinct in terms of their safety authorisation implications. This following sub-sections provide a description and explanation.

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 vertical and lateral active secondary suspensions are likely to degrade ride quality but will not cause unsafe instability, excessive wheel loads or derailment. However, active secondary suspensions, particularly tilting, may have an influence on gauging, which is a safety relevant topic.

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 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 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 now a risk-based authorisation methodology will be needed meet the specified integrity levels defined for the associated hazards.

2.4.2 Systems incorporating electronics and software

The CENELEC standards EN50126-1/2 (2017) deal with railway safety cases where electronics and software are a key part of the system, and in particular supports the principles of establishing multiple related safety cases, stating that the following three different types of safety case can be considered:

- A Generic Product Safety Case (GPSC) to provide evidence that a generic product is safe in a variety of applications
- A Generic Application Safety Case (GASC) to provide evidence that a specific class of applications are safe

- A Specific Application Safety Case (SASC) that is relevant to one specific application

Table 1 lists these: the first column is from the standard, and the other two suggest descriptions that are relevant to active suspension systems and the Run2Rail research.

Table 1: Development of CENELEC safety case structure

General descriptions from CENELEC standards	Descriptions specific to Active Suspension	Possible T3.3 research aspects
Generic Product Safety Case GPSC *It provides evidence that a generic product is safe in a variety of applications*	*This provides evidence that an Active Suspension Controller product (set of actuators, sensors and controller) is safe in a variety of Active Suspension applications* ➢ *May need different GPSCs for different (actuator) technologies*	• *Assessment of actuator technologies* • *Probabilities of fault modes* • …
Generic Application Safety Case GASC It provides evidence that a generic product is safe in a specific class of applications	*This provides evidence that an Active Suspension Controller product is safe in a specific class of Active Suspension Applications* ➢ *May need different GASCs for different class of Active Suspension Application, e.g. active guidance control, active steering control, active secondary suspension etc.*	• *Generic assessment (by simulation?) of (for example) active secondary v. active primary solutions* • …
Specific Application Safety Case SASC This would be relevant to one specific application	*This would be prepared for a particular Active Suspension Controller product for a specific Active Suspension Application (on a specific train and a specific route)*	• *Case studies of applications from T3.2* • …

Figure 2 is an adaptation of a diagram in [16]. It illustrates how the three types of Safety Case can be linked in a generalised sense. The left-hand panel of the figure illustrates safety cases for generic products (GPSCs), which are the components that make up the system; for example, actuators or 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 integrated from the components and how the overall application has been configured to ensure safety. Whilst there may be a GPSC for each component, the GASC must describe the interfaces between the components and possible failure modes of the interfaces. 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, 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 a specific vehicle operating on a specific route. 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.

The various SC documents can therefore be used provide modularity and substantial re-usability.

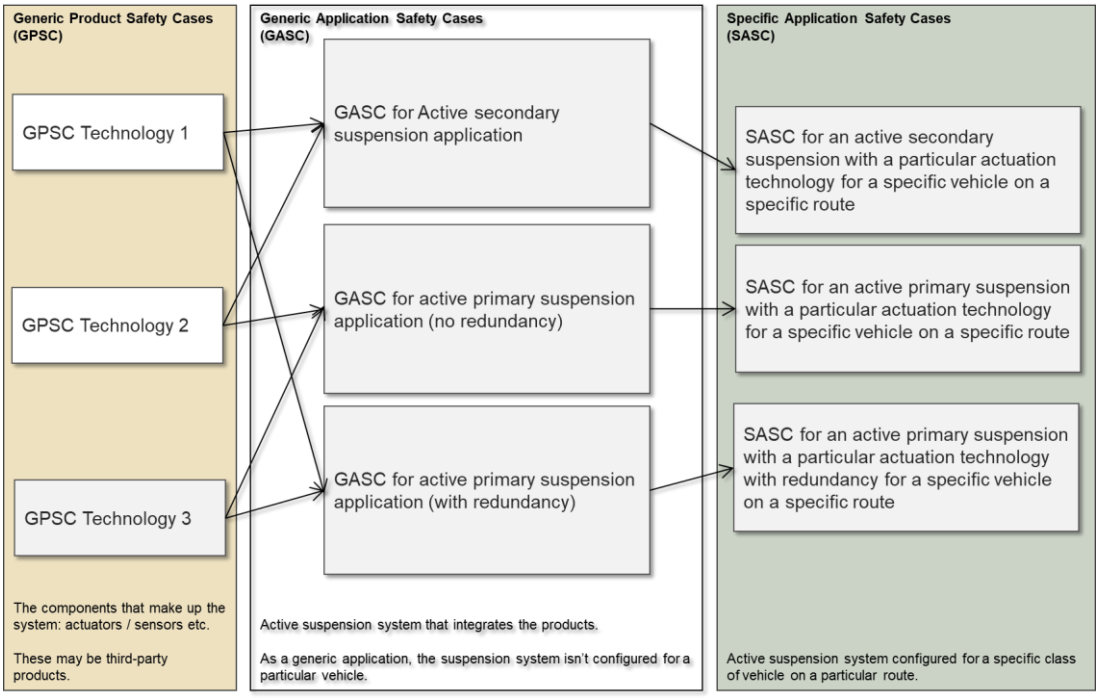


Figure 2 Links between Safety Case documents

2.4.3 Safety Case framework

Producing actual safety cases is not realistic within the resources allocated to the task, not least because of the limited resources, and so it has been decided that the Authorisation Strategy should consist of a framework of templates, guidelines and examples, as illustrated in Figure 3: Authorisation strategy framework. The blocks with a thick border identify specific research activities undertaken within WP3.3: the two GPSC examples will address the two actuation technologies that were prioritised in WP3.1, and the two GASC examples relate to concepts chosen as part of WP3.2. There is a template with guidelines for the SASC, but since these are generally very specific (e.g. to a particular vehicle, fleet, route etc.) they will not be dealt with in the T3.3 research task.

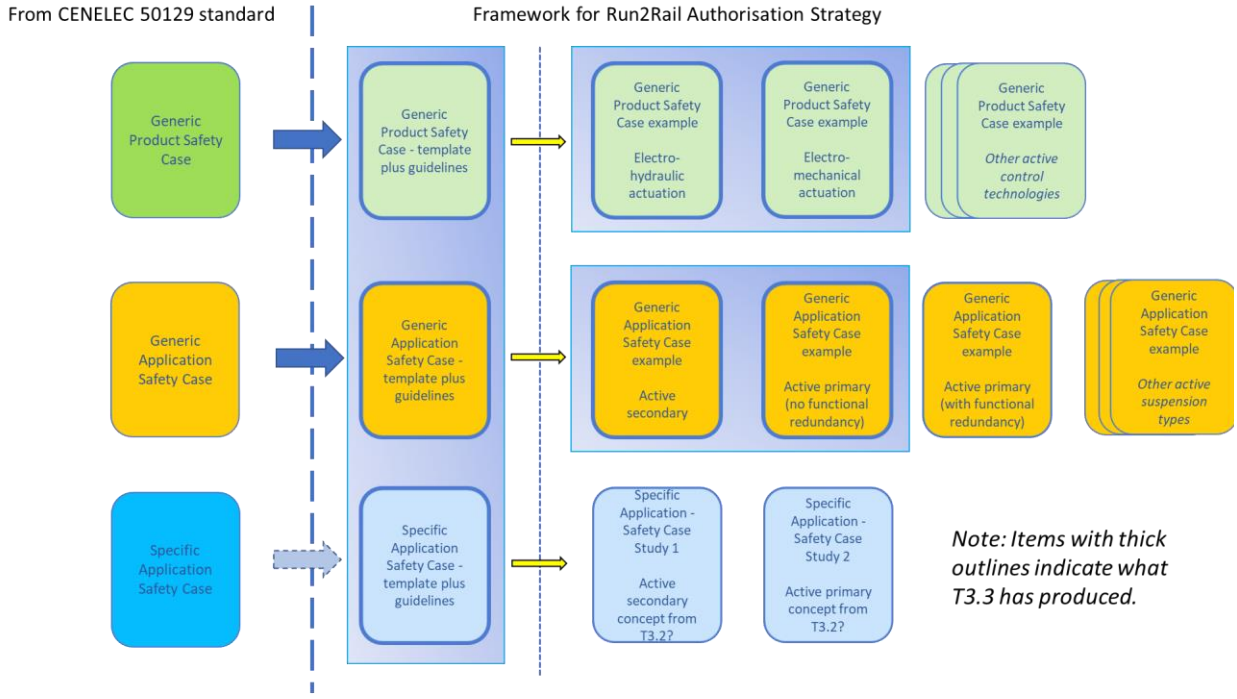


Figure 3: Authorisation strategy framework

The overall approach therefore is to prepare an authorisation strategy based on the existing safety-case way-of-thinking for the future (nearer future for secondary suspension, further away for primary suspension). This incorporates the current way of thinking as a part of the GASC or SASC, but extends the current way of thinking by exploring how additional tests could be specified for a specific application based on simulation results. A risk-based approach will be needed for the more advanced active suspension concepts, i.e. where functional redundancy is used.

The Strategy developed as part of the Run2Rail project therefore consists of:

1. A set of templates for the GPSC, GASC and SASC documents based upon [16].

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 prepared as part of task WP3.3, as shown in Figure 3. 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.

3. TEMPLATES FOR SAFETY CASE GUIDELINES

As explained, producing actual safety cases is not realistic within the task, and so this section describes a set of templates for the GPSC, GASC and SASC.

- Generic Product Safety Case Template Plus Guidelines
- Generic Application Safety Case Template Plus Guidelines
- Specific Application Safety Case Template Plus Guidelines

The templates are based on the requirements for safety cases described in EN50126, which provides a detailed description of the information that should be contained within a safety case. The standard sets out that the main sections of a safety case shall be: the Safety Management Report; the Quality Management Report; and the Technical Safety Report. Guidance is given for content that should be provided within each section. The templates are structured in accordance with this structure and provide detail on the information that should be provided for a safety case for an active suspension system. For example, EN50126 describes that the Safety Management Report should contain information on configuration management. Within each of the templates, guidance is provided at the appropriate section describing the information on configuration management relevant to an active suspension system that should be provided. These templates also emphasise that the complete development life cycle must be followed and documented, and they suggest the inclusion of a V-diagram or similar.
The guidelines included within the templates are in colour-coded text as follows:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is

required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Section 4 describes how the templates have been part completed for the two GPSCs and the three GASCs in order to provide examples. Since they are derived from the templates they also provide a comprehensive description of what will be required for industrial practitioners to develop safety cases in the future.

The three templates are provided as Appendices 8.2-8.4.

4. EXAMPLE SAFETY CASES

As noted previously, since Run2Rail is a research activity the examples that have been derived from the templates are not intended to be complete, partly because of the limited resources but also because some of the sections such as the Quality Management Report are only appropriate for a real industrial organisation.

The aim therefore has been to provide examples that are indicative, i.e. sufficient that a reader can pick up the main ideas underlying the examples.

The four examples are provided as Appendices 8.5-8.8. Some attention is given to the need to describe the complete development lifecycle as part of the process, and the examples include part-completed V-diagrams.

4.1 INTRODUCTION

The examples developed in the Run2Rail project are based upon a system shown in the generalised diagram given in Figure 4.

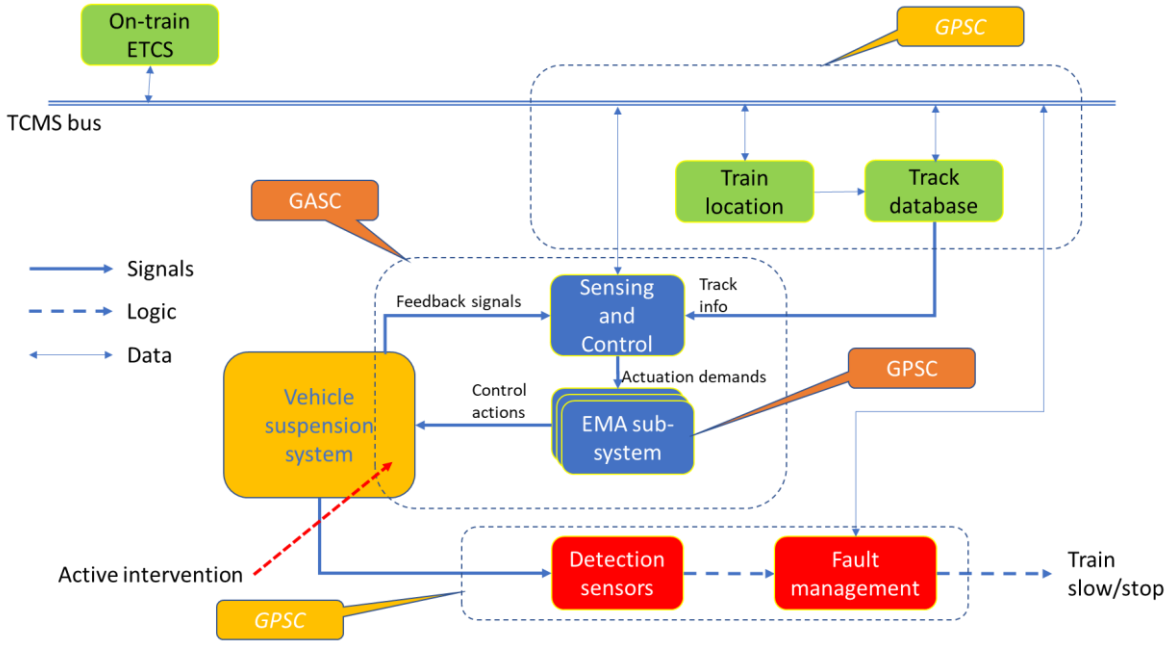


Figure 4 Generalised active suspension diagram

This includes the possibility of three GPSCs and can apply to a variety of secondary or primary active suspension applications:

1. An actuation system, shown here as an electro-mechanical product (EMA) but other technologies are possible
2. A device to provide “feedforward” information from a track database system, for example design alignment data such as curvature
3. 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 may be a desirable approach

Items 2 and 3 are not essential system requirements, whereas an active suspension must have at least one actuation device and Figure 5Figure 5 is an extended version of Figure 3 (adapted from [16]). This illustrates how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems.

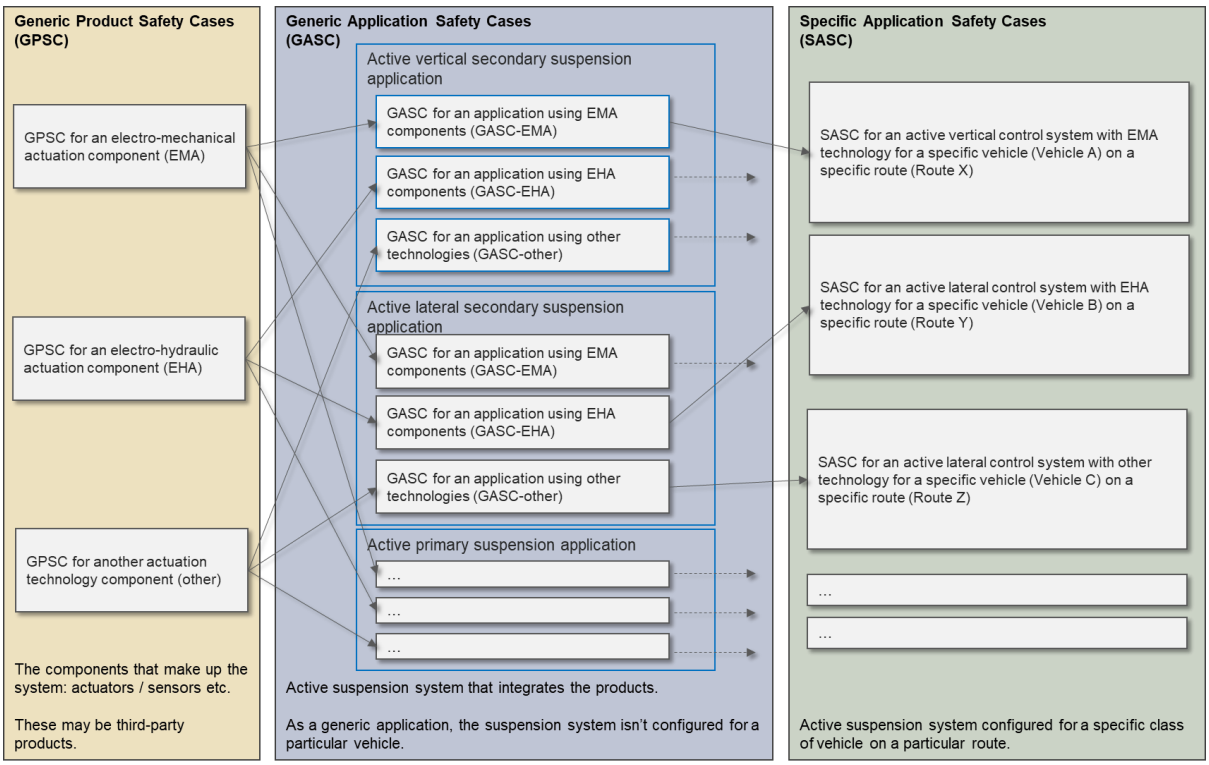


Figure 5 Relationship between SC documents

In fact, the system diagram Figure 4 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 actuators, or a combination of the two. This GPSC is focussed upon the intrinsic safety of a single actuation sub-system, whereas coordination of a set of actuators (perhaps including more than one actuator technology) or the provision of functional redundancy will be covered by the GASC.
There are therefore two GPSC examples (electro-hydraulic and electro-mechanical technology, which were prioritised from Task 3.1) and two GASC examples taken from T3.2.

4.2 GENERIC PRODUCT SAFETY GUIDELINES

4.2.1 Electro-hydraulic

The electro-hydraulic (compact) actuator is one of the most used in railway vehicle active suspensions today. It was given high scores in the evaluation made in Task 3.1 for application in the secondary suspension for vehicles both with two suspension stages and for application in the suspension for vehicles with one suspension stage. The prevailing design of EHAs is pressure-controlled, which means that the controller gives a reference to the EHA with relation to the wanted hydraulic pressure, and hence the applied force. Figure 6 shows the main parts of the actuator.

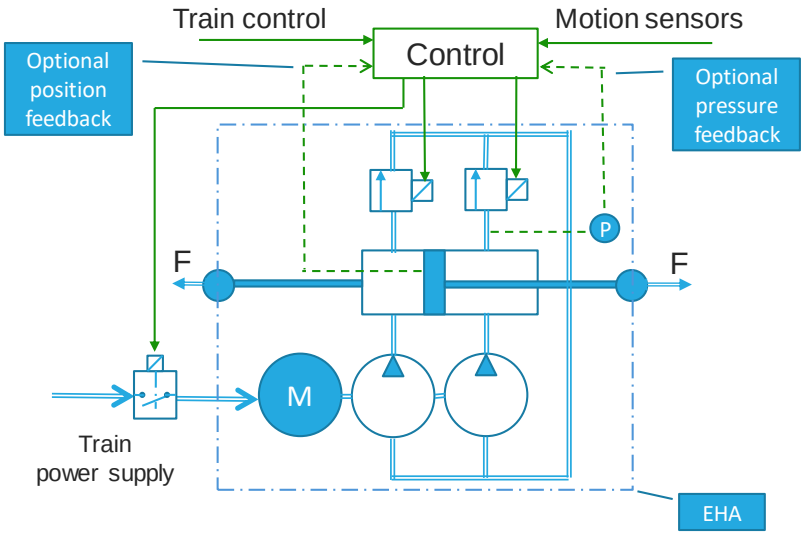


Figure 6 Scheme of EHA actuation

The EHA is a robust design with failure modes as free (mechanically broken) and zero force (passive). In some applications this means that system is safe even in failed state. The GPSC, included as an example, is principally based upon explicit risk estimation and analysis approach. This approach, following the EN 50126, can be applied when the safety cannot be ensured in all failure states.

4.2.2 Electro-mechanical

The electro-mechanical actuator is the second actuator type that was prioritised in WP3.1. It has previously been used widely in tilting trains and sometimes for active suspension development projects.

Figure 7**Error! Reference source not found.** provides a diagram of the EMA scheme and its interfaces within the overall system. It has 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 a DC electrical motor driven by a power amplifier comprising high frequency switched semiconductors giving high efficiency bi-directional control of the power supplied to/from 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 is focussed upon identifying failure modes for the EMA, the effects of which in terms of safe operation must be analysed within each application, which may have differing needs in terms of safe failures.

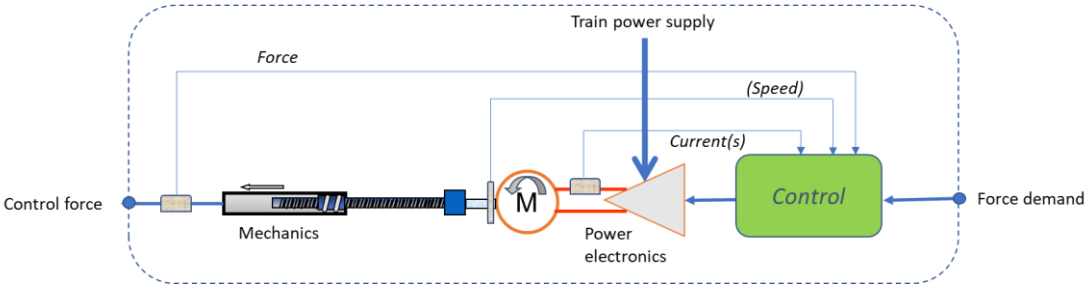


Figure 7 EMA system block diagram

4.3 GENERIC APPLICATION SAFETY GUIDELINES

4.3.1 Active lateral secondary suspension

Active lateral control of the secondary suspension is probably the most relevant example because it is more commonly considered by rail manufacturers than active vertical.

The system description is shown in Figure 8. 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).

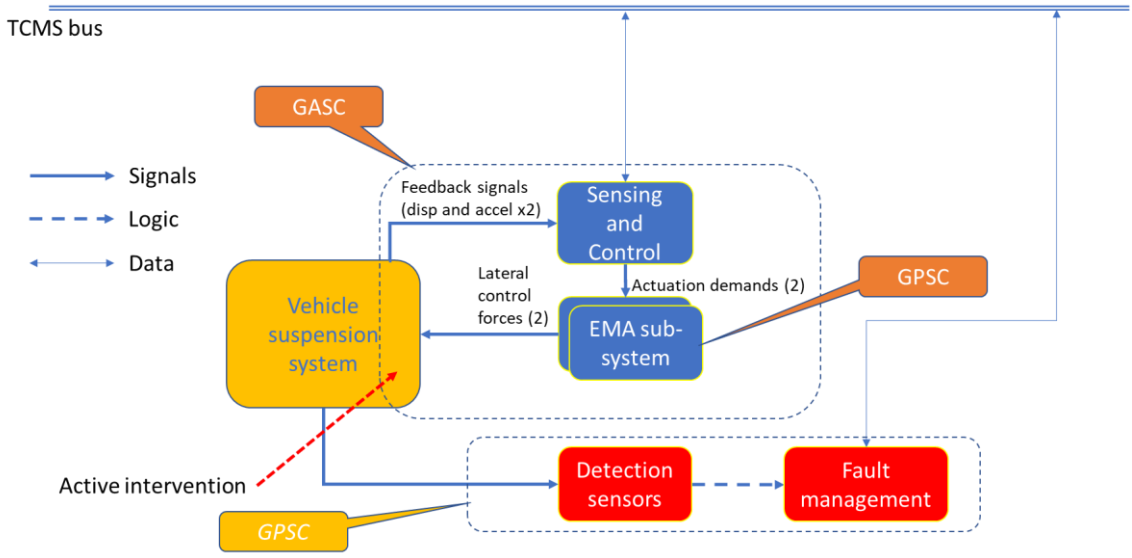


Figure 8 Overall system diagram for active lateral secondary suspension

The scheme indicates an additional GPSC as a simple, independent monitoring system which detects high levels of lateral acceleration on the vehicle body, but the corresponding example GPSC has not been prepared as part of the Run2Rail project.

4.3.2 Active Primary – no redundancy

An example is provided for an active primary suspension. The main goal of the active suspension is to provide active steering of the wheelsets in a vehicle with bogies, thus reducing creep forces, improving running safety and reducing wear and damage of the wheels and of the rails especially in short radius curves.
The active primary suspension considered in this case is not resorting to redundancy of actuators, the back-up to the active suspension in case of actuator failure being provided by a passive primary suspension in parallel to the active suspension, see Figure 9.

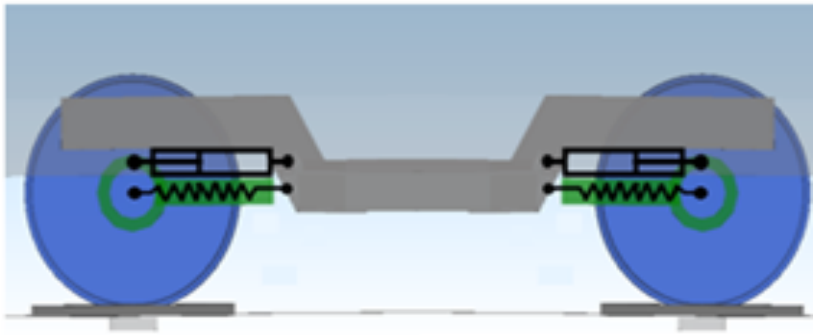


Figure 9 - Schematic side view of the bogie showing the arrangement of the active primary suspension with EHAs in parallel to a passive suspension

As described in Chapter 3 of Deliverable D3.2, the use of a passive primary stiffness in parallel to the active suspension reduces somehow the performance of the vehicle, however, this active primary suspension scheme can be designed to be tolerant to failures in the actuators, sensors and control system.

The system description is shown in Figure 10. It utilises two electro-hydraulic actuators (EHAs) per wheelset (therefore a total of four EHAs per bogie), one on each side of the bogie. The actuators are mounted in longitudinal direction between the bogie frame and one axle box of the wheelset. Active control is achieved by measuring the bogie frame yaw rate at each bogie and processing these signals together with vehicle speed available from the TCMS to define a desired steering angle of each wheelset relative to the bogie frame. The angle is then actuated using as the reference displacement for the two actuators mounted on the two sides of the same wheelset opposite displacements having appropriate amplitude so that the wheelsets can be steered to take a nearly radial direction.

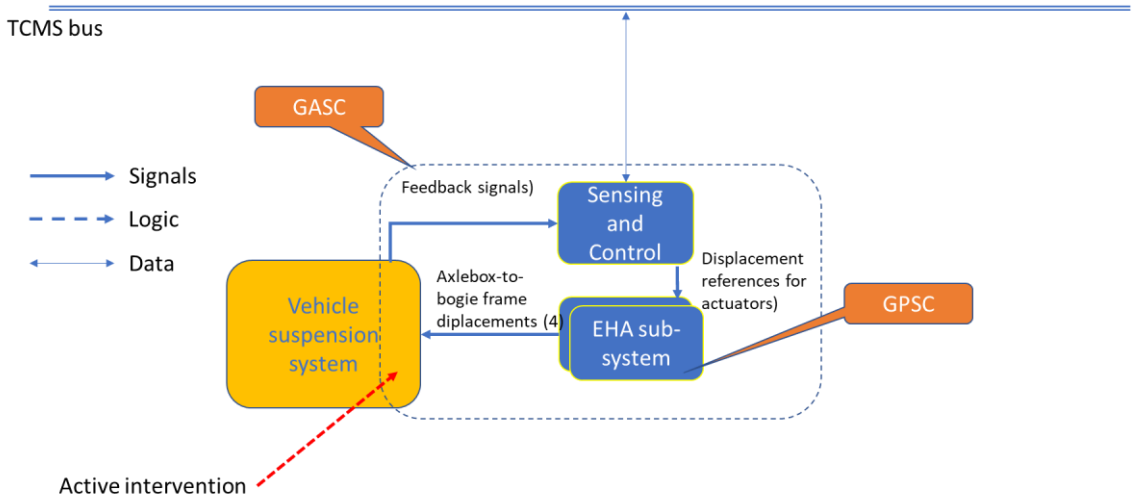


Figure 10 - Overall system diagram for active primary suspension

5. OUTPUTS TO REGULATION AND STANDARDISATION

The strategy described above based on GPSC, GASC and SASC templates plus examples for GPSCs GASCs may be used for vehicle authorisation purposes under the umbrella of the TSI Loc&Pas requirement for running dynamic behaviour (§4.2.3.4.2).

The Active Lateral Suspension GASC example focuses on demonstrating compliance with the EN 14363 limit values (systems with mechanical backup).

The Active Steering (Primary Suspension) GASC example falls under the case of the TSI "additional requirements when active systems are used: "*…When active systems (based on software or programmable controller controlling actuators[3]) are used, the functional failure has typical credible potential to lead directly to 'fatalities' for both of the following scenarios:*

1. failure in the active system leading to a non-compliance with limit values for running safety ...,

2. failure in the active system leading to a vehicle outside of the kinematic reference contour of the carbody and pantograph, due to tilting angle (sway) leading to non-compliance ...

Considering this severity of the failure consequence it shall be demonstrated that the risk is controlled to an acceptable level."

Demonstration of compliance (conformity assessment) is described in §6.2.3.5:

"The compliance with the safety requirements that are specified in clauses 4.2.3.4.2, ...in terms of level of severity/consequences associated to hazardous failure scenarios shall be demonstrated by one of the two following methods:

1. Application of a harmonised risk acceptance criterion associated to the severity specified in the clause 4.2 (e.g. 'fatalities' for emergency braking.). The applicant may choose to use this method, provided that there is an available harmonized risk acceptance criterion defined in the CSM on Risk Assessment and its amendments [13].

….."

Since the issue of the TSI, a harmonised risk acceptance criterion (redefined as 'design target' DT) has been established in the CSM RA regulation (now Reg. 2013/402/EU as amended by Reg. 2015/1136/EU) and inserted into the "explicit risk estimation" part of the CSM RA:

"2.5.5 Where hazards arise as a result of failures of functions of a technical system.., the following harmonised design targets shall apply to those failures:

(a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.

(b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable.

...

2.5.6....the harmonised design targets set out in point 2.5.5 shall be used for the design of electrical, electronic and programmable electronic technical systems....

They shall neither be used as overall quantitative targets for the whole railway system of a Member State nor for the design of purely mechanical technical systems.

For mixed technical systems composed of both a purely mechanical part and an electrical, electronic and programmable electronic part, hazard identification shall be carried out ... The hazards arising from the purely mechanical part shall not be controlled using the harmonised design targets set out in point 2.5.5.

Within the above R&S framework, and considering the proposed GPSC, GASC, SASC structure, a possible process is outlined for the technical assessment for vehicle authorisation comprising "mixed technical systems composed of both a purely mechanical part and an electrical, electronic and programmable electronic part".

1. Analyse fault modes.
2. Set CSM RA (probability) Design Target corresponding to catastrophic consequences for the electrical, electronic and programmable electronic part. **Demonstrate that this part meets the DT**.
3. Mechanical components (actuators…..), first step:
    a. set probability DT for the purely mechanical part the same as CSM RA DT, including ensuring functionality by means of design, maintenance and inspection requirements.
    b. Analyse redundancy requirements (dimensional and cost constraints) and classify fault modes accordingly:
        i. Case 1, fault modes with no problem in meeting the CSM RA DT: redundancy with no mechanical backup. **Demonstrate that the design solution meets the CSM RA DT for these fault modes.**
        ii. Case 2, fault modes close to the DT but not quite if an acceptable redundancy level (dimensional/cost constraints) is chosen: iteration to check whether a slightly higher DT may be set or reduced safety margin in the limit values of the EN 14363 assessment quantities (which are recognised in some cases to be conservative). This depends on the consequences of the fault mode as determined with a validated MBS model. An initial screening may be performed without following the full EN 14363 process. If the final decision is to set a higher DT then the full simulation process is required.
        iii. Case iii, fault modes that will be far from compliance with the DT because of the constraints. A mechanical backup is needed and must be adequately designed.
4. Second step, set differentiated DT for specific fault modes and demonstrate case 2, bring case 3 fault modes to case 2 through mechanical backups.
    a. Case 2, full EN 14363 simulations to determine a severity index for the fault mode consequences (e.g. [17]). For severity index less than or equal to that corresponding to "running safety limits met", set higher DT (trying to respect an inverse proportionality principle, criteria are needed for this). **Demonstrate that the design solution meets the DT for these fault modes.**

[3] Note: active systems based on analogue systems (i.e. not based on software or programmable controller) are also possible.

b. Case 3. The fault modes that have not fallen in Case 1 or Case 2 fall in Case 3. Design mechanical backup ('barrier' of CSM RA) so that the consequences are brought to those of case 2.

5. Final step, set DT for Case 3 (now 2) fault modes and demonstrate compliance
   a. Case 3 (now 2), full EN 14363 simulations to determine a severity index for the fault mode consequences (now with mechanical backup). For severity index less than or equal to that corresponding to "running safety limits met", set higher DT (trying to respect an inverse proportionality principle, criteria are needed for this). **Demonstrate that the design solution meets the DT for these fault modes.**
6. Static commissioning and on-track testing is required for the fault modes for which the simulation results were not conclusive.

6. SUMMARY AND CONCLUSIONS

This deliverable for sub-task 3.3 has provided an overview of the research work undertaken. The area of authorisation of rail vehicles is a complex one with a diverse range of standards, directives and other documentation, and so the work has been largely technically focussed so that it sits alongside the other research studies, but it is recognised that it's not complete. In addition to this deliverable document, the project has produced three templates for the GPSC, GASC and SASC documents with guidelines to help authors in industrial organisations, supported by four example documents, two GASCs and two GASCs. As mentioned, the example SCs are not intended to be complete, rather they sit alongside the template/guidelines to provide illustrations and clarfications.

7. REFERENCES

1. Collinson, R. (1999). Fly-by-wire flight control. COMPUTING & CONTROL ENGINEERING JOURNAL, 141-152.
2. Kornecki, A. J., & Hall, K. (2004). Approaches to assure safety in fly-by-wire systems: Airbus vs. Boeing. Conf. on Software Engineering and Applications. IASTED.
3. Le Tron, X. (2018, June). A380 Flight Controls overview - presentation at Hamburg University of Applied Sciences 2007. Retrieved from Hamburg University of Applied Sciences: http:/hamburg.dglr.de
4. Briere, D., & Traverse, P. (1993). AIRBUS A320/A330/A340 electrical flight controls - A family of fault-tolerant systems. FTCS-23 The Twenty-Third International Symposium on Fault-Tolerant Computing, (pp. 616-623).
5. McWha, J. (August 2003). Development of the 777 Flight Control System. AIAA Guidance, Navigation, and Control Conference. Austin, Texas: AIAA.
6. Boeing 787–8 Critical Systems Review Team. (2013). Boeing 787–8 Design, Certification, And Manufacturing Systems Review. Federal Aviation Administration.
7. Automotive Safety Integrity Levels. (2018, June). Retrieved from https://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level
8. ISO 26262. (2018, June). Retrieved from https://en.wikipedia.org/wiki/ISO_26262
9. Yeh, Y. (1998). Design Considerations in Boeing 777 Fly-By-Wire Computers. Third IEEE International Conf. High-Assurance Systems Engineering Symposium.

10. Qazizaden, A., Stichel, S., & Persson, R. (2016). Proposal for Systematic Studies of Active Suspension Failures in Rail Vehicles. Proc IMechE Pt F, 199 - 213.
11. Mechatronic Technologies for Trains of the Future. (2001). BE97-4387 Final Report. Brite-Euram BE97-4387.
12. Technical Standard for Interoperability 1302/2014 "Locomotives and passenger rolling stock" (TSI LOC&PAS)
13. Commission Implementing Regulation (EU) 2015/1136, "Common safety method for risk evaluation and assessment"
14. ERA/TD/2012-17/INT rev 3.0 "Running Dynamics, Application of EN 14363:2005 – Modifications And Clarifications"
15. BS EN 14363:2016+A1:2018 Railway applications. "Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests"
16. EN50126-1/2 (2017) "Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS)"
17. Fu, B., Bruni, S. (2019). Fault-tolerant analysis for active steering actuation system applied on conventional bogie vehicle. 26th IAVSD Symposium on Dynamics of Vehicles on Roads and Tracks, 12-16 August 2019, Gothenburg, Sweden

8. APPENDICES

8.1 DEFINITIONS AND REQUIREMENTS FROM THE EU'S COMMON SAFETY METHODS REGULATIONS

Basic definitions

- "Hazard" means a condition that could lead to an accident
- "Risk" means the frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm;
- "Catastrophic accident" means an accident typically affecting a large number of people and resulting in multiple fatalities
- "Critical accident" means an accident typically affecting a very small number of people and resulting in at least one fatality

Safety probabilities

- "Highly improbable" means an occurrence of failure at a frequency less than or equal to 10^{-9} per operating hour
- "Improbable" means an occurrence of failure at a frequency less than or equal to 10^{-7} per operating hour

8.2 TEMPLATE FOR GENERIC PRODUCT SAFETY CASE GUIDELINES

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Template for Generic Product Safety Case Guidelines

This document is one of three templates that has been prepared to allow for safety cases to be developed for active suspension systems for rail vehicle.
The three templates are for a:

- *Generic Product Safety Case (GPSC) – this document;*
- *Generic Application Safety Case (GASC); and*
- *Specific Application Safety Case (SASC).*

These templates provide a general framework for all active suspension systems for railway applications. Figure 1 is adapted from a European Standard [1] and illustrates how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems. The various SC documents therefore provide modularity and substantial re-usability.

The left-hand panel of the figure illustrates safety cases for generic products (GPSCs), which are the components that make up the system; for example, actuators or sensors. The components may implement different technologies for example electro-mechanical actuation devices or electro-hydraulic activation. A GPSC will provide a safety case for the product and may describe, for example,

individual failure modes such as failure of the component to provide any force, or the component locking up. 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.

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 integrated from the components and how the overall application has been configured to ensure safety. Whilst there may be a GPSC for each component, the GASC must describe the interfaces between the components and possible failure modes of the interfaces. The GASC will consider failure modes of the application such as providing lateral force to an axle when not required. The GASC will also describe non-function 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 1); 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 a specific vehicle operating on a specific route. 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.

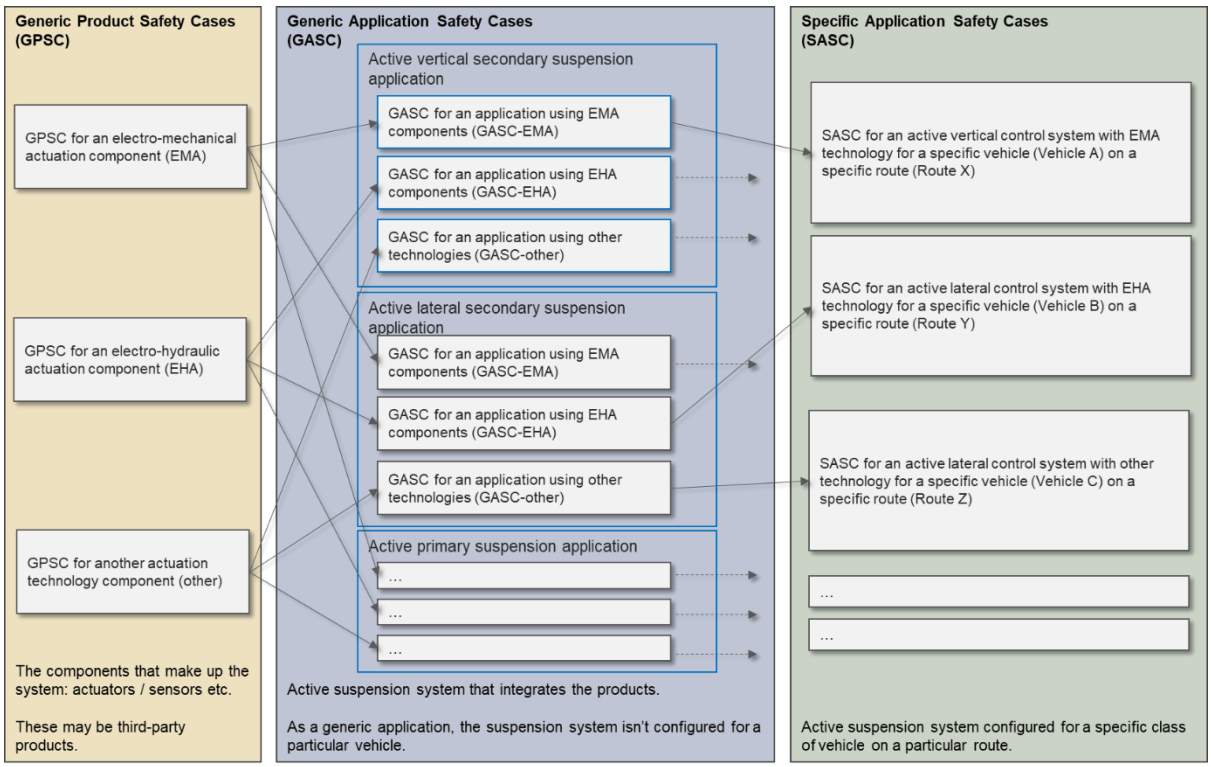


Figure 1: Illustration of the combination of numerous safety cases for different specific applications, adapted from [1]

Consistent with the European Common Safety Method (CSM) the templates allow for safety to be demonstrated using one of the following methods:

- *demonstration of compliance to existing codes e.g. EN 14363 [2];*
- *comparison with a reference active suspension system that has an existing safety case;*
- *a risk-based approach compliant with EN 50126 [1] and EN 50657 [3]; or*
- *a combination of the above approaches.*

Contents

The introduction section will be the same regardless of the method that has been chosen to demonstrate safety compliance. It is expected that this guidance will apply to one of three types of suspension system:

Type I: active secondary suspensions including tilting systems. It is expected that for Type I systems, whilst faults in either the vertical or lateral active secondary suspensions are likely to degrade ride quality, they are unlikely to cause unsafe instability, excessive wheel loads or derailment. As such, it is expected that safety assurance for Type I systems would be provided by demonstrating compliance to EN 14363.

Type II: active primary suspensions with mechanical constraints. In such systems, safe operation in the event of an active system fault can be assured by means of a combination of mechanical back-ups and limited force capability from the actuators. Where Type II systems have mechanical constraints to assure against unsafe instability, excessive wheel loads or derailment, it is expected that safety assurance for Type II systems could be provided by demonstrating compliance with EN 14363.

Type III: active primary suspensions with functional redundancy. In many cases, the constraints associated with Type II systems may limit the performance of an active primary suspension. Type III active suspension systems overcome the constraints by use of control systems. To achieve the safety integrity required for railway systems, any such control system is likely to implement functional redundancy to reduce the likelihood that failure of an active component will result in adverse safety consequences. For Type III systems, the requirements of existing standards for stability, derailment and wheel loads (including EN 14363) would still apply, but would need to be complemented by a risk-based demonstration of correct safe behaviour.

This safety case provides evidence that *provide the working title or description of the generic product* is adequately safe when integrated within active suspension systems. It can be referred to in various GASCs according to the class or type of active suspension application as listed above.

This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the generic product and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.

Provide any additional information necessary for a reader to understand the reason for the safety case, for example background to the project, regulatory or legislative requirements particular to the product or its intended application.

An example is provided in Section 8.1.1.

This safety case applies only to a *provide the working title or description of the generic product.*

Describe the generic product and the main features of the system. Describe the boundaries and interfaces of the system, clearly describing components at the interface that are outside the scope of this safety case.

Generic Application Safety Cases and Specific Application Safety Cases *provide references if applicable* support this safety case and describe:

- reasonably foreseeable safety hazards associated with the installation, operation, and maintenance of generic applications and their specific applications; and
- the controls required to reduce the risk associated with these hazards to an acceptable level.

An example is provided in Section 8.1.2.

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations (European Union, 2013). Figure 2 is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

The three approaches are not exclusive and could be used in combination. *Describe the approach that has been used for the generic product.*
An example is provided in Section 8.1.3

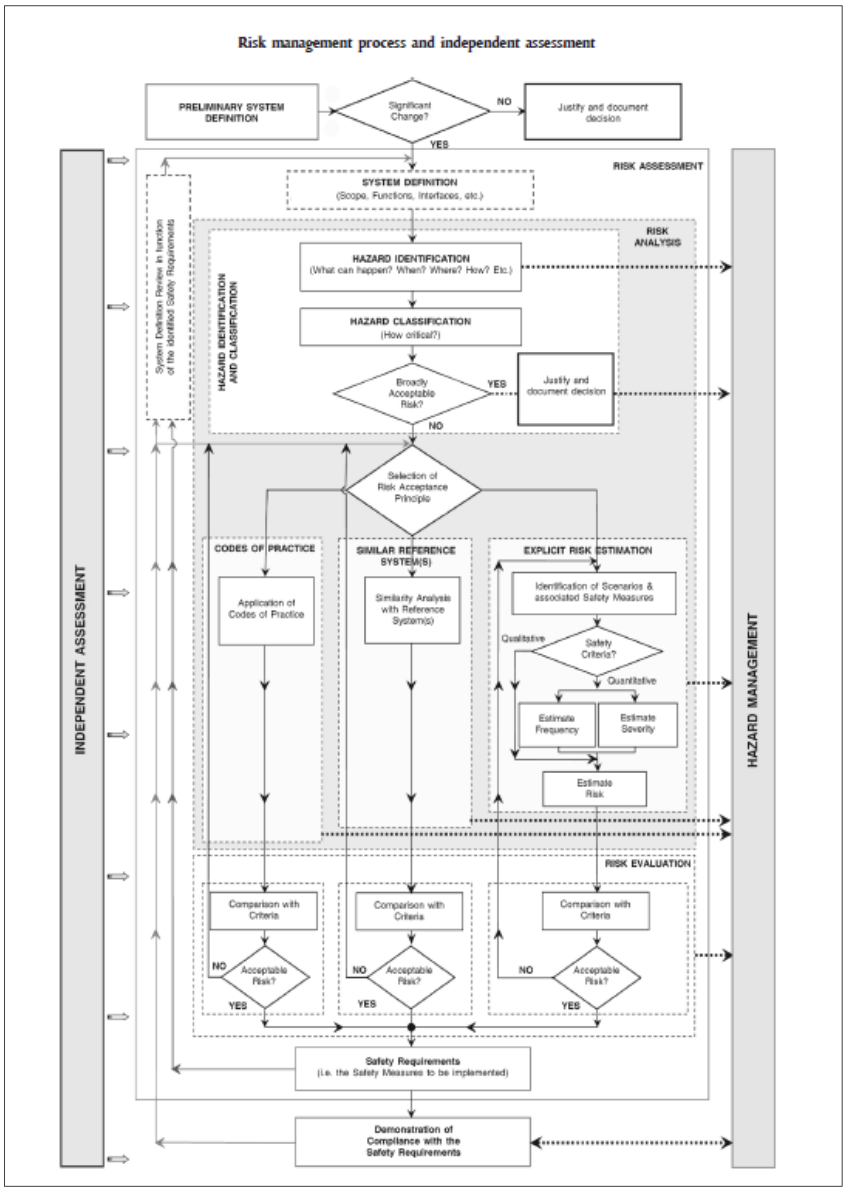


Figure 2: Overall approach to providing safety assurance [4]

The detailed demonstration of safety compliant with this overall strategy will be achieved through compliance with the European standard for demonstrating reliability, availability, maintainability, and safety for railway applications (European Union Standard EN 50126). This standard requires a safety case to be developed that is comprised of:

- system description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

A System Description is required regardless of the method that has been chosen to demonstrate safety compliance.

Describe the generic product: it is strongly recommended to provide a block diagram of the system architecture. The nature of the block diagram may vary depending on the point in the design process. For example for a generic product, detailed design may not be available as such the block diagram will probably be only a description of the main functional components of the proposed system. Where a detailed design is available, the block diagram may be schematic description of the actual architecture of the proposed system.

Describe the function of each of the subsystems shown in the diagram and its interfaces with other subsystems. Provide a description of the interfaces between the generic product and users and external systems.

Describe the operation of the generic product during normal operation and, where applicable, degraded operation. Describe alarms generated by the generic product together with the conditions under which they arise and the intended response to alarms. Where appropriate the description of the generic product should be supported by use cases or use of other design techniques such as event sequence diagrams.

Where possible describe physical design of the generic product or any physical design constraints. Describe physical interfaces with other systems.

Where safety demonstration is to be achieved by comparison to a reference system, the system description shall describe both the reference system and the new system; a subsection is required that lists all differences between the generic product and the reference system.

An example is provided in Section 8.2.

An example system description is shown in Figure 3.

Refer to figures in Section 8.2

Figure 3: Example system description block diagram

The system description must provide an indication of how safety will be demonstrated for each subsystem. Consistent with the approach described by the European Union (2013) there are three approaches listed on Page 2, viz:

- *demonstration of compliance to EN 14363;*
- *comparison with a reference active suspension system that has an existing safety case;*
- *a risk-based approach compliant with EN 50126 and EN 50657; or*
- *a combination of the above approaches.*

Table 1 Sub-system list

Subsystem	Approach to demonstrate safety
Name of the subsystem	*Approach to safety demonstration from the list above*
Name of the subsystem	*Ditto*
etc	*etc*

[List fault modes v. sub-systems list here, e.g. as in the example GPSCs]

Note regarding proof of safety by reference to a similar subsystem.

There are two ways safety can be demonstrated by reference to a similar subsystem.

Firstly where the similar subsystem has an approved safety case, then the safety case for the subsystem can be used as the demonstration of safety. For example the proposed active suspension system may contain a communications interface to received train speed information from existing on-board systems. The communications interface may be a high-integrity device for which a safety case already exists. In such case, reference to the existing safety case provides a substantial part of the safety demonstration for that subsystem. In addition to reference to the existing safety case it will still be necessary to demonstrate that:

- *operation and maintenance of the subsystem within the proposed system is fully in accordance with the scope of the existing safety case; and*
- *the interfaces between the subsystem and other subsystems have the required safety integrity.*

Secondly, it is possible that the reference system does not have an explicit safety case. This can occur when a subsystem or component has been used for a long time in railway applications. Sometimes components were developed prior to a need for specific safety demonstration. Rather the long history of use of the components across a large number of applications has provided proof in service *that the component or subsystem works correctly and safely in a wide range of applications. In such case, it will be necessary to demonstrate that:*

- *operation and maintenance of the subsystem within the proposed system is consistent with how the subsystem has been used throughout its life to establish proof in service of safety; and*
- *the interfaces between the subsystem and other subsystems have the required safety integrity.*

A Quality Management Report is required regardless of the method that has been chosen to demonstrate safety compliance, although the level of detail will vary depending on the method. If the safety case is based entirely on demonstrating compliance to EN 14363, then the QMR is required only to show that sufficient quality controls are in place to ensure adequately compliance. Since a risk-based safety case requires considerably more analysis, there will be a requirement to demonstrate that suitable quality management processes are in place for the additional activity, in particular to demonstrate that processes are appropriate for the selection and implementation of the safety techniques described in the Safety Management Report.

This section describes the quality management processes applied during the design of the generic product.

Describe the quality management system applicable during the design, and where applicable development, of the generic product. Provide a list of standards, processes, procedures and other documentation that comprises the quality management system applicable to the design, and where applicable development, of the generic product. List all internal documents such as policies and standards as well as external documents such as customer requirements, standards, or codes of practice. Justify why these documents are appropriate for the generic product. Include quality management documentation related directly to design and development activities, as well as supporting activities such as training, supplier management, purchasing etc.

Wherever possible refer to an accredited quality management system and provide evidence of currency of the system, for example of copy of a valid accreditation certificate. Describe the scope of the quality management system and demonstrate how it covers activities undertaken in the development of the generic product.

Where activities are taking place between more than one organisation, show how the different quality management systems interface; demonstrate that all activities are covered by the quality management process of one of the organisations.

For each organisation describe the structures to ensure that quality is managed throughout the organisation. Describe the oversight activities that take place to ensure that quality management processes are operating as intended.

Describe the organisational structure applicable for the development of the generic product. Where more than one organisation was involved clearly show the interfaces between the organisations. Describe the responsibilities of each organisation and each person. It is strongly recommended that an organisation chart is used.

Clearly show the safety organisation for the development of the generic product. Show the roles and responsibilities of all staff involved in safety-related activities. Clearly show how the safety organisation complies with the independence requirements specific in EN50129 §5.3.3. List the staff who were incumbent in the roles throughout the entire project, provide details of the qualifications and experience of the staff that make them suitable for the roles; include details of membership of any professional organisations.

Show what evidence will be provided to demonstrate that staff in safety-related roles carried out their responsibilities; this requirement may be met by listing the sign-off requirements for all documents that contain safety-related information and showing which staff in the safety organisation will be responsible for sign-off. Sign-off should include responsibilities for authorship of a document, independent review, and oversight to ensure that a correct process has been followed.
Where staff require specific skills to perform their safety-related duties, provide evidence of training and assessment for those skills; provide evidence that their skills were current at the time of undertaking work. Provide evidence of professional memberships appropriate to the task.

List the quality management processes that are in place for:

- *product design and development*
- *validation and verification activities*
- *purchasing and supplier management*
- *inspection and testing*
- *non- conformance detection and corrective actions*
- *installation and commissioning*
- *configuration management including control of parts, products, documents and data*
- *personnel competence and training*
- *audits and assessments*
- *management review process*

For each process, list the people within the organisation structure who are responsible for: complying with the process; checking the results of the process; overseeing operation of the process and ensuring the process is correctly completed.
Provide a schedule of assurance activities (audits of other activities) that were undertaken to determine whether each process was correctly undertaken. List the results of all assurance activities. List all non-compliances that were detected and the corrective actions that were taken.

An SMR is required regardless of the method that has been chosen to demonstrate safety compliance, although the level of detail will vary depending on the method. If the safety case is based entirely on compliance on EN 14363, the SMR will describe the:

- *methods that will be used to demonstrate that no further safety analysis is required*
- *tests that will be conducted in accordance with EN 14363 and a description of why these tests are adequate to fully demonstrate the correct behaviour of the system.*

Where a risk-based approach is to be undertaken, the SMR will provide considerably more detail including the selection of risk identification and analysis techniques (for example FMEA) and an explanation of why these techniques are adequate and sufficient. The SMR should be consistent with the information in the safety plan or describe any differences between the safety plan and the activities that were undertaken.

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic application is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

This section describes the safety management techniques that were employed during the design, and where applicable development, of the generic product. This section should refer to the safety plan that was used for design and development activities. Describe the criteria that was used to determine acceptability of residual safety risk; where necessary refer to national legislation on acceptability of safety risk. It is recommended that legal advice is sought if the acceptability criteria are unclear.

Describe and provide a diagram of the safety lifecycle that was employed. If a Safety Plan exists for the development activities, describe any deviations from the safety plan and approval for the deviations from the Independent Safety Assessor (ISA). Describe the techniques that were used for:

- *hazard identification and risk assessment;*
- *design and development of risk controls;*
- *demonstration of suitability of risk controls; and*
- *demonstration on acceptability of residual safety risks.*

Show where the activities were carried out during the safety lifecycle. Describe any standards, guidelines, codes of practice or other documents that were used during the activities.

Compliance with EN 50126 is facilitated when a V lifecycle is applied to product development. Figure 4 is reproduced from [1] and shows a V lifecycle. It is strongly recommended that the SMR structures the safety management activities in a form that can be readily understood as a V lifecycle.

It should be noted that the electronic controller has to meet EN 50155, and all other on-board systems containing electronics need to be compliant with this standard and must pass the type tests defined in this standard (e.g. EMC, environmental conditions (heat, cold, humidity), vibration and shock etc.) This also applies to sensors and actuators which usually contain electronics.

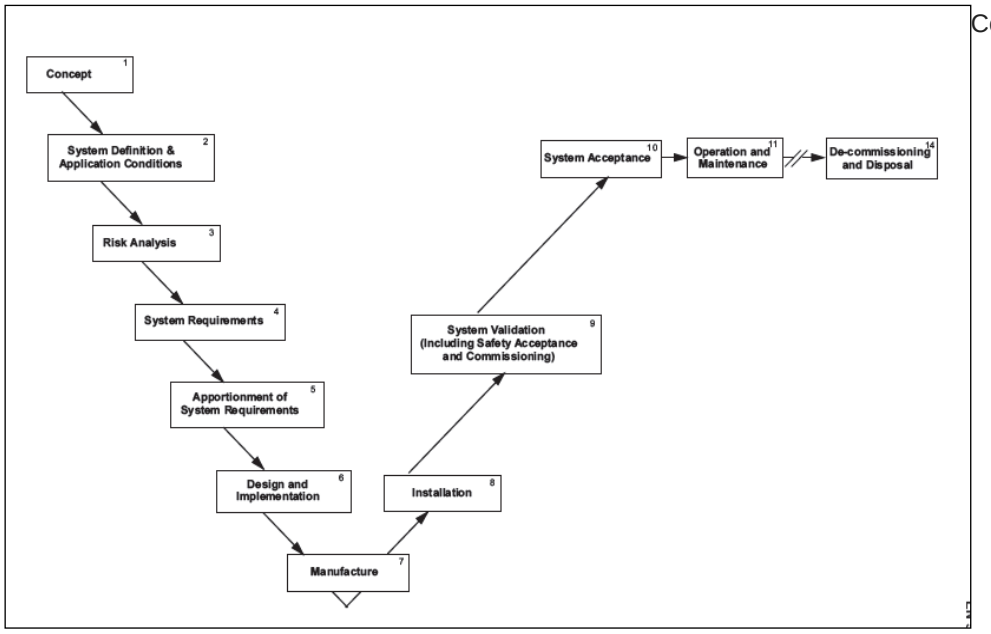


Figure 4: V lifecycle reproduced from [1]

Describe details of all techniques applied and, if necessary, justify any deviation from standard techniques; explain the guidewords that were used during a failure modes and effects analysis. It is essential that justification is provided to describe why these techniques are appropriate to the design, and where applicable development, of the generic product. Where it is foreseeable that specific products will contain software or are configured by data, describe the software safety techniques and measures that are to be applied in accordance with EN50657.

Provide evidence to demonstrate that these activities cover the full scope of the generic product as described in the Section 2.

Provide documentary evidence, or refer to other documents that show that the techniques were applied correctly and that the results of each activity were integrated into the design and development lifecycle. Demonstrate that documents have been signed-off in accordance with the sign-off requirements described in Section 3.

The SMR needs to identify the techniques that will be followed to produce the results shown in the TSR (see Section 5). Amongst other evidence, the TSR requires evidence of correct functional behaviour and demonstration that the product's effect within an active suspension system cannot cause an unsafe condition when operating as designed. It may be practical to integrate the tests to provide this evidence with other functional testing that demonstrates the system meets its functional specification. In these cases, the SMR will need to show how the functional testing activities integrate. It must be clear which evidence from functional testing will be used in the TSR.

Example content can be provided to demonstrate a part of the information that would be required for the example system shown in Figure 3.

A TSR is required regardless of the method that has been chosen to demonstrate safety compliance, although the level of detail will vary depending on the method. If the safety case is based entirely on compliance to EN 14363, the TSR will contain the results of simulation tests. Where a risk-based approach is taken, the TSR will provide the documentation created as a result of implementing the techniques described in the SMR.

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

This section is required regardless of the approach taken to assure safety.

Provide a list of all design documentation associated with the product for use within an active suspension system. For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles.

As above, no example should be provided because any example would be fictional.

Where the safety argument is based entirely on compliance with EN 14363, this section would be simply a list of documentation that provides the results of the tests defined in the SMR in accordance with EN 14363.

Provide a list of the safety analysis techniques described in the SMR. For each technique, provide the technical results. For example if an FMEA is stipulated in the SMR, then provide details of the FMEA, details of staff who were involved together with references to the QMR that describes staff expertise. Provide the results of the FMEA.

Two examples can be provided here to show example of: what sort of documentation would be demonstrated for EN 14363 compliance; and what sort of evidence is provided for a risk-based approach.

Where the safety argument is based entirely on compliance with EN 14363, a hazard log discussing possible fault modes would not be required.

The following hazard log presents the safety hazards (possible safety-related fault modes) identified during the safety analysis.

Hazard summary table.

Hazard ID	Hazard name	Status	Other responsible party	Risk	Comments	Reference to other hazards
e.g. H001	*e.g. Insufficient yaw stiffness*	*[open / closed / deleted]*	*[no] or name of other party*	*risk ranking*	*comment*	

An example summary hazard table can be provided that is relevant to the example system shown in Figure 3.

Provide a detailed description of each hazard.

Hazard ID	*Provide a hazard ID number that corresponds with the hazard summary table.*
Hazard name	*Provide a hazard name that corresponds with the hazard summary table.*
Status	*Provide a status that corresponds with the hazard summary table.*
Hazard cause	*List the causes of the hazard, provide full technical detail or a reference to where detail can be found.*
Hazard consequence	*Where possible described the con*
Hazard source	*Describe the analysis technique where the hazard was identified, if necessary list more than one technique. Refer to the results of the processes described in the SMR.*
Severity	*Describe the reasonable worst case that could occur if the hazard were to manifest. Refer to the risk calculation method described in the SMR.*
Frequency	*Describe the likelihood of the nominated severity occurring. Refer to the risk calculation method described in the SMR.*
Risk	*Describe the risk considering the severity and frequency of the hazard. Refer to the risk calculation method described in the SMR.*
Safety requirements	*Describe, or provide reference to, all controls necessary to reduce the risk to an acceptable level. Safety requirement may include function requirements of the active suspension system, non-function requirement, operational and maintenance procedures. Fully describe any assumptions regarding the system, its operation and environment that were made during the analysis of the hazard.*
Justification of risk acceptance	*Provide a description of why the safety requirements are adequate to reduce the safety risk to an acceptable level.*
Interface hazard	*Describe whether the safety requirements for the hazard require activity by another party, if so identify the other party.*
Reference to further analysis	*Where necessary describe where further analysis or description of the hazard can be found.*
Comments	*Provide any further discussion of the hazard as necessary.*
Proof of hazard closure	*State where evidence of closure of the hazard can be found, in many cases the evidence will be another part of the TSR.*
Date added	*State the date the hazard was added to the hazard log; this might be the data of the safety analysis that first identified the hazard.*
Date closed	*State the date the hazard was closed; this might be the data of the publication of the documentation that describes all safety requirements for the hazard.*
Change log	*Describe any changes made the hazard, its analysis, description, safety requirements etc.*
Reference to other hazards	*Where a hazards is a specific case of, or a cause of, another hazard, the parent or child hazards should be listed here.*

Example hazard descriptions can be provided that are relevant to example hazard summary table shown above.

This section is required regardless of the approach used to demonstrate safety. Where safety is being demonstrated by compliance with EN 14363, this section will include the results of the functional tests. Where a risk-based approach is applied this section will include the results of analysis or simulation.
Provide evidence that the system, when working as intended without faults, does not produce an unsafe condition. For example, there will be a need to demonstrate that the design constraints of the system prevent wheel unloading to a point that derailment can occur for all cases based on foreseeable vehicle loading, track curvature, track cant, cross-winds etc.
For a risk-based method of safety demonstration, it is necessary to demonstrate that all safety requirements identified in the hazard log have been met in so far as they relate to the functional behaviour of the system.
It may be adequate to provide evidence for only the whole active suspension system, however for complex systems that include software or are configured by data, it may be infeasible to provide exhaustive testing of all foreseeable states of the system. In such cases it will be necessary to provide assurance of the correct operation of all subsystems as well as the results of functional testing that demonstrate correct operation of the overall system. Refer to EN50657 for information on how to demonstrate correct software function. In these cases there will also be a need to demonstrate that the programmable electronics that implement the software function correctly.
Two examples can be provided here to show example of: what sort of documentation would be demonstrated for EN 14363 compliance; and what sort of evidence is provided for a risk-based approach.

This section is required regardless of the approach used to demonstrate safety. Where safety is being demonstrated by compliance with EN 14363, it may be possible for the evidence required in this section to be provided by completing tests in accordance with EN 14363.
Provide evidence that the system remains safe in the presence of both random and systematic faults. Where safety is being demonstrated by compliance to EN 14363, it may possible to provide this evidence during functional testing or simulation. For example it may be possible to perform a function test with an active damping component inactive or set at its softest setting.
For a risk-based demonstration of safety, it will be necessary to perform analyses that specifically consider faults and their effects, such as Fault Tree Analysis (FTA), Failure Modes Effects And Criticality Analysis (FMECA), Functional Failure Analysis (FFA) and Common Cause Failure analysis (CCF).
This section must demonstrate that either:

- *the system remains safe in the presence of multiple simultaneous faults, or*
- *a combination of failures that leads to unsafe behaviour has such a low likelihood that the risk of multiple simultaneous faults is so low that the risk is acceptable.*

When considering the effect of multiple faults, independence of components must be demonstrated. Where there is a single underlying cause that can cause multiple faults, these faults cannot be considered independent. For example a single cause such as failure of a power supply or water ingress may introduce multiple simultaneous faults to the system: these faults are not independent since they occur as the result of the same cause. The point is especially relevant when considering redundant components that, for example, may contain identical software.

Where necessary it must be demonstrated how faults will be detected and corrected. For example a system that uses a two-out-of-three redundant architecture may be safe only if the failure of a single system is detected within an hour of the fault occurring. In these cases it is necessary to demonstrate how the fault will be detected and what actions will be taken to ensure safety, including immediate actions to mitigate the effect of the fault and remedial actions. It is necessary to demonstrate that the likelihood of the fault not being detected is so low that the residual risk is acceptable.

Two examples can be provided here to show example of: what sort of documentation would be demonstrated for EN 14363 compliance; and what sort of evidence is provided for a risk-based approach.

This section is required regardless of the approach used to demonstrate safety.

Provide analysis to demonstrate that external influences and their effect on safety have been considered. External influences include: weather conditions; electro-magnetic interference; physical impacts; unauthorised access to, or use of, the system; vandalism; temperature extremes; contamination by water, smoke, pollution etc.

Provide information on how external influences will be detected and how the system will remain safe in the presence of external influences. There will always be external influences, or combinations of external influences, that will defeat the inherent safety of the system. These cases must be identified and credible information should be provided explaining why the likelihood of these events is so low that the residual risk is acceptable.

It is possible that all information relevant to this section has already been included in other parts of the TSR. In such cases, this section should still be included to facilitate demonstration of completeness of the safety case. It is not necessary to repeat information, rather this section can refer to where the required information can be found in other parts of this document.

An example can be provided based on the system description provided in Figure 3.

This section is required regardless of the approach used to demonstrate safety.

Provide a full list of all rules, conditions, constraints and assumptions that must be maintained for the system to remain in a safe state. Where necessary provide references to other documentation that detail the necessary information; for example the system maintenance manual. Where assumptions have been made in the safety case, evidence must be provided for why the assumptions are reasonable.

It is possible that all information relevant to this section has already been included in other parts of the TSR. In such cases, this section should still be included to facilitate demonstration of completeness of the safety case. It is not necessary to repeat information, rather this section can refer to where the required information can be found in other parts of this document.

An example can be provided based on the system description provided in Figure 3.

This section provides enumerated information that supports the safety argument for the system. In some cases the safety argument relies on, for example, failure rate data or information showing that a component will operate after immersion in water. In many cases these data can be sourced from

component manufacturer's data sheets. In other cases, however, specific tests must be carried out for the purpose of this safety case. This section includes the relevant information.
If safety is being demonstrated by compliance to EN 14363, it is possible that no information is required in this section. In such cases so that completeness of the safety case can be demonstrated, the section header should be included in the safety case document and information should be included justifying why no detail is required.
Describe the safety quantification testing that was performed, describe the experimental method, and the results of the experiments. Make clear why the results are relevant to the safety argument being presented in this safety case. Where necessary refer to other parts of the safety case, for example information on safety-related application conditions and assumptions that are relevant to the results of the tests.
An example can be provided based on the system description provided in Figure 3.

It is possible that no additional information is required to support the safety argument. In such cases, in order to demonstrate completeness of the safety case, the heading should be retained and a note should be made that no further information is necessary.
Describe any further information that is relevant to the safety argument that has not been included in other parts of this document. In particular, where the information in the TSR demonstrates that any tests were failed, provide a description of the failed test, an analysis of the impact of the failure, and information on how the system will remain safe regardless of the failure. Where necessary refer to other parts of this safety case.
An example can be provided based on the system description provided in Figure 3.

A conclusion is required for all safety cases.

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

1. EN50126-1/2 (2017) “Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS)”
2. BS EN 14363:2016+A1:2018 Railway applications. “Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests”
3. European Standard EN 50657:2017; Railways Applications. Rolling stock applications. Software on Board Rolling Stock; European Union; 2013.
4. Commission Implementing Regulation (EU) 2015/1136, “Common safety method for risk evaluation and assessment”

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.
List any related safety cases, such as safety cases for sub-systems or components that are required as a part of the generic product.

This provides example texts that are directly linked to the GPSC text. There is also a separate, fuller example document.

> This safety case provides evidence that the electro-mechanical actuation system (EMA) with associated sensing and control can operate safely when used within active suspension systems. It is intended that this document be referred to by appropriate GASCs according to the class or type of active suspension application as listed above.
>
> This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the generic product and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.
>
> Active suspension systems invariably require a controllable force- or torque-generating device plus sensors and control electronics. This GPSC is intended to provide evidence that the EMA has the necessary safety-related characteristics for a range of active suspension possibilities. For this reason it includes aspects that may not be required for all such possibilities, in which case any restricted scope of this GPSC is identified in the GASC, perhaps also in the SASC.
>
> The EMA uses an electric motor, which can be DC or various forms of AC machine, combined with gearing. In this EMA the gearing is a ball- or roller-screw arrangement in order to produce a linear motion/force. It is controlled by a power electronic amplifier that takes the primary electrical supply on board the train and produces variable voltage and current to drive the motor. The nature of this power amplifier depends upon the type of motor, but invariably nowadays it will be a switched-mode device. The drive control involves electrical feedback of current (DC or AC) which is representative of the torque being produced by the motor.
>
> This GPSC is principally based upon demonstration of safety by explicit risk estimation and analysis. Some supporting evidence is available from EMAs used elsewhere, in particular tilting trains using the same technology.
>
> The overall system diagram for which the EMA is intended is shown in Figure 3a; Figure 3b provides the EMA scheme and its interfaces within the overall system.
>
> The system diagram provides a framework for a variety of applications, both secondary and primary suspension. 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.

This 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) or the provision of functional redundancy will be covered by the GASC.

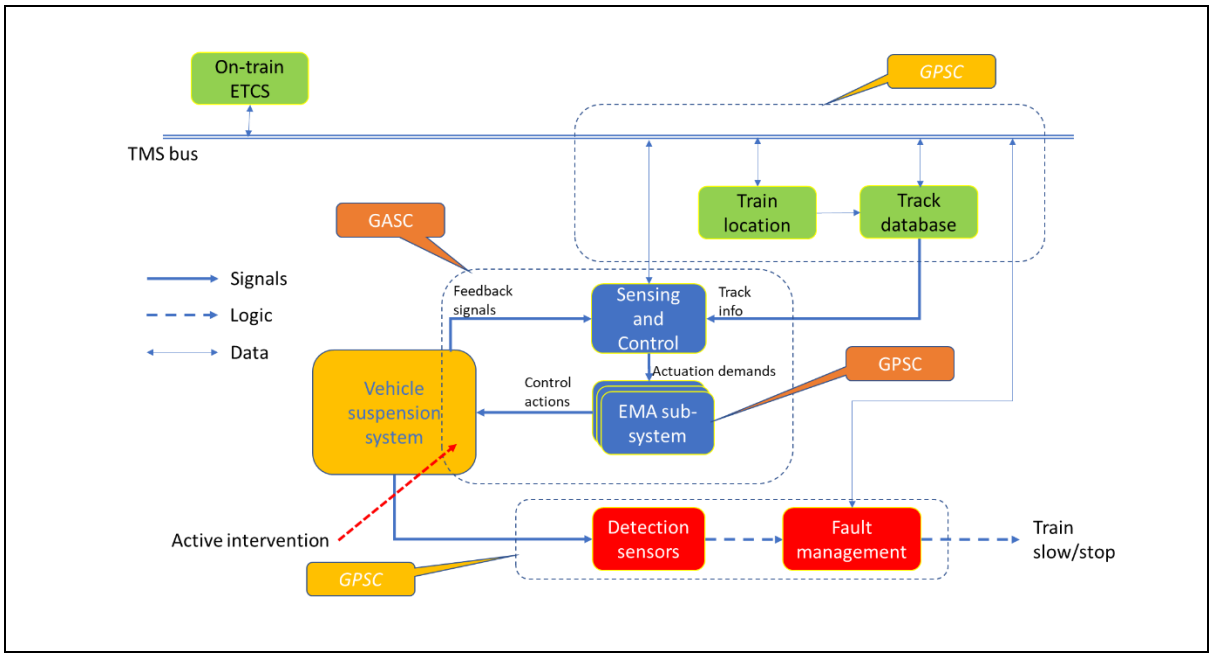


Figure 3a: General active suspension system block diagram

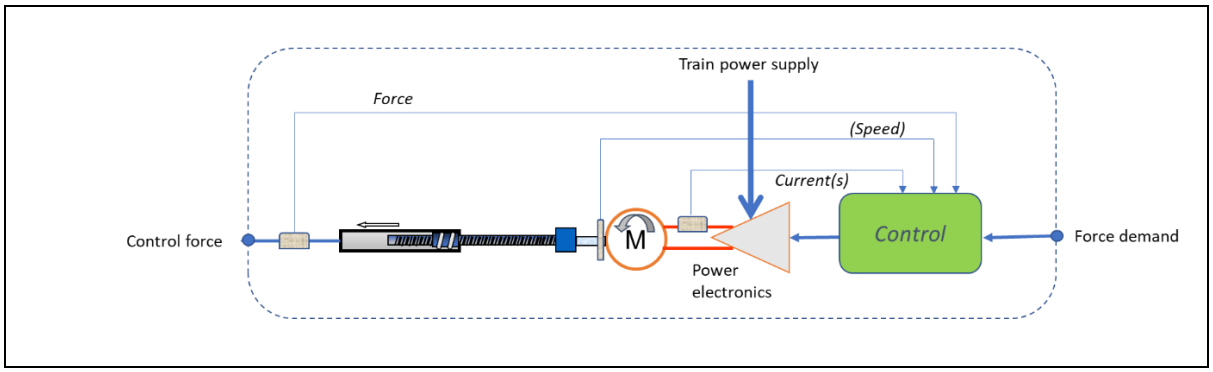


Figure 3b EMA system block diagram

The EMA sub-system in Figure 3b 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 a DC electrical motor driven by a power amplifier comprising high-frequency switched semiconductors giving high efficiency bi-directional control of the power supplied to/from 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.

This GPSC identifies failure modes for the EMA, the effects of which in terms of safe operation must be analysed within each application, which may have differing needs. For an active secondary suspension fail-soft is generally desirable, but for an active primary system providing running stability this may not be appropriate. Both analytical/simulation-based assessment are used, supported by hardware-in-the-loop (HiL) bench-testing of one or more of the EMAs.

Information in the quality management report is dependent on the nature of the organisation, as such no exemplary information can be provided.

Introductory text required.

Table 4 provides an overview of the safety management activities that will be applied for each subsystem.

Table 4: safety management activities for each subsystem

Subsystem		Method of safety demonstration
1	On-train ETCS	The on-train ETCS is an existing part of the train. Safety demonstration of the ETCS is provided in [reference to related safety case].
2	TMS bus	a. The interface to the ETCS will be demonstrated by technical design review to ensure compliance with the requirements of the ETCS safety case for interfacing systems. b. Interfaces with the train location and track database sub-systems will be demonstrated by technical design review and failure analysis as part of the safety demonstration of each sub-system. c. The TMS bus has physical components that run throughout the train. For each specific application there will be a need to ensure that the presence of the TMS bus, together with its operation and associated maintenance activities do not interfere with the correction operation of the train; for example as a result of electromagnetic interference, or maintenance procedures that impact on other safety-related equipment. This analysis will be part of the GASC for the implementation of the system. It is expected that the demonstration of safety will be obtained by technical review and approval by the railway's Chief Rolling Stock Engineer, however the procedure may vary depending on the target rolling stock, route and railway. This gives rise Hazard H001 (refer to the Hazard Log) and the Safety Requirement 001-001.
3	Train location	The ETCS provides some train location, but a more accurate location might be required if it is to give high quality “feedforward” information for the active suspension
4	Track database	a. The train location database will be implemented in a standard high-integrity database system that has been validated to SIL-4 for use as an on-board data store for railway application [reference to related safety case]. The database manages data integrity and provides protection against data decay. b. Preparation and installation of the data for the train location database will be demonstrated by application of data preparation procedures. Refer to Hazard 0002 and Safety Requirement 002-001. c. The correct operation of the interface between the track database and the TMS bus will be demonstrated by: 1 – functional failure analysis; 2 – failure modes, effects and criticality analysis; 3 - design review; 4 – functional testing.
5	Sensing and control subsystem	
6.1	EMA subsystem: control subsystem	
6.2	EMA subsystem: motor	
6.3	EMA subsystem: force actuator	
7	Vehicle suspension system	
8	Detection sensors	
9	Fault management	
10	Interface to train speed control (slow / stop)	

Demonstration of appropriate system integration.

8.5 Example technical safety report

8.5.1 Example review of safety-related documentation

8.5.2 Example results of SMR processes

8.5.2.1 FMECA for physical connection between TMS bus and the track interface

Exemplar material is not provided as the FMECA for the interface would depend on the exact nature of the interface including pin design, physical connection, casing etc.

8.5.2.2 Functional failure analysis in accordance with Safety Management Activity 4c1: functional failure analysis of the interface between the TMS bus and the track database.

ID	Function	Failure Mode	Effect	Reference
1	Provision of track data information to the TMS	a: No data provided	Loss of data when required will be detected by the sensing and control subsystem which will provide commands to perform graceful shutdown of the system.	H003
		b: Spurious provision of data (data provided when not required for operational purposes)	Small amounts of spurious data will not affect the system. Where the quantity of spurious data is so large it affects the availability of the TMS bus for other systems, there would be an operational effect on the system. The effect would be that other subsystems are not able to provide safety-critical data to the TMS bus.	H003
		c: Data incorrect although in valid format	Data will be treated as correct by the sensing and control subsystem and the EMA subsystem. Initially this could lead to incorrect control of the vehicle suspension system. In the worst case this could lead to damage to the track and rolling stock. Consistent erroneous control will be detected by the fault management system which will being graceful shutdown of the system.	H004
		d: Data in invalid format / data corruption	The corruption will be detected by the EMA subsystem which will commence graceful shutdown.	H005
		e: Data provided at the wrong time (too early, too late)	*As for earlier failure modes (1a, 1b, 1c)*	*As for earlier failure modes (1a, 1b, 1c)*
2	System health status reported to the TMS	a: No data provided	Loss of data when required will be detected by the sensing and control subsystem which will provide commands to perform graceful shutdown of the system.	H003
		b: Spurious provision of data	Small amounts of spurious data will not affect the system. Where the quantity of spurious data is so large it affects the availability of the TMS bus for other systems, there would be an operational effect on the system.	H003
		c: Data incorrect although in valid format	Detection of incorrect information by the EMA subsystem is possible as a result of the error-detection wrapper and pseudo-random message sequencing (PRMS) for TMS traffic. The EMA subsystem will comment graceful shutdown.	H006
		d: Data in invalid format / data corruption	The corruption will be detected by the EMA subsystem which will commence graceful shutdown.	H005

8.5.3 Example hazard log

Hazard ID	Hazard name	Status	Other responsible party	Risk	Comments	Associated Safety Requirements	Reference to other hazards
H001	Operation of EMA adversely affects existing on-board systems.	open	Railway where the system will operate	Medium	*none*	SR-001-001	*n/a*
H002	Incorrect track database information	open	*none*	Medium	The inherent risk of incorrect data is mitigated by operation of other subsystems, in particular the EMA.	SR-002-001	H003
H003	Failure of subsystems to provide safety-critical data to the TMS	open	*none*	Medium	The inherent risk of data loss is mitigated by function of the EMA.	SR-003-001	*n/a*
H004	Incorrect data in correct format on TMS bus	open	*none*	High	It is possible that the error could persist for 1.2 seconds prior to detection by the fault management system	SR-004-001	

Safety Requirements

Safety Requirement	Requirement	Responsibility
001-001	Procedures to be included in any GASC implementing this EMA to ensure that the presence, operation, and maintenance of the TMS bus do not adversely interfere with existing on-board systems.	[Customer]
002-001	Data preparation and installation for the track database shall be performed in accordance with safety related data preparation standard SRS-ABC-567.	Data preparation team
003-001	Design requirement EMA-XXX-888: The EMA shall tolerate loss or corruption of a single safety critical data packet from each subsystem. In the event of the loss of a single packet, the EMA shall wait for the next data cycle. If, on the next cycle, the same subsystem fails to provide correctly formatted data, the EMA shall initiate graceful shutdown.	System engineering team
004-001	The fault management system shall detect configurations of the suspension system that out-of-range (iaw Specification YYY-999) within 400 ms. When an out-of-range configuration persists for more than 200 ms, the fault management system shall commence graceful shutdown.	System engineering team

8.3 TEMPLATE FOR GENERIC APPLICATION SAFETY CASE GUIDELINES

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Template for Generic Application Safety Case Guidelines

This document is one of three templates that has been prepared to allow for safety cases to be developed for active suspension systems for rail vehicle.
The three templates are for a:

- *Generic Product Safety Case (GPSC);*
- *Generic Application Safety Case (GASC) – this document; and*
- *Specific Application Safety Case (SASC).*

This document makes reference to the GPSC template; it is intended that the GPSC template should be read in conjunction with this document. Figure 1 in the GPSC template provides an illustration of the how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems.
Consistent with the European Common Safety Method (CSM) [1] the templates allow for safety to be demonstrated using one of the following methods:

- *demonstration of compliance to existing codes, e.g. EN 14363 [2];*
- *comparison with a reference active suspension system that has an existing safety case;*
- *a risk-based approach compliant with [3]; or*
- *a combination of the above approaches.*

Contents

The introduction section will be the same regardless of the method that has been chosen to demonstrate safety compliance. Refer to the GPSC template for a description of the three types of suspension systems that these guidelines apply to.

This safety case provides evidence that *provide the working title or description of the generic application* is safe.
This safety case extends the Generic Product Safety Case *(provide a reference)* from which the generic application has been derived. This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the generic application and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.
Provide any additional information necessary for a reader to understand the reason for the safety case, for example background to the project, regulatory or legislative requirements particular to the product or its intended application.

This safety case applies only to a *provide the working title or description of the generic application. Describe the generic application and the main features of the system. Describe the boundaries and interfaces of the system, clearly describing components at the interface that are outside the scope of this safety case.*
Specific Application Safety Cases *provide references if applicable* support this safety case and describe:

- reasonably foreseeable safety hazards associated with the installation, operation, and maintenance of specific applications; and
- the controls required to reduce the risk associated with these hazards to an acceptable level.

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations (European Union, 2013). Figure 2 is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

The three approaches are not exclusive and could be used in combination. *Describe the approach that has been used for the generic application.*
Refer to the notes in the GPSC template regarding methods of demonstrating safety. It is most likely that the methods of demonstrating safety for the generic application will be the same as for the generic product then reference can be made to the information provided in the GPSC. Where the

methods differ then new information should be provided to make clear the changes and how safety will be demonstrated in the GASC.

I don't recommend providing an example here because the likelihood of there being any differences is very low. It would be artificial to create an illustration where different methods of safety demonstration are provided between the GPSC and the GASC. I fear that such an artificial example would confuse readers. In the worst case, even if readers provide incorrect information in the GASC, it is the role of the independent safety assessor (ISA) to address inconsistencies.

If the GPSC and GASC are being combined, Figure 2 from the GPSC template should be included here.

The detailed demonstration of safety compliant with this overall strategy will be achieved through compliance with the European railway RAMS standard [3]. This standard requires a safety case to be developed that is comprised of:

- system description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

A System Description is required regardless of the method that has been chosen to demonstrate safety compliance.

Describe the generic application: it is strongly recommended to provide a block diagram of the system architecture. The block diagram should extend the functional description provided in the GPSC to show subsystems, and components that implement the generic product and any physical constraints. Static parts of the generic application, such as heat sinks, shielding to reduce electro-magnetic inference, or dust filters should be included in the system description. Describe the interfaces between subsystems and between the generic application and external systems.

Provide any detail necessary to extend the description in the GPSC that describes the operation of the generic application during normal operation and degraded operation, alarms and their required responses. The description of the generic application should be supported by use cases or use of other design techniques such as event sequence diagrams.

Where safety demonstration is to be achieved by comparison to a reference system, the system description shall describe both the reference system and the new system in detail. The comparison should state the configuration of all items used in the generic application and the reference system include version numbers of each product or software item. All differences between the generic application and the reference system should be highlighted.

An example system description is shown in Figure 2.

TBD

Figure 2: Example system description

A Quality Management Report is always required. In many cases the content of the QMR for the GASC will be the same as the content in the GPSC. In these cases the relevant content should not be repeated*. Instead reference should be made to the content in the GPSC. In all cases section headings should be provided for each section and either reference should be made to the GPSC or relevant new content should be provided.*

This section describes the quality management processes applied during the design of the generic application.

As for the GPSC, I don't recommend providing an example within the T3.3 research task because any information would be entirely fictional and silly.

If appropriate refer to the description of the quality management system and certification provided in the GPSC.

It is not uncommon that design of the generic product and the build of the generic application are carried out by different organisations or different parts of a large organisation. In which case the quality management and certification processes may be different. New information needs to be provided where this is the case. Similarly the time between design of a generic product and development of a generic application may be a number of years. During this time there may have been changes to the quality management system, or accreditation to the system may have been renewed. Again, in these cases new information is required to describe all changes.

Refer to the guidance in the GPSC template for the information that should be included.

It is possible that the organisational structure for the generic product and the generic application will be the same. Where the GPSC and the GASC are to be combined, it is possible that a single organisational structure description can be provided. For large organisations, or in cases where the generic product design and the generic application are being developed by different organisations then it is likely that new information will be needed in the GASC.

Refer to the guidance in the GPSC template for the information that should be included.

As for the organisational structure, in some cases the quality assurance processes, and the assurance methods for the processes, will be the same as for the GPSC. Where there are differences, new information should be provide on the processes relevant to the GASC.

Refer to the guidance in the GPSC template for the information that should be included.

An SMR is always required. The SMR should be consistent with the information in the safety plan or describe any differences between the safety plan and the activities that were undertaken. For the GASC, the SMR should describe any additional safety management activities that were undertaken to ensure that safety of the generic application that were not undertaken for the generic product. If the detailed design of the generic application was not known at the time of the design of the generic product, then the SMR needs to describe the activities relevant to the design and components of the generic application.

It is strongly recommended that the criteria to determine acceptability of residual risk should be the same as was used in the GPSC. Where different criteria are used these should be made clear and a subsection should be created to explain the difference in acceptability criteria. Where necessary refer to national legislation on acceptability of safety risk. It is strongly recommended that legal advice is sought if varying acceptability criteria are used.

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic application is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

Describe any specific safety management activities that need to be undertaken to address the generic application that were not included in the generic product. For example the GPSC may describe that a communications interface will exist between the generic product and on-board train systems that communicate the current speed of the train, without describing the components used to implement the interface. The generic application will need to specify the components used to ensure correct and reliable communications. The GASC will need to provide information on the safety assurance techniques for the generic application.

Refer to the guidance in the GPSC template for the information that should be included.

The example from the GPSC can be extended for this document.

A TSR is always required. The TSR for the GASC needs to correspond with the SMR for this document and provide the results of any safety analysis techniques that were undertaken for the generic application that were not undertaken for the generic product, see the guidance at the beginning of Section 4 of this document.

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

Where the design document for the generic application differs from the design for the generic product, detail the differences in the documentation and the review processes that were followed. For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles.

Provide a list of the safety analysis techniques described in the SMR. For each technique, provide the technical results. For example if an FMEA is stipulated in the SMR, then provide details of the FMEA, details of staff who were involved together with references to the QMR that describes staff expertise. Provide the results of the FMEA.

The examples provided in the GPSC can be extended here.

The following hazard log presents the safety hazards identified during the safety analysis.

The hazard log from the GPSC should be extended to provide new information identified during the analysis techniques specified in Section 4 of this document. It is likely that hazards identified in the GASC are specific cases, or causes, of general hazards identified in the GPSC. For example the GPSC may have identified that a hazard may arise if the active suspension system cannot change the stiffness of a damper within a specified time; the GASC may identify that fluid leaking from a bleed valve may cause low pressure that would result in the hazard occurring. New information added to the hazard log should refer to earlier information in the hazard log and clear references should be provided between hazards.

NOTES:

1. *At this level of detail for the GASC the hazards might be a catalogue of the fault modes of the product*
2. *If new hazards are identified that are not specific cases of, or causes of, hazards included in the GPSC this is an indicator of a possible deficiency in the hazard identification process used during the GPSC. In such cases a review must be undertaken to ensure that the hazard identification process used for the GPSC was adequate and information should be provided to explain why new generic hazards were identified at this stage.*

Hazard summary table.

Hazard ID	Hazard name	Status	Other responsible party	Risk	Comments	Reference to other hazards
e.g. H001	*e.g. Insufficient yaw stiffness*	*[open / closed / deleted]*	*[no] or name of other party*	*risk ranking*	*comment*	

The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.

Refer to the guidance in the GPSC template for the information that should be included.
The examples shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The examples shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

A conclusion is required for all safety cases.
Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product defined by the associated GPSC for use within the particular active suspension system described herein under reasonably foreseeable conditions.
Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

1. EN50126-1/2 (2017) “Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS)”
2. BS EN 14363:2016+A1:2018 Railway applications. “Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests”
3. European Standard EN 50657:2017; Railways Applications. Rolling stock applications. Software on Board Rolling Stock; European Union; 2013.
4. Commission Implementing Regulation (EU) 2015/1136, “Common safety method for risk evaluation and assessment”

Update the above reference details as appropriate.
List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.
List any related safety cases, such as safety cases for subsystems or components that are required as a part of the generic application.

8.4 TEMPLATE FOR SPECIFIC APPLICATION SAFETY CASE GUIDELINES

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Template for Specific Application Safety Case Guidelines

This document is one of three templates that has been prepared to allow for safety cases to be developed for active suspension systems for rail vehicle.
The three templates are for a:

- *Generic Product Safety Case (GPSC);*
- *Specific Application Safety Case (GASC); and*
- *Specific Application Safety Case (SASC) – this document.*

This document makes reference to the GASC template; it is intended that the GPSC and GASC templates should be read in conjunction with this document. Figure 1 in the GPSC template provides an illustration of the how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems.
Consistent with the European Common Safety Method (CSM) [4] the templates allow for safety to be demonstrated using one of the following methods:

- *demonstration of compliance to EN 14363 [2];*
- *comparison with a reference active suspension system that has an existing safety case;*
- *a risk-based approach compliant with [1]; or*
- *a combination of the above approaches.*

Contents

The introduction section will be the same regardless of the method that has been chosen to demonstrate safety compliance. Refer to the GPSC template for a description of the three types of suspension systems that these guidelines apply to.

This safety case provides evidence that *provide the working title or description of the specific application* is safe.
This safety case extends the Generic Product and Generic Application Safety Cases *(provide references)* from which the specific application has been derived. This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the specific application and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.
Describe the specific application to which this safety case applies, where appropriate differentiate this specific application from other specific applications derived from the same generic application.

This safety case applies only to a *provide the title or description of the specific application.*
Describe the specific application and the main features of the system. Describe the boundaries and interfaces of the system, clearly describing components at the interface that are outside the scope of this safety case.
Clearly define cases that are outside the scope of the specific application. For example the specific application may be use of a generic application product on a particular class of rolling stock operating on a specific route. Describe the boundaries of the route and the limits of operation for the route such as maximum speed. The specific application may apply only when certain infrastructure constraints are maintained (for example maximum cant). Where necessary refer to the specific railway standards that are required for this SASC to be valid.

Describe the safety assurance strategy that has been used for the specific application, refer to the guidance in the GPSC template for the information that should be included. Where the method of safety assurance differs from the approach in the GASC, provide an explanation for the differences.

A System Description is required regardless of the method that has been chosen to demonstrate safety compliance.

Describe the specific application making clear all interfaces with the intended rolling stock. Provide a description of how the specific application will be installed on, and configured for the rolling stock.

The example from the GASC can be extended, although it may be fictional as examples will have to be given for specific rolling stock.

A Quality Management Report is always required. For the SASC will have to describe the processes for ensuring safety during installation, configuration, operation and maintenance of the specific application. It is expected that the QMR will need to refer to the safety management system for the rolling stock operator and any subcontractors they use for activities such as maintenance.

This section describes the quality management processes applied during the design of the specific application.

Again, I don't recommend providing an example within the T3.3 research task because any information would be entirely fictional and silly.

Describe the quality management system for all organisation involved in installation, configuration, operation and maintenance of the specific application. Where organisations have an accredited safety management or safety management system refer to the system and its accreditation. Describe the specific parts of each system that will be relevant to the specific application.

Even in cases where the installation will be carried out by the organisation that developed the generic application, new information may be required that is not in the GASC. For example the time between design of a generic application and installation of a specific application may be a number of years. During this time there may have been changes to the quality management system, or accreditation to the system may have been renewed. In such cases new information is required to describe all changes.

Describe the quality management system applicable during installation, configuration, operation and maintenance of the specific application. Provide a list of standards, processes, procedures and other documentation that comprises the quality management system applicable to specific application. List all internal documents such as policies and standards as well as external documents such as standards, or codes of practice. Justify why these documents are appropriate for the specific application. Include quality management documentation related to supporting activities such as training, supplier management, purchasing etc.

Refer to the GPSC template for further guidance on information that should be included.

It is possible that different organisations will be involved in the installation, configuration, operation and maintenance. Describe the organisations and the interfaces between them. Make clear which organisation has responsibility for each part of the specific application's lifecycle. For example make clear the responsibility of the rolling stock operator for identifying and reporting faults; the responsibility of the maintainer to test for, detect, and respond to faults. Provide a clear description of who (by organisation and position title) has authority to remove the specific application from service and who (by organisation and position title) is the single point of authority to permit the specific application to be used in service.

An example can be provided here even though it will be fictional we do not need to refer to individuals (such as A.N. Other), rather we could refer to the *chief rolling stock engineer* for the train operator, the *shift maintenance supervisor* for the maintenance contractor etc.

For installation and configuration of the specific application, describe the process that will be followed and list all rolling stock (by unique identifier) that the specific application will be installed on. Describe the process that will be used the ensure the correctness of the installation and configuration; describe the checking and authorisation process that will be followed for the installation, and what evidence will be provided to demonstrate correct installation and configuration.

List the staff who are authorised to perform installation and configuration, together with any training they will receive and certification that is required prior to undertaking the work.

For operation and maintenance of the specific application describe the procedures that need to be followed.

An SMR is always required. For the SASC, the SMR should describe any additional safety management activities that were undertaken to ensure that safety of the specific application that were not undertaken for the generic application, including activities to ensure the safety of the active suspension system on specific rolling stock or in particular applications.
It is possible that the GASC provided analysis sufficient to ensure the safety of the specific application, in which case it is possible to combine the GASC and the SASC so long as a description should be provided to make clear why the scope of the GASC fully covers the specific application.
It is strongly recommended that the criteria to determine acceptability of residual risk should be the same as was used in the GASC. Where different criteria are used these should be made clear and a subsection should be created to explain the difference in acceptability criteria. Where necessary refer to national legislation on acceptability of safety risk. It is strongly recommended that legal advice is sought if varying acceptability criteria are used.

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the specific application is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

Describe any specific safety management activities that need to be undertaken to address the specific application that were not included in the generic product. For example the GASC may describe operation of the active suspension system on pneumatically braked passenger rolling stock with a maximum speed of 180 km/h. The SASC would need to identify the specific rolling stock to which the active suspension system is to be fitted and determine that the scope of the GASC is consistent with the specific application. The SASC would also need to explain the exact interface between the active suspension system and the target rolling stock.
There may be a need for safety management activities to be undertaken for individual rolling stock items. For example, a rolling stock operator may be intending to install the active suspension system on a fleet of trains that have slightly different configurations: perhaps different maintenance activities undertaken at different times has results in two different types of brake systems being installed across the fleet. The different braking systems may require different installations of the active suspension system due to the differences in physical size and shape of the components. Difference safety analysis may need to be undertaken to ensure that the active suspension system can be installed in accordance with the requirements of the GASC on each configuration of rolling stock.
Where necessary describe additional safety management activities that were undertaken for the specific application; these activities may be repeats of the activities described in the GASC that were tailored for the specific application. Refer to the safety plan that was used for design and development activities and describe any deviations from the safety plan and approval for the deviations from the Independent Safety Assessor (ISA).
Refer to the GPSC template for additional guidance on the information that should be included.
The example from the GASC can be extended for this document.

A TSR is always required. The TSR for the SASC needs to correspond with the QMR and SMR for this document and provide the results of assurance activities any safety analysis techniques that were undertaken for the specific application.

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the QMR and SMR and that the residual safety risk of the system is acceptably low.

Where additional safety management activities were carried out for the specific application, the design document for the specific application, detail the new documentation and the review processes that were followed. For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles.

Provide a list of the safety analysis techniques described in the SMR. For each technique, provide the technical results. For example if additional safety analyses were undertaken due to different configurations of the target rolling stock, then provide the results of the additional analyses.

The examples provided in the GASC can be extended here.

The following hazard log presents the safety hazards identified during the safety analysis.

Where necessary, the hazard log from the GASC should be extended to provide new information identified during the analysis techniques specified in Section 4 of this document. It is likely that hazards identified in the SASC are specific cases, or causes, of general hazards identified in the GASC. New information added to the hazard log should refer to earlier information in the hazard log and clear references should be provided between hazards.

NOTE: if new hazards are identified that are not specific cases of, or causes of, hazards included in the GASC this is an indicator of a possible deficiency in the hazard identification process used during the GPSC and SASC. In such cases a review must be undertaken to ensure that the hazard identification process used for the GPSC was adequate and information should be provided to explain why new generic hazards were identified at this stage.

Hazard summary table.

Hazard ID	Hazard name	Status	Other responsible party	Risk	Comments	Reference to other hazards
e.g. H001	*e.g. Insufficient yaw stiffness*	*[open / closed / deleted]*	*[no] or name of other party*	*risk ranking*	*comment*	

The example shown in the GASC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.

Refer to the guidance in the GPSC template for the information that should be included.
The examples shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The examples shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

This section is required regardless of the approach used to demonstrate safety.
Provide evidence that the procedures for installation and configuration have been correctly followed for every installation, refer to the QMR to show that only qualified people have performed installation and configuration and that appropriate people have checked and authorised the work. Where different organisations are responsible for installation, configuration, operation and maintenance describe how the appropriate procedures have been integrated into the existing safety management system or quality management system of the organisations responsible for these activities. Otherwise provide evidence that the organisations have been provided with full copies of the procedures and have acknowledged receipt.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

Refer to the guidance in the GPSC template for the information that should be included.
The example shown in the GPSC template can be extended here.

A conclusion is required for all safety cases.

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under all reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

1. EN50126-1/2 (2017) “Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS)”
2. BS EN 14363:2016+A1:2018 Railway applications. “Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests”
3. European Standard EN 50657:2017; Railways Applications. Rolling stock applications. Software on Board Rolling Stock; European Union; 2013.
4. Commission Implementing Regulation (EU) 2015/1136, “Common safety method for risk evaluation and assessment”

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.
List any related safety cases, such as safety cases for subsystems or components that are required as a part of the specific application.

8.5 EXAMPLE: GENERIC PRODUCT SAFETY CASE FOR ELECTRO-HYDRAULIC ACTUATION AND CONTROL

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Example: Generic Product Safety Case for Electro-Hydraulic actuation and control (Draft)

Contents

1. Introduction

Background

The Generic Product Safety Case (GPSC) can be applied to one of three types of suspension system, more description of which is provided in corresponding Generic Application Safety Case (GASC)s.

Type I: active secondary suspensions including tilting systems.

Type II: active primary suspensions with mechanical constraints.

Type III: active primary suspensions with functional redundancy.

It provides evidence that the electro-hydraulic actuation system (abbreviated to EHA) with associated sensing and control can operate safety when used within active suspension systems. It can be referred to in various GASCs according to the class or type of active suspension application as listed above. Figure 1 is an adaptation of a diagram in European Standard EN 50126 [1]. It gives examples (the red arrows) of how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems, although others are possible.

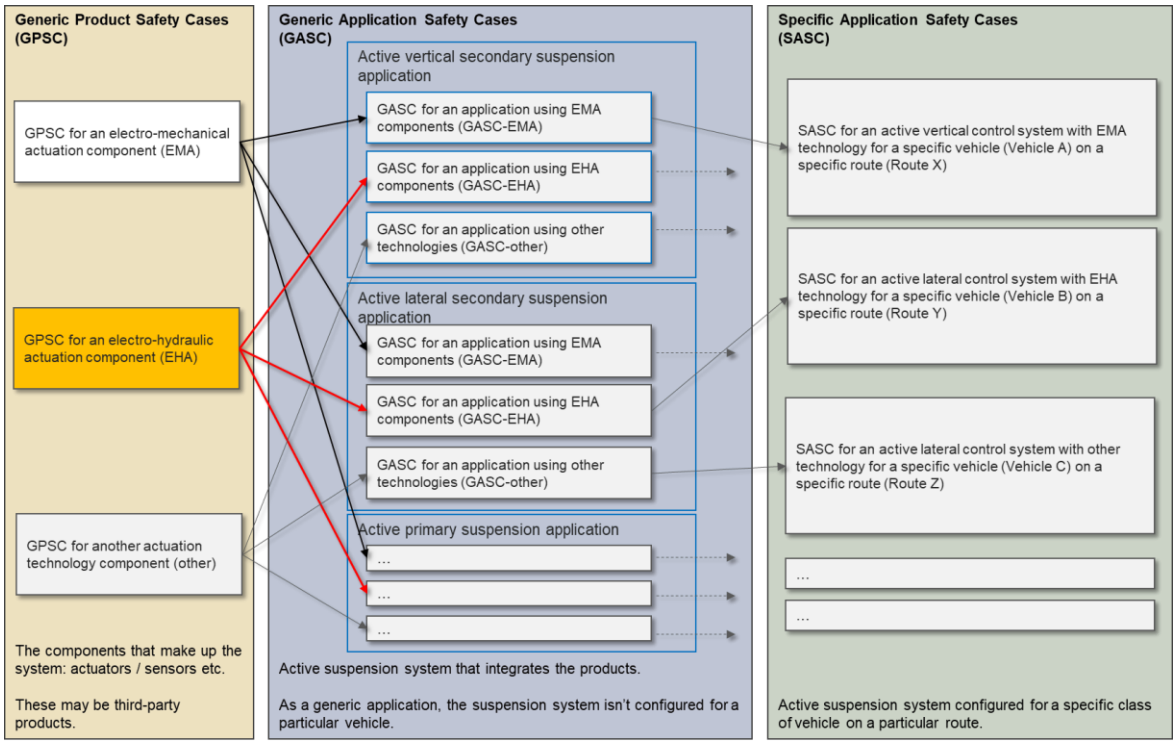


Figure 1 Relationship between Safety Case documents

This safety case identifies reasonably foreseeable safety hazards and safety-related fault modes associated with the operation and maintenance of the generic product and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.

This safety case applies only to an EHA.

Summary description

Active suspension systems invariably require a controllable force- or torque-generating device plus sensors and control electronics. This GPSC is intended to provide evidence that the EHA has the necessary safety-related characteristics for a range of active suspension possibilities. For this reason it includes aspects that may not be required for all such possibilities, in which case any restricted scope of this GPSC is identified in any related GASC.
An EHA uses an electric motor, which can be DC or various forms of AC machine, combined with some form of pump and cylinder. The electrical motor is powered by the train power supply. The motor drives two pumps through a coupling, which create flow into the cylinder. The motor runs with constant speed and as also the pumps have constant displacement, the flow into the cylinder will be constant. The pressure in the cylinder is controlled by pressure valves, one for each side of the piston. The pressure valves are fed by current from small size amplifiers and constitutes closed loops. The reference currents to these control loops are given by the system controller, which thereby can control the pressure on each side of the piston in the actuator and thereby the force the actuator shall produce.

Safety assurance approach

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations [2]. Figure 2 is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

This GPSC is principally based upon the third approach, i.e. explicit risk estimation and analysis. Some supporting evidence may be available from experience with using EHAs in similar application. The detailed demonstration of safety compliance with this overall strategy will be achieved through compliance with the European standard for demonstrating reliability, availability, maintainability, and safety for railway applications [1]. This standard requires a safety case to be developed that comprises:

- System description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

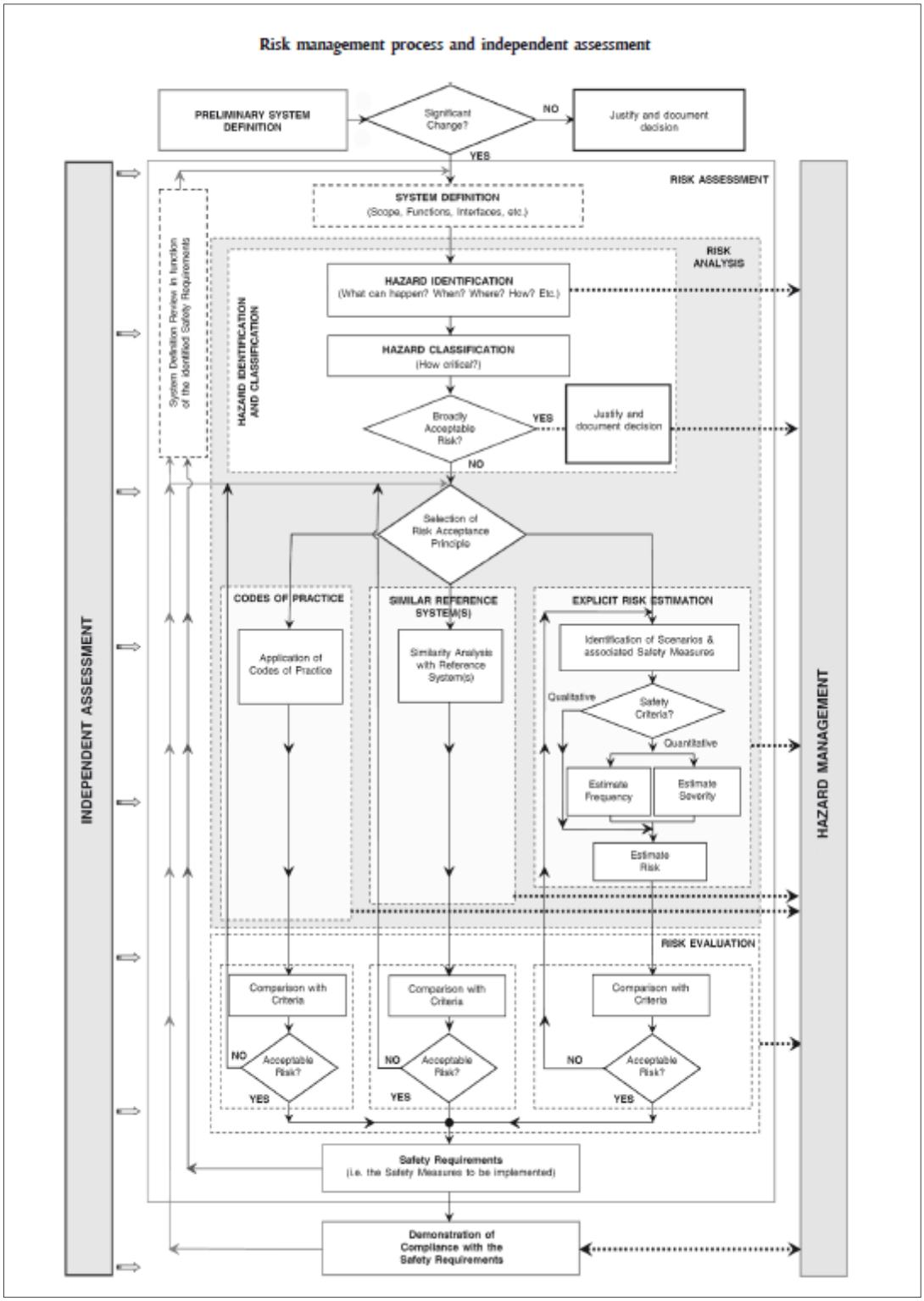


Figure 2 Overall approach to providing safety assurance shown in European Union (2017)

2. System Description

Application or System context.

The overall system diagram for which the EHA is intended is shown in Figure 3. 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.

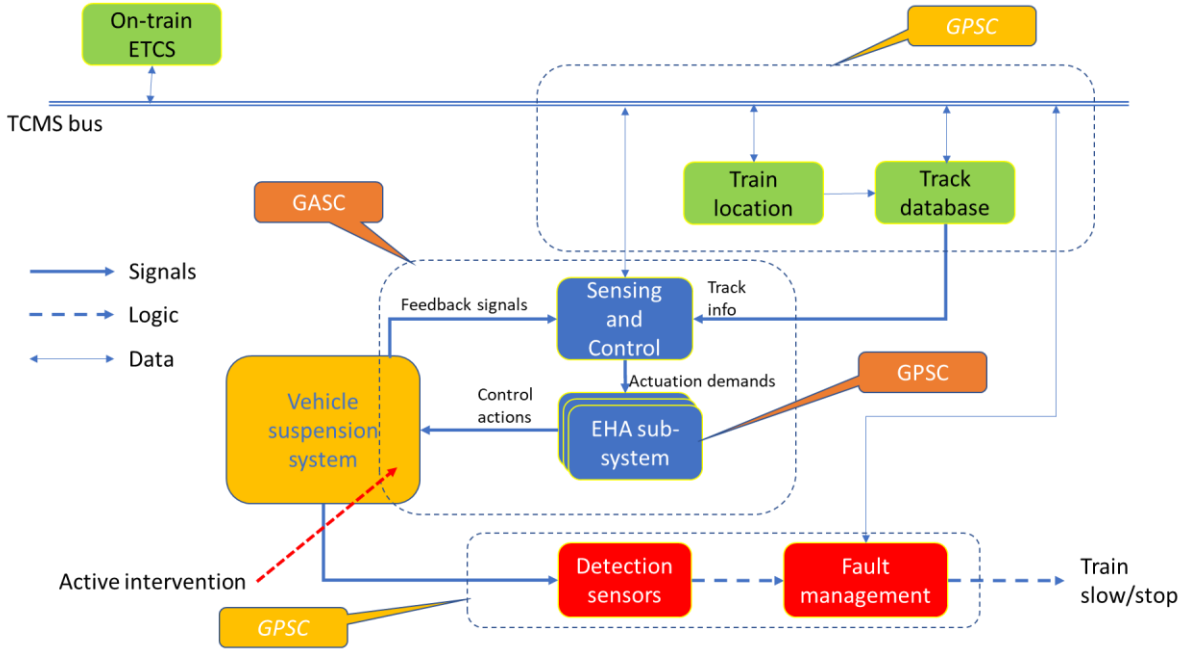


Figure 3 General active suspension system block diagram

Detailed description

This GPSC describes the use of an EHA, 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 EHAs, or a combination of the two. This GPSC is focussed upon the intrinsic safety of a single EHA sub-system, whereas coordination of a set of EHAs (or other actuator technologies) or the provision of functional redundancy will be covered by the GASC.

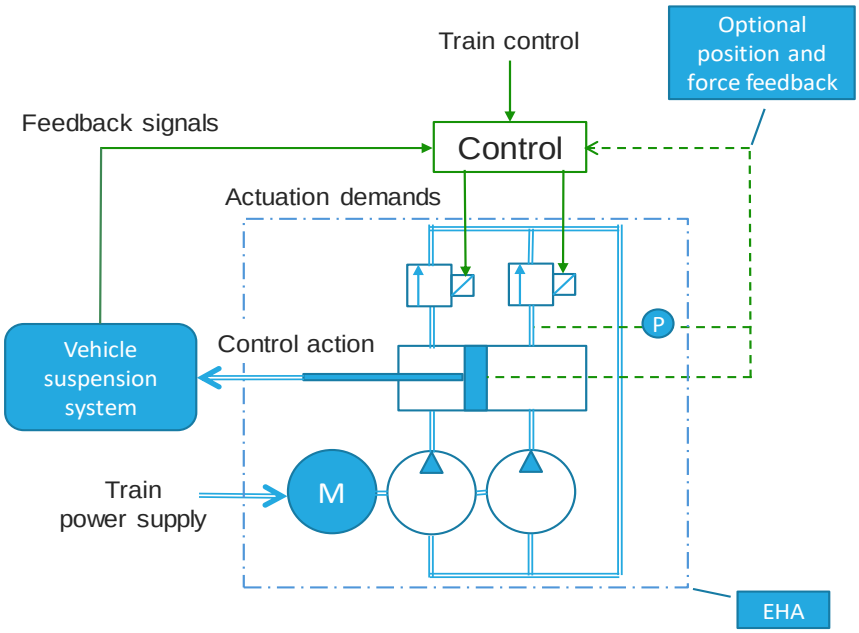


Figure 4 EHA system block diagram

Figure 4 provides a diagram of the EHA scheme and its interfaces within the overall system. The actuator interface consists of the actuation demands from the controller and an output force that would be applied to the vehicle dynamic system in order to provide “active intervention”. The actuator position and oil pressure are two optional feedbacks from the EHA to the controller mainly for supervision.

The EHA consists of an electrical motor powered by the train power supply. The motor drives through a coupling the pumps, which creates oil flow into the cylinder. The pressure in the cylinder is controlled by pressure valves. The pressure has a relation to the actuator force output, which influence the vehicle suspension system. The controller receives feedback signals from the vehicle suspension system and information from train control to calculate the actuation demands to the pressure valves.

The GPSC is focussed upon identifying failure modes for the EHA, the effects of which in terms of safe operation must be analysed within each application, which may have differing needs in terms of safe failures. Both analytical/simulation-based assessment are used, supported by hardware-in-the-loop (HiL) bench-testing of one or more of the EHAs.

Identification of sub-systems

The following are the EHA’s principal sub-systems:

- Electric motor (asynchronous AC-motor)
- Pumps
- Cylinder with piston
- Pressure valves
- Cabling (incl. contactor to switch power on and off)

These are referred to again in Section 4.

3. Quality Management Report

Quality Management System and Certification Organisational Structure

4. Safety Management Report

This section describes the safety management techniques that were employed during the design, and where applicable development, of the generic product. This section should refer to the safety plan that was used for design and development activities.

Overall safety approach

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic product is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

The safety management approach involves identifying all fault modes that can occur in the EHA, and then assessing their effect upon the system. The safety plan involves a hierarchical assessment approach adopted as part of the design and development process. Note that, as observed earlier, the effect of each fault mode upon safety risk depends upon the particular nature of the application and the manner in which the EHAs are to be used. Hence the associated GASC will fully assess the fault effects upon system safety.

General safety (environment, electrical, maintenance

[to come]

Functional safety

All subsystems that are identified in Section 2 have documentation and test processes that are required prior to being assembled into a working EHA. These are listed in Table 1.

Table 1 Subsystem documents and tests

Subsystem	Approach to demonstrate safety	Failure probability
Electric motor	Initial supplier's QC test certificate Initial product bench test Regular maintenance testing (insulation etc.) Quantification of failure rates	
Pumps	Initial supplier's QC test certificate Initial product bench test Maintenance checks	
Cylinder with piston	Initial product bench test Maintenance checks	
Pressure valves	Initial supplier's QC test certificate Initial product bench test Running supervision	
Cabling (incl. contactor to switch power on and off)	Pre-installation test Running supervision	

Faults in the various subsystems can create or contribute to a variety of EHA fault modes that may be potential hazards within an active suspension application, and Table 2 identifies these causalities.

Table 2 Subsystems and fault modes

Fault mode	**Sub-system**				
	Motor	Pump	Cylinder	Valves	Cabling
Locked	×	×	×	×	×
Free	×	×	✓	×	×
Zero force	×	×	×	✓	✓
Semi-active	✓	✓	×	×	✓
Force excess	×	×	×	✓	×
Inversion	×	×	×	×	✓
Random force	×	×	×	✓	✓

Locked	The actuator is mechanically jammed to give a rigid connection between the two actuator ends.
Free	The actuator ends have no mechanical connection
Zero force	The actuator is running with zero force reference
Semi-active	No flow into the cylinder, but the valves can still be used to control the force
Force excess	The actuator is producing more force than requested
Inversion	The actuator is producing force in the opposite direction
Random force	The actuator is producing a random force

V-lifecycle diagram

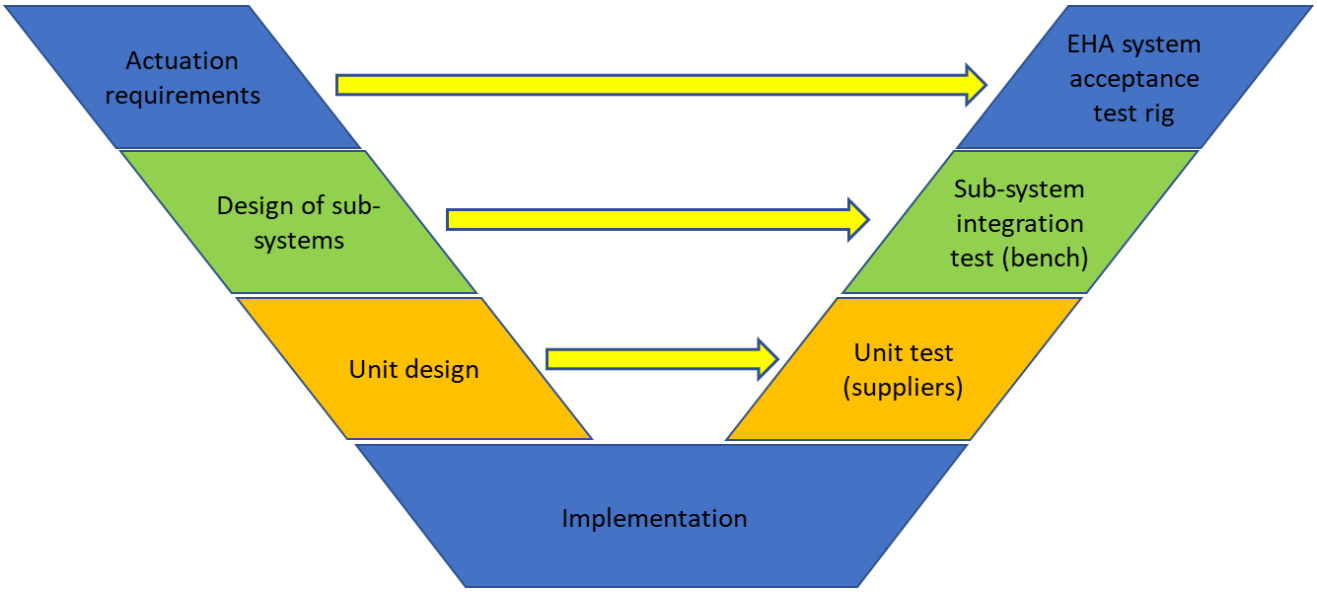


Figure 5 V lifecycle for EHA

Figure 5 shows the V-diagram for the EHA design and development process, and indicates the safety-related checks at each level of the lifecycle:
[List of safety-related checks here]

Actuation testing strategy

It is necessary to ensure that the fault modes identified above are physically tested as identified at the various levels of the V-diagram.
Describe and provide a diagram of the safety lifecycle that was employed. If a Safety Plan exists for the development activities, describe any deviations from the safety plan and approval for the deviations from the Independent Safety Assessor (ISA). Describe the techniques that were used for:

- *functional hazard identification and risk assessment;*
- *design and development of risk controls;*
- *demonstration of suitability of risk controls; and*
- *demonstration on acceptability of residual safety risks.*

Show where the activities were carried out during the safety lifecycle. Describe any standards, guidelines, codes of practice or other documents that were used during the activities.
Describe details of all techniques applied and, if necessary, justify any deviation from standard techniques; explain the guidewords that were used during a failure modes and effects analysis. It is essential that justification is provided to describe why these techniques are appropriate to the design, and where applicable development, of the generic product. Where it is foreseeable that specific products will contain software or are configured by data, describe the software safety techniques and measures that are to be applied in accordance with EN50128 [3].
Provide evidence to demonstrate that these activities cover the full scope of the generic product as described in the Section 2.

Provide documentary evidence or refer to other documents that show that the techniques were applied correctly and that the results of each activity were integrated into the design and development lifecycle. Demonstrate that documents have been signed-off in accordance with the sign-off requirements described in Section 3.
The SMR needs to identify the techniques that will be followed to produce the results shown in the TSR (see Section 5). Amongst other evidence, the TSR requires evidence of correct functional behaviour and demonstration that the product's effect within an active suspension system cannot cause an unsafe condition when operating as designed. It may be practical to integrate the tests to provide this evidence with other functional testing that demonstrates the system meets its functional specification. In these cases, the SMR will need to show how the functional testing activities integrate. It must be clear which evidence from functional testing will be used in the TSR.

5. Technical Safety Report

Review of safety-related documentation

Provide a list of all design documentation associated with the product for use within an active suspension system. For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

Sub-system analysis and fault

Table 3 presents the fault modes that might create safety hazards when the EHA is used in an active suspension application.

Table 3 Fault mode descriptions

ID	Failure mode	Description	Cause(s)	Quantitative probability	Mitigation
1	Locked	Actuator mechanically jammed	Gross failure of piston	Very unlikely	No need [1)]
2	Free	Actuator disconnected from load	Broken piston	Very unlikely	Designed for life
3	Zero force	No force command	Valve failure	Possible	Application dependent [2)]
			Cabling failure	Possible	Application dependent [2)]
4	Semi-active	No flow into the cylinder	Motor failure	Possible	Application dependent [2)]
			Pump failure	Possible	Application dependent [2)]
			Cabling failure	Possible	Application dependent [2)]
5	Force excess	Maximum force (either direction)	Valve failure	Unlikely	Supervision [3)]
6	Inversion	Output force in wrong direction	Incorrect installation	Very unlikely	Acceptance testing
7	Random	Intermittent failures	Valve failure	Unlikely	Supervision [3)]
			Cabling failure	Possible	Supervision [3)]

1) Like hydraulic dampers, where this mode is disregarded
2) Depending on application, this mode can possibly be shown to safe without any further mitigation, if not supervision is needed
3) Supervision can mitigate this risk if the supervision is independent from the failure source

Fault mode probabilities

These are derived from the known failure rates of the subsystems and their contributions to the different faults given in Table 2.

[Quantification using FMEA analysis to be added here]

Assessment of fault mode effects - actuator dynamic properties and model

In some cases, assessment of the effects of the fault modes will require dynamic analysis (and or testing). For this reason, a dynamic model of the EHA is provided that can be used as part of the corresponding GASC. Figure 6 is a general diagram for a force-controlled actuator within an active suspension. The force command to the actuator would be generated by an active suspension controller, which will be detailed within the GASC. The track input will impact upon the dynamic system, and this will cause actuator movement which will impact the actuator's capability to produce the requested force. How well the actuator generates the force required of it in the presence of actuator movements depends upon the characteristics of the actuator, and it is not possible to generalise.

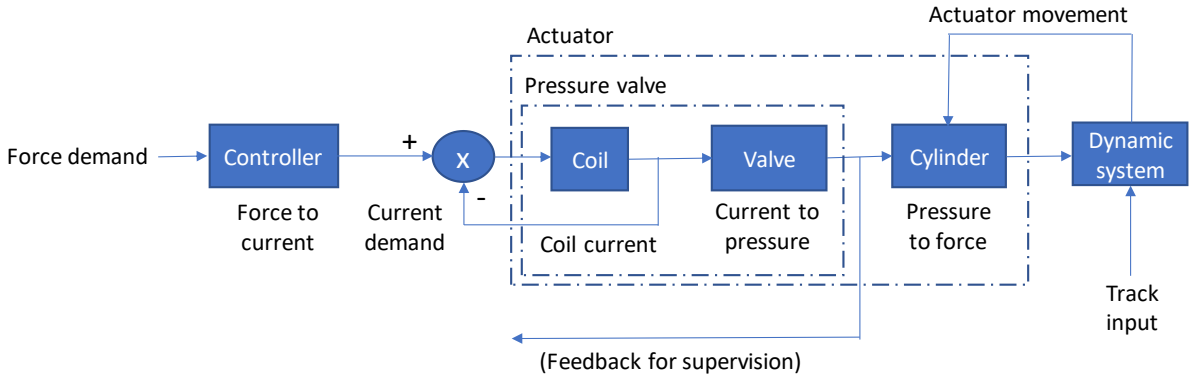


Figure 6 Force-controlled actuator – generic scheme

It is however essential that the actuator's dynamic model provides the actuator movement feedback, which would only be quantified in the context of an application, i.e. within an associated GASC. **Error! Reference source not found.** provides the model which is used, and Appendix 1 provides parameter information.

\

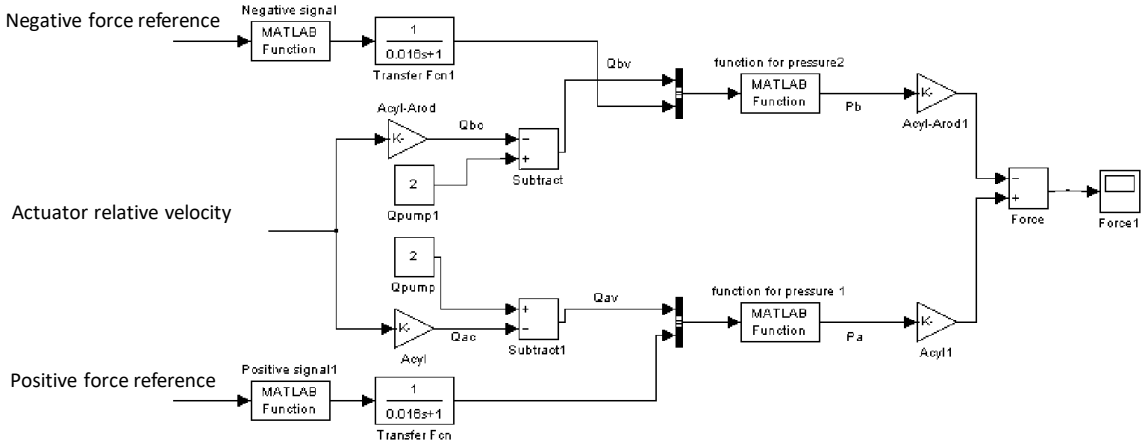


Figure 7 Block diagram dynamic model for EHA showing force control loop

The model enables the fault modes listed above to be simulated in conjunction with the vehicle model, and the corresponding effects to be assessed in the context of the particular application.

Actuation test results

[Would be included in a real GPSC

Operation with External Influences

This section is required regardless of the approach used to demonstrate safety.

Safety-related Application Conditions & Assumptions

This section is required regardless of the approach used to demonstrate safety.
Provide a full list of all rules, conditions, constraints and assumptions that must be maintained for the system to remain in a safe state. Where necessary provide references to other documentation that detail the necessary information; for example the system maintenance manual. Where assumptions have been made in the safety case, evidence must be provided for why the assumptions are reasonable.

Other Outstanding Safety Issues

It is possible that no additional information is required to support the safety argument. In such cases, in order to demonstrate completeness of the safety case, the heading should be retained and a note should be made that no further information is necessary.
Describe any further information that is relevant to the safety argument that has not been included in other parts of this document. In particular, where the information in the TSR demonstrates that any tests were failed, provide a description of the failed test, an analysis of the impact of the failure,

and information on how the system will remain safe regardless of the failure. Where necessary refer to other parts of this safety case.

6. Conclusion

A conclusion is required for all safety cases.

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under all reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

7. References

1. European Standard EN 50126-1 and 2:2017; Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
2. Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009
3. EN 50128/AC:2014 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems
4. European Union; 2013. Official Journal of the European Union L 121; Legislation Volume 56; 03 May 2013.

[Perhaps need a reference for EHA dynamic model]

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.
List any related safety cases, such as safety cases for sub-systems or components that are required as a part of the generic product.

8. Appendices

Appendix 1 Parameter information relevant to actuator model (**Error! Reference source not found.**)

[list needed here for the specific actuator design]

Contract No. 777564

8.6 EXAMPLE: GENERIC PRODUCT SAFETY CASE FOR ELECTRO-MECHANICAL ACTUATION AND CONTROL

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Example: Generic Product Safety Case for Electro-Mechanical actuation and control (01/07/19)

Contents

Introduction

Background

The GPSC can be applied to one of three types of suspension system, more description of which is provided in corresponding GASCs.

Type I: active secondary suspensions including tilting systems.

Type II: active primary suspensions with mechanical constraints.

Type III: active primary suspensions with functional redundancy.

It provides evidence that the electro-mechanical actuation system (abbreviated to EMA) with associated sensing and control can operate safety when used within active suspension systems. It can be referred to in various GASCs according to the class or type of active suspension application as listed above. *Figure 1* is an adaptation of a diagram in European Standard EN 50126-2:2007. It gives examples (the red arrows) of how the different safety cases may combine to provide the safety assurance for different specific applications of active suspension systems, although others are possible.

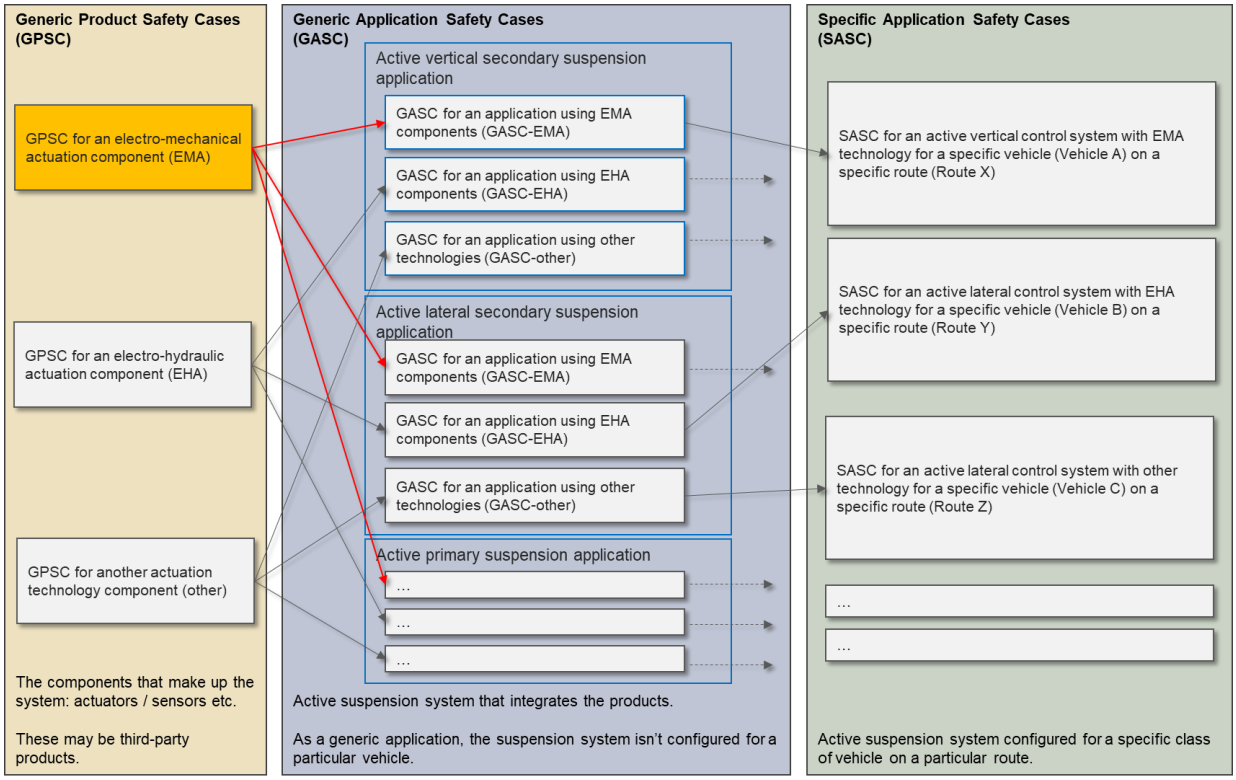


Figure 1 Relationship between Safety Case documents

This safety case identifies reasonably foreseeable safety hazards and safety-related fault modes associated with the operation and maintenance of the generic product and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.

This safety case applies only to an EMA.

Summary description

Active suspension systems invariably require a controllable force- or torque-generating device plus sensors and control electronics. This GPSC is intended to provide evidence that the EMA has the necessary safety-related characteristics for a range of active suspension possibilities. For this reason it includes aspects that may not be required for all such possibilities, in which case any restricted scope of this GPSC is identified in any related GASC.

An EMA uses an AC permanent-magnet electric motor (it could be a DC or various other forms of AC machine), combined with some form of gearing. In this EMA the gearing is a ball- or roller-screw arrangement in order to produce a linear motion/force. It is controlled by a power electronic amplifier that takes the primary electrical supply on board the train and produces variable voltage and current to drive the motor. The nature of this power amplifier depends upon the type of motor, but here it is a three-phase inverter, a high-efficiency switched-mode device. The drive control involves electrical feedback of current provided from the inverter which is representative of the torque being produced by the motor.

Safety assurance approach

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations (European Union, 2013). *Figure 2* is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

This GPSC is principally based upon the third approach, i.e. explicit risk estimation and analysis. Some supporting evidence may be available from experience with using EMAs elsewhere, in particular tilting trains using the same technology.

The detailed demonstration of safety compliance with this overall strategy will be achieved through compliance with the European standard for demonstrating reliability, availability, maintainability, and safety for railway applications (European Union Standard EN 50126). This standard requires a safety case to be developed that comprises:

- System description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

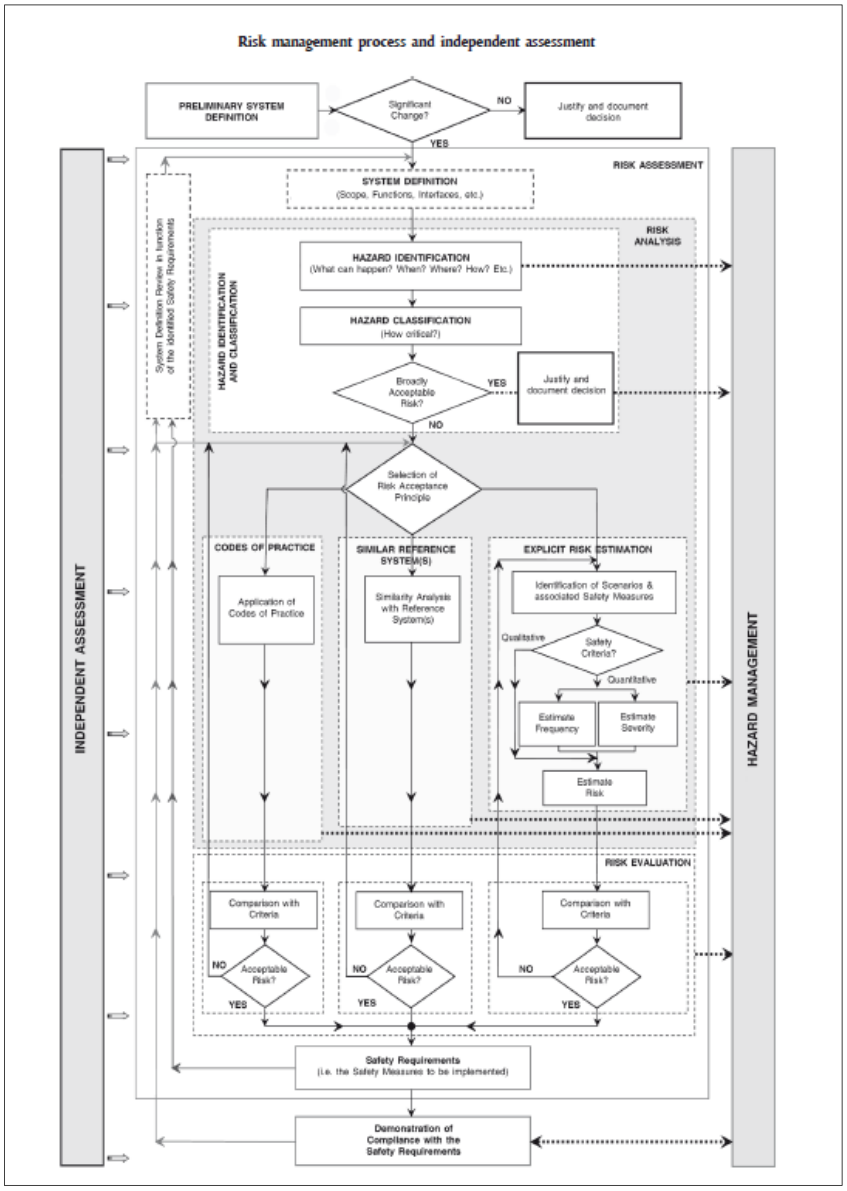


Figure 2 Overall approach to providing safety assurance shown in European Union (2013)

System Description

Application or System context.

The overall system diagram for which the EMA is intended is shown in *Figure 3*. 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 which 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 configuration may be a desirable approach which would be described by a separate GPSC, but is not an essential system requirement.

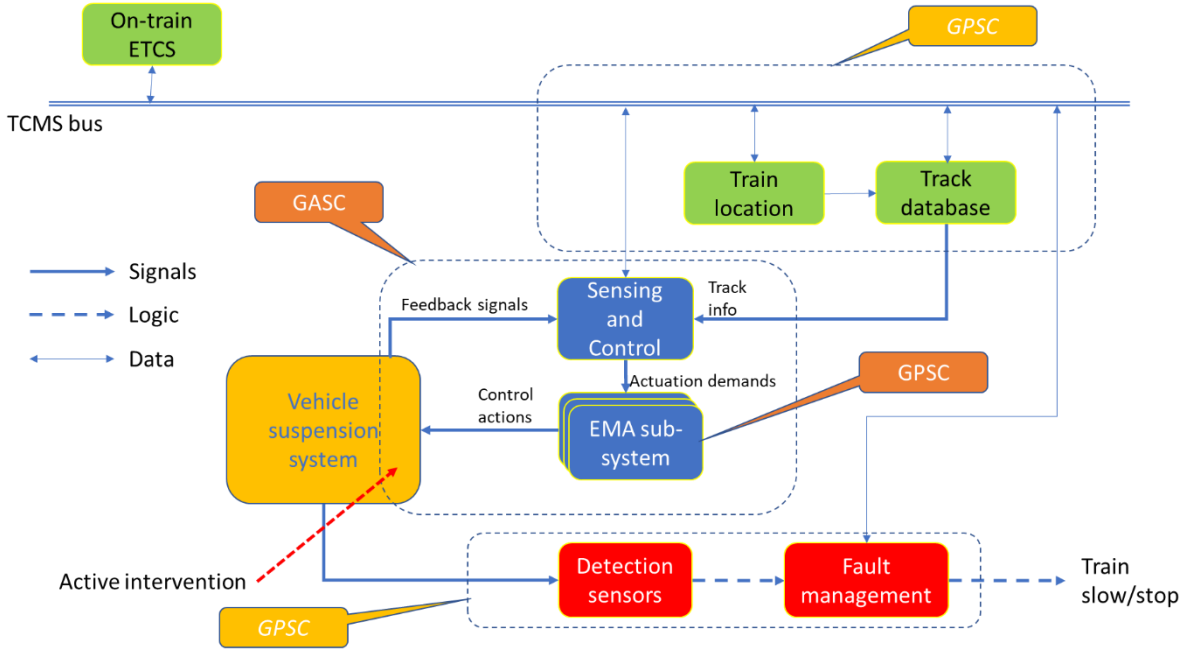


Figure 3 General active suspension system block diagram

Detailed description

This 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) or the provision of functional redundancy will be covered by the GASC.

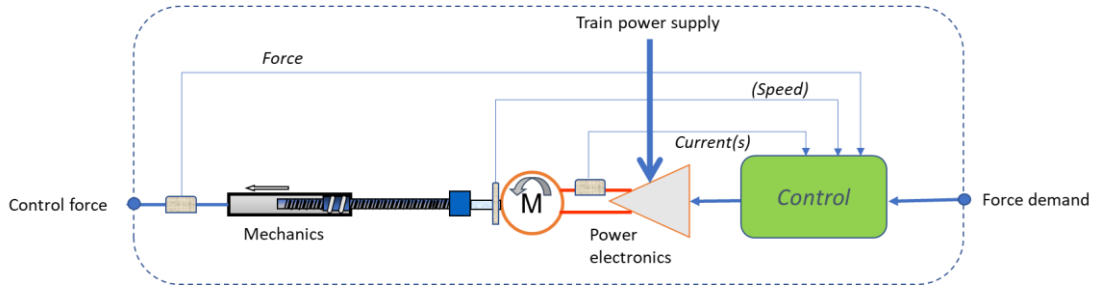


Figure 4 EMA system block diagram

Figure 4 provides a diagram of the EMA scheme and its interfaces within the overall system. It has 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 a DC electrical motor driven by a power amplifier comprising high frequency switched semiconductors giving high efficiency bi-directional control of the power supplied to/from 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 is focussed upon identifying failure modes for the EMA, the effects of which in terms of safe operation must be analysed within each application, which may have differing needs in terms of safe failures. Both analytical/simulation-based assessment are used, supported by hardware-in-the-loop (HiL) bench-testing of one or more of the EMAs.

Identification of sub-systems

The following are the EMA's principal sub-systems:

- Electric motor
- Power electronic amplifier
- Mechanics of lead screw
- Sensors: force, current, (speed)
- Controller
- Cabling (incl. power input)

These are referred to again in Section 4.

Quality Management Report

More guidance is provided in the GPSC template

Quality Management System and Certification

Organisational Structure

Quality processes and assurance of processes

Safety Management Report

This section describes the safety management techniques that were employed during the design, and where applicable development, of the generic product. This section should refer to the safety plan that was used for design and development activities.

Overall safety approach

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic product is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

The safety management approach involves identifying fault modes that can occur in the EMA, and then assessing their effect upon the system. The safety plan involves a hierarchical assessment approach adopted as part of the design and development process. Note that, as observed earlier, the effect of each fault mode upon safety risk depends upon the particular nature of the application and the manner in which the EMAs are to be used. Hence the associated GASC will fully assess the fault effects upon system safety.

General safety (environment, electrical, maintenance, etc.)

[to come]

Functional safety

All subsystems that are identified in Section 2 have documentation and test processes that are required prior to being assembled into a working EMA. These are listed in *Table 1*.

Table 1 Subsystem documents and tests

Subsystem	Approach to demonstrate safety	Failure probability
Electric motor	Initial supplier's QC test certificate Initial product bench test Regular maintenance testing (insulation etc.) Quantification of failure rates	$20x10^{-6}$ /h
Power electronic amplifier	Initial supplier's QC test certificate Initial product bench test Maintenance checks	$20x10^{-6}$ /h
Mechanics of lead screw	Initial product bench test Maintenance checks	$0.025x10^{-6}$ /h (locked)
Sensors: force, current, (speed)	Initial supplier's QC test certificate Initial product bench test Regular maintenance testing Quantification of failure rates	$20x10^{-6}$ /h
Control electronics	Functional hardware design document (and software?) Independent bench test Regular maintenance checks	$10x10^{-6}$ /h (but SIL4 units available)
Cabling	Pre-installation test	$4x10^{-6}$ /h (value for a databus)

Faults in the various subsystems can create or contribute to a variety of EMA fault modes that may may lead to unsafe failures within an active suspension application, and *Table 2* identifies these causalities.

Table 2 Subsystems and fault modes

			Sub-system					
		Motor	Power amp	Mechanics	Sensors	Control electronics	Cabling	Totals need adding
	Per hour	$20x10^{-6}$	$20x10^{-6}$	$0.025x10^{-6}$	$10x10^{-6}$	$10x10^{-6}$	$4x10^{-6}$	
	Fault mode							
H001	Locked	×	×	✓	×	×	×	$0.025x10^{-6}$
H002	Free	×	×	✓	×	×	×	$0.025x10^{-6}$
H003	Zero force	✓	✓	×	✓	✓	✓	Polynomial expansion of 5 terms
H004	Force excess	×	×	×	✓	✓	✓	
H005	Inversion	×	×	×	?	✓	×	$14x10^{-6}$
H006	Random force	×	×	×	✓	✓	×	$14x10^{-6}$
H006	Pulse force	×	✓	×	✓	✓	×	

Locked: This is a purely mechanical fault, arising principally from a catastrophic failure of nut which essentially jams it onto the screw. This only arises if the maintenance checks of the mechanism (too much free play, loss of lubrication) are neglected.

Free: This fault mode would be caused by a mechanical breakage and is distinct from “Zero force” described below.

Zero force: In contrast to the “Free” mode the motor inertia will still be connected to the output

Force excess:

Inversion:

Random force:

Pulse force:

Note: The power amps have a lot of self-protection that disables them, in particular over-current and under- or over-voltage. This would lead to the “Free” fault mode, and this choice of unit is a significant mitigation.

[Still need to complete the descriptions of the other fault modes]

V-lifecycle diagram

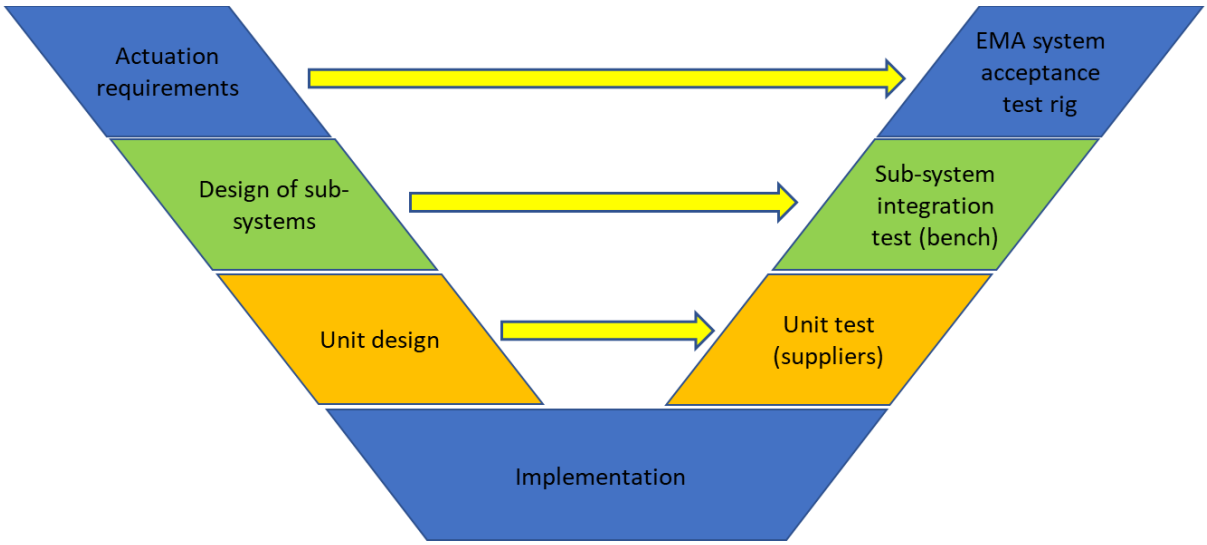


Figure 5 V lifecycle for EMA

Figure 5 shows the V-diagram for the EMA design and development process, and indicates the safety-related checks at each level of the lifecycle:

[List of safety-related checks here]

Actuation testing strategy

It is necessary to ensure that the fault modes identified above are physically tested as identified at the various levels of the V-diagram.

Describe and provide a diagram of the safety lifecycle that was employed. If a Safety Plan exists for the development activities, describe any deviations from the safety plan and approval for the deviations from the Independent Safety Assessor (ISA). Describe the techniques that were used for:

- *functional hazard identification and risk assessment;*
- *design and development of risk controls;*
- *demonstration of suitability of risk controls; and*
- *demonstration on acceptability of residual safety risks.*

Show where the activities were carried out during the safety lifecycle. Describe any standards, guidelines, codes of practice or other documents that were used during the activities.

Describe details of all techniques applied and, if necessary, justify any deviation from standard techniques; explain the guidewords that were used during a failure modes and effects analysis. It is essential that justification is provided to describe why these techniques are appropriate to the design, and where applicable development, of the generic product. Where it is foreseeable that specific products will contain software or are configured by data, describe the software safety techniques and measures that are to be applied in accordance with EN50128.

Provide evidence to demonstrate that these activities cover the full scope of the generic product as described in the Section 2.

Provide documentary evidence or refer to other documents that show that the techniques were applied correctly and that the results of each activity were integrated into the design and development lifecycle. Demonstrate that documents have been signed-off in accordance with the sign-off requirements described in Section 3.

The SMR needs to identify the techniques that will be followed to produce the results shown in the TSR (see Section 5). Amongst other evidence, the TSR requires evidence of correct functional behaviour and demonstration that the product's effect within an active suspension system cannot cause an unsafe condition when operating as designed. It may be practical to integrate the tests to provide this evidence with other functional testing that demonstrates the system meets its functional specification. In these cases, the SMR will need to show how the functional testing activities integrate. It must be clear which evidence from functional testing will be used in the TSR.

Technical Safety Report

Review of safety-related documentation

Provide a list of all design documentation associated with the product for use within an active suspension system. For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

Sub-system analysis and fault modes

Table 3 presents the fault modes that might create safety hazards when the EMA is used in an active suspension application.

Table 3 Fault mode descriptions

ID	Failure mode	Description	Cause(s)	Quantitative probability	Mitigation
1	Locked	Actuator mechanically jammed	Gross failure of ball or roller screw	Possible	Maintenance checks
			Gross failure of motor bearing	Very unlikely	As above
2	Free	Actuator disconnected from load	Broken output shaft	Very unlikely	Shaft designed for life
3	Zero force *[1]*	Motor open circuit	Motor winding fault	Possible	
			Power electronics fault	Possible	
4	Force excess	Maximum or minimum force	Power electronics fault	Possible	
			Force sensor failure	Possible	
5	Inversion	Output force in wrong direction	Incorrect installation	Not possible	Acceptance testing
			Control electronics fault	Possible	
6	Pulse		Control electronics or sensor intermittent fault	Possible	
7	Random		Control electronics or sensor intermittent fault	Possible	

Fault mode probabilities

These are derived from the known failure rates of the subsystems and their contributions to the different faults given in *Table 2*.

[Quantification using FMEA analysis to be added here]

Assessment of fault mode effects - actuator dynamic properties and model

In some cases, assessment of the effects of the fault modes will require dynamic analysis (and or testing). For this reason, a dynamic model of the EMA is provided that can be used as part of the corresponding GASC. *Figure 6* is a general diagram for a force-controlled actuator within an active suspension. The force command to the actuator would be generated by an active suspension controller, which will be detailed within the GASC. The track input will impact upon the dynamic system, and this will cause actuator movement which the force control loop must counteract in order to keep its force as close as possible to that being demanded. Since the actuator is connected across the secondary suspension, its movements at low frequencies will be small as the vehicle follows the intended features of the track, but relatively large at high frequencies as the suspension provides isolation by absorbing the track irregularities. How well the actuator generates the force required of it in the presence of the high frequency movement depends upon the characteristics of the actuator, and it is not possible to generalise.

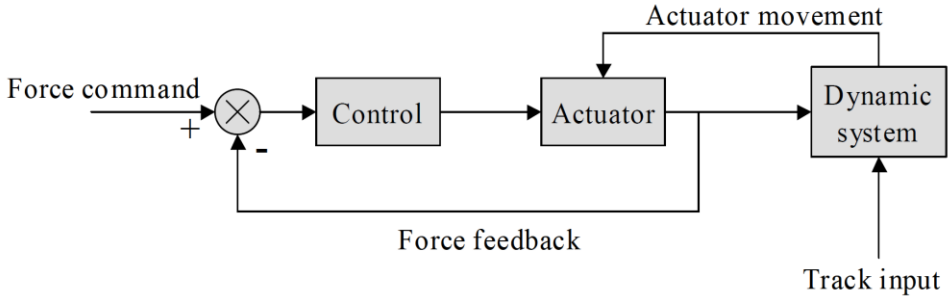


Figure 6 Force-controlled actuator – generic scheme

It is however essential that the actuator's dynamic model provides the actuator movement feedback, which would only be quantified in the context of an application, i.e. within an associated GASC. *Figure 7* provides the model which is used [add ref], and Appendix 1 provides parameter information. A key feature is the "Series stiffness 1" element connected to the output of the actuator which has the effect both of facilitating the force loop control at higher frequencies if required and providing isolation in the case of a locked actuator. The value of this will be chosen to suit the type of active suspension application, i.e. within the GASC.

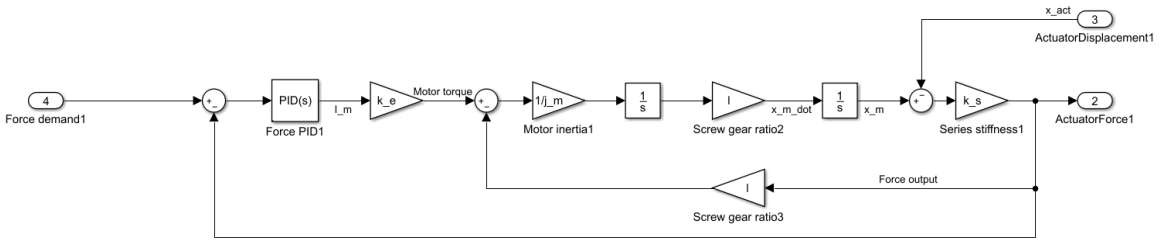


Figure 7 Block diagram dynamic model for EMA showing force control loop and assuming the motor is current-controlled

The model enables the fault modes listed above to be simulated in conjunction with the vehicle model, and the corresponding effects to be assessed in the context of the particular application.

Actuation test results

[Would be included in a real GPSC]

Operation with External Influences

This section is required regardless of the approach used to demonstrate safety.

Safety-related Application Conditions & Assumptions

This section is required regardless of the approach used to demonstrate safety.

Provide a full list of all rules, conditions, constraints and assumptions that must be maintained for the system to remain in a safe state. Where necessary provide references to other documentation that detail the necessary information; for example the system maintenance manual. Where assumptions have been made in the safety case, evidence must be provided for why the assumptions are reasonable.

Other Outstanding Safety Issues

It is possible that no additional information is required to support the safety argument. In such cases, in order to demonstrate completeness of the safety case, the heading should be retained and a note should be made that no further information is necessary.

Describe any further information that is relevant to the safety argument that has not been included in other parts of this document. In particular, where the information in the TSR demonstrates that any tests were failed, provide a description of the failed test, an analysis of the impact of the failure, and information on how the system will remain safe regardless of the failure. Where necessary refer to other parts of this safety case.

Conclusion

A conclusion is required for all safety cases.

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under all reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

References

European Standard EN 50126-1:2017; Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS process.

European Standard EN 50126-2:2017; Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems approach to safety.

European Union; 2013. Official Journal of the European Union L 121; Legislation Volume 56; 03 May 2013.

[add ref for EMA dynamic model]

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.

List any related safety cases, such as safety cases for sub-systems or components that are required as a part of the generic product.

Appendices

Appendix 1 Parameter information relevant to actuator model (*Figure 7*)

[list needed here for the specific actuator design]

Contract No. 777564

8.7 EXAMPLE: GENERIC APPLICATION SAFETY CASE FOR ACTIVE LATERAL SUSPENSION WITH ELECTRO-MECHANICAL ACTUATORS (EMAS)

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Example: Generic Application Safety Case for Active Lateral Suspension with Electro-Mechanical Actuators (EMAs)

Contents

Introduction

Background: purpose and scope

This document is the Generic Application Safety Case (GASC) that provides evidence that an active lateral secondary suspension using electro-mechanical actuators (EMAs) is safe.

Summary description of active suspension application

The aim is to use a pair of force-controlled EMAs horizontally fitted between the bogie frame and the vehicle car body, one actuator for each bogie. This configuration enables the lateral and yaw modes of the secondary suspension to be controlled to provide improved suspension performance. The sensing involves displacement sensors measuring the lateral secondary suspension displacements and lateral accelerometers to measure the absolute motions of the vehicle body. A variety of control approaches are possible.

The system has an independent monitoring function (perhaps part of the Condition Monitoring System) which has a separate set of inertial sensors that is used to detect an unacceptably high level of acceleration in the vehicle body that might arise in the case of one of the EMA fault modes. The monitoring system is used to disable the active suspension system if required.

Brief description of safety approach

This document makes reference to the (example) GPSC for an electro-mechanical actuator. It also refers to an additional monitoring GPSC (example not yet written). It is intended that both GPSCs should be read in conjunction with this GASC document.

Figure 1 illustrates how in general the different safety cases may combine to provide the safety assurance, and also has highlighting to show the relationship for this specific application of an active lateral secondary suspension system using EMAs.

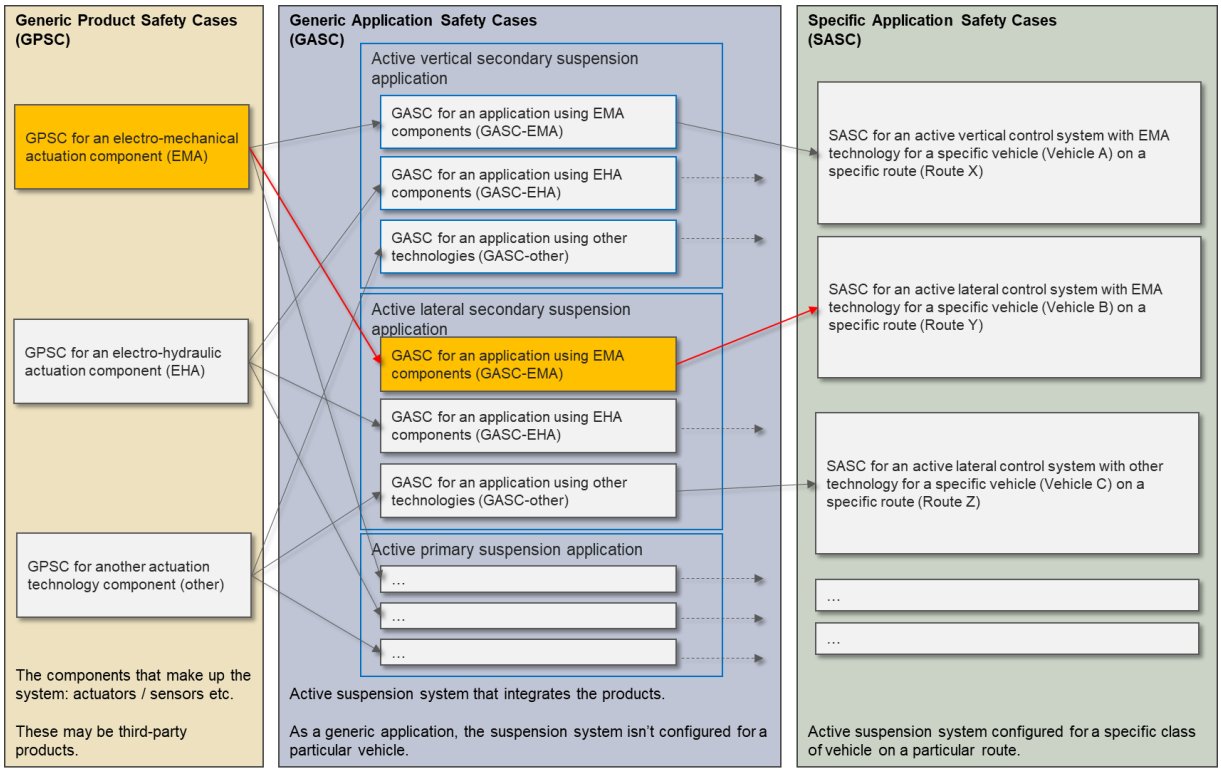


Figure 1 Relationship between Safety Case documents

This GASC focusses on the essential functionality of the active lateral secondary suspension utilising EMAs, although it might also rely upon other Generic Product Safety Cases (GPSCs) that deal with additional technologies to be incorporated, e.g. a track database system to provide "preview" information for the active control system, in this particular application this function is not used. This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the generic application and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.

Safety assurance strategy and method

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations [1]. *Figure 2* is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

This GASC is based upon the third option, explicit risk estimation, but still involving codes of practice, in particular EN14363 [2]. Evidence will be provided that no combination of the EMA fault modes (as set out in the EMA GPSC) will create an unsafe running condition.

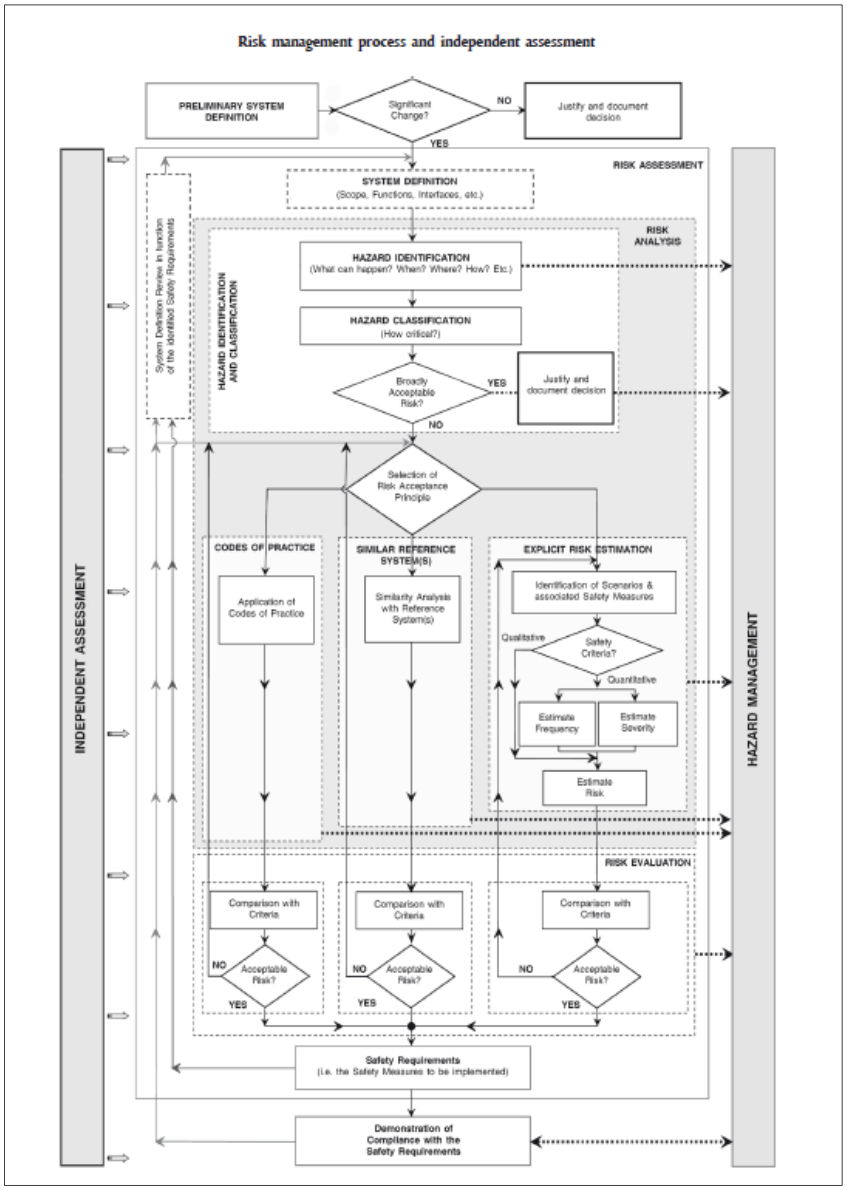


Figure 2 Overall approach to providing safety assurance shown in European Union (2013)

The detailed demonstration of safety compliance within this overall strategy will be achieved through compliance with the European standard for demonstrating reliability, availability, maintainability, and safety for railway applications [3]. This standard requires a safety case to be developed that comprises:

- system description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

System Description

Detailed active suspension description

The system description is shown in *Figure 3*. 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 (described in sub-section "Control functionality and diagram"). 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).

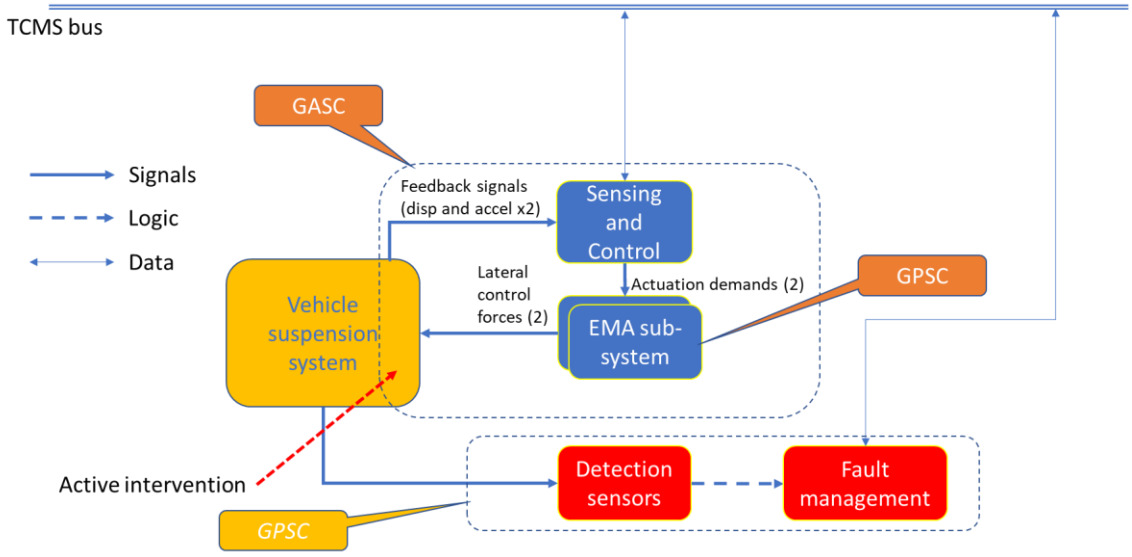


Figure 3 Overall system diagram for active lateral secondary suspension

The detection system 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 is described in the "High Acceleration Detection" GPSC.

Interfaces to GPSCs

EMA GPSC: As shown in *Figure 3* the EMAs receive force commands from the sensing and control subsystem and produce corresponding forces to be applied to the vehicle suspension system in order to change its dynamic characteristics.

High Acceleration Detection GPSC: There are no direct interfaces because a high acceleration event is communicated to the Active Suspension System via the TCMS so that the driver is aware of the problem on one of the vehicles.

[Probably there should be a reference to the TCMS but this will be provided separately]

Control functionality and diagram

Controller description – non-modal and modal, "Skyhook" or "Complementary filter" types.

[To be added, although probably not important for fault mode analysis]

Quality Management Report

The Quality Management Report (QMR) provides information on the management and assurance procedures that were in place to achieve and demonstrate quality of the product. Information in the QMR is typically the same for all systems developed within the same organisation. Guidance on appropriate content for the QMR has been provide in the GASC template and has not been repeated in this document.

Quality Management System and Certification

Refer to GASC template for guidance regarding what is required

Organisational Structure

Refer to GASC template for guidance regarding what is required

Quality processes and assurance of processes

Refer to GASC template for guidance regarding what is required

Safety Management Report

This section describes the safety management techniques that were employed during the design, and where applicable development, of the generic application. This section should refer to the safety plan that was used for design and development activities.

Overall safety approach

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic application is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

The safety management approach includes the identification of fault modes that can occur in the EMA, and then an assessment their effect upon the system. The safety plan involves a hierarchical assessment approach adopted as part of the design and development process. Note that, as observed earlier, the effect of each fault mode upon safety risk depends upon the particular nature of the application and the manner in which the EMAs are to be used.

General safety (environment, electrical, maintenance, etc.)

[to come]

Functional safety

The individual EMA fault modes are assessed firstly using dynamic simulation based upon a well-established Multi-Body Software against the requirements of EN14363 and other relevant codes. This approach identifies the fault modes that may cause unsafe conditions and which need some mitigating action, in particular the High Acceleration Detection System.

Fault modes which simulation has shown not to cause an unsafe condition are assessed by static/depot testing during initial commissioning in order to verify that the fault mode effect results from static tests are consistent with the simulation results. Track testing is used to validate the mitigation measures used to ensure the safety of fault modes that simulation has shown might otherwise be unsafe. Similarly additional track tests may be specified where static/depot testing has not proved the safety of other EMA fault modes.

[Need to show that the High Acceleration Detection device meets the specified safety level]

V-lifecycle diagram

Figure 4 shows the development of the active suspension system.

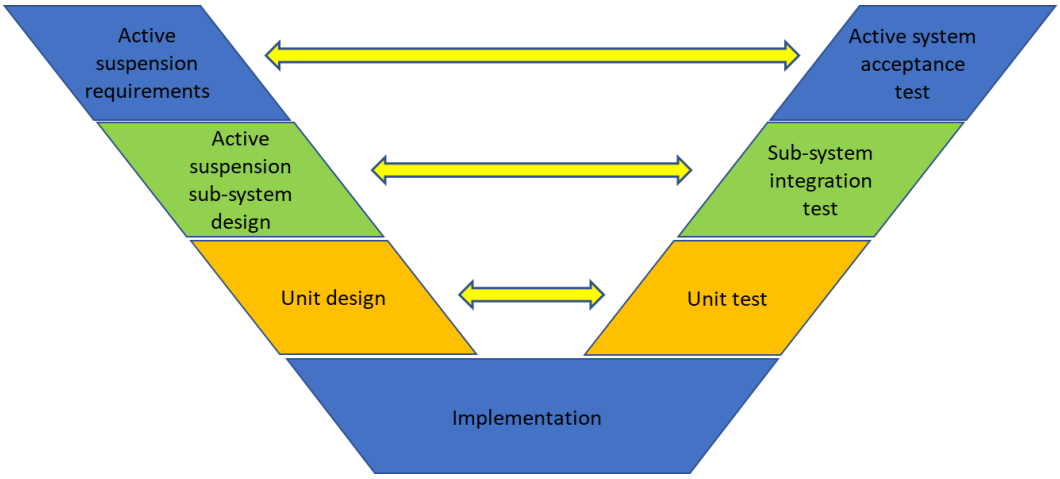


Figure 4 V diagram for active suspension system

Testing requirements

[A full GASC would describe in detail the overall approach involving simulation, laboratory (static) testing and track testing.]

Vehicle testing strategy

[A comprehensive statement setting out the track testing strategy needed here.]

Technical Safety Report

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

Review of Safety-Related documentation

For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles.

Analysis of fault mode effects

Provide a list of the safety analysis techniques described in the SMR. For each technique, provide the technical results. For example if an FMEA is stipulated in the SMR, then provide details of the FMEA, details of staff who were involved together with references to the QMR that describes staff expertise. Provide the results of the FMEA.

Initial filtering of fault modes is carried out via simulation to determine any that might affect upon safe operation. The model provided within the GPSC has been used in co-simulation with a Simpack dynamic model of the vehicle.

The hazard log shown in *Table 1* presents the safety hazards identified during the safety analysis based upon both the actuator model from the EMA GPSC and a detailed vehicle model in an MBS simulation package. (**Note**: table is indicative to illustrate the principles, i.e. not complete.)

Table 1 Hazard list

Hazard ID	Hazard name (EMA fault mode)	Status	Other responsible party	Risk	Comments	Reference to other hazards
H001a	Leading EMA locked	Closed	Maintainer	None	Car body accel increased	
H001b	Trailing EMA locked	Closed	Maintainer	None	Car body accel increased	
H002a	Leading EMA free	Closed				
H002b	Trailing EMA free	Closed				
…		Open/closed				
…						
H005a	Leading EMA force inversion	Open				

H005b	Trailing EMA force inversion	Open				

For each hazard listed in *Table 1* the following Tables (2-?) provide full technical comments related to their effect upon vehicle safety. (**Note**: only two of the tables are complete to illustrate the principles, i.e. not complete. One example illustrates a safe fault effect, one illustrates a potentially unsafe fault)

Table 2 Hazard 001a description

Hazard ID	H001a
Hazard name	Leading EMA locked.
Status	Closed
Hazard cause	Refer to GPSC
Hazard consequence	Increased carbody acceleration (lower ride quality) but not unsafe
Hazard source	Identified in the GPSC (Table?), analysed by simulation as part of GASC safety process
Severity	Enhanced levels of acceleration on car body, but no effect upon EN14363 safety criteria
Frequency	Very infrequent (?? per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*State where evidence of closure of the hazard can be found, in many cases the evidence will be another part of the TSR.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

[Table 3 very similar to Table 2; Tables 4-9 would be completed in a full SC]

Table 10 Hazard 005a description

Hazard ID	H005a
Hazard name	Leading EMA force inversion.
Status	Closed
Hazard cause	Refer to GPSC (Table ?)
Hazard consequence	Transient exceedances of EN 14363 Y/Q limits and high lateral forces on the track

Hazard source	Identified in the GPSC (Table?), analysed by simulation as part of GASC safety process
Severity	Potentially infringing EN14363 safety criteria
Frequency	Very infrequent because potential causes of inversion should be eliminated during commissioning. Software correctness needs to be assured.
Risk	Low
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*State where evidence of closure of the hazard can be found, in many cases the evidence will be another part of the TSR.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

[Table 11 similar to Table 10, and remaining Tables 11-15 would need to be completed]

Summary of dynamic simulations

Results of the fault mode analysis using Simpack/Simulink co-simulation are given in Appendix 1. All fault modes have been tested, although always on one bogie only. The series stiffness of the EMA (mentioned in the GPSC) has been selected to have a relatively low level of 1MN/m which both enables effective force loop control at higher frequencies and mitigates the effect of the Locked Actuator fault mode.

These indicate that the only fault mode for which there is a possible effect upon running safety is the inverted force output from the EMA. This shows a derailment ratio Y/Q which exceeds the limit level defined in EN45363, although these are occurrences for which the simulation didn't actually predict derailment. This fault mode also predicted excessive lateral track forces, maximum levels of around ??kN compared with the EN14353 code of practice's maxima of ??kN. This is certainly a condition that needs to be avoided.

Mitigation measures

Associated with the high Y/Q and lateral force levels arising from the inversion fault modes is a profound increase in car body acceleration levels.

(Static test results)

[Needed for a complete GASC]

(Track test results)

[Needed for a complete GASC]

Operation with External Influences

Refer to the guidance in the GPSC template for the information that should be included.

Safety-related Application Conditions & Assumptions

Refer to the guidance in the GPSC template for the information that should be included.

Other Outstanding Safety Issues

Refer to the guidance in the GPSC template for the information that should be included.

Conclusion

A conclusion is required for all safety cases.

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under all reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

References

1. Commission Implementing Regulation (EU) 2015/1136, “Common safety method for risk evaluation and assessment”
2. BS EN 14363:2016+A1:2018 Railway applications. “Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests”
3. EN50126-1/2 (2017) “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)”.

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.

List any related safety cases, such as safety cases for subsystems or components that are required as a part of the generic application.

Appendices

Appendix 1 Detailed simulation analysis of Fault Cases

A secondary lateral active suspension system is utilized to investigate the consequence of the actuator failure. In this active control system, the classic skyhook method is adopted to improve the lateral dynamic behaviours of the carbody. In this lateral control system, the lateral and yaw motions of the carbody are controlled separately via the modal control approach. The dynamics parameters of the Run2Rail conventional bogie vehicle are adopted in this example. The track irregularity of British Railway 'Track110' is utilized in this simulation task. For the condition of the simulation, the bogie vehicle operates on the tangent track at a speed of 110 km/h. The Co-simulation of Simapck and Matlab/Simulink is chosen to realize the simulation of the active suspension system.

Figure A1 and Figure A2 demonstrate wheel/rail lateral force and derailment coefficient of the leading wheelset of the leading bogie without any fault in the control system, which keep at reasonable values according to the standard EN14363. The following figures (Fig. A3 and Fig. A4) represent the lateral acceleration and displacement of the carbody without any faults in the control loop. It can be noticed these signals stay in a low level due to the active suspension system.

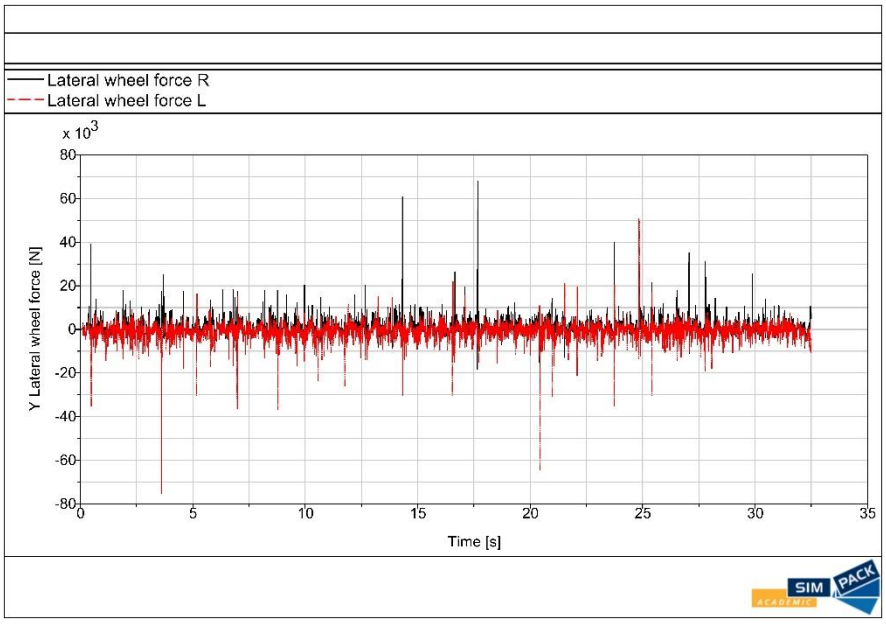


Figure A1. Lateral wheel/rail lateral force of the leading wheelset without fault in control system.

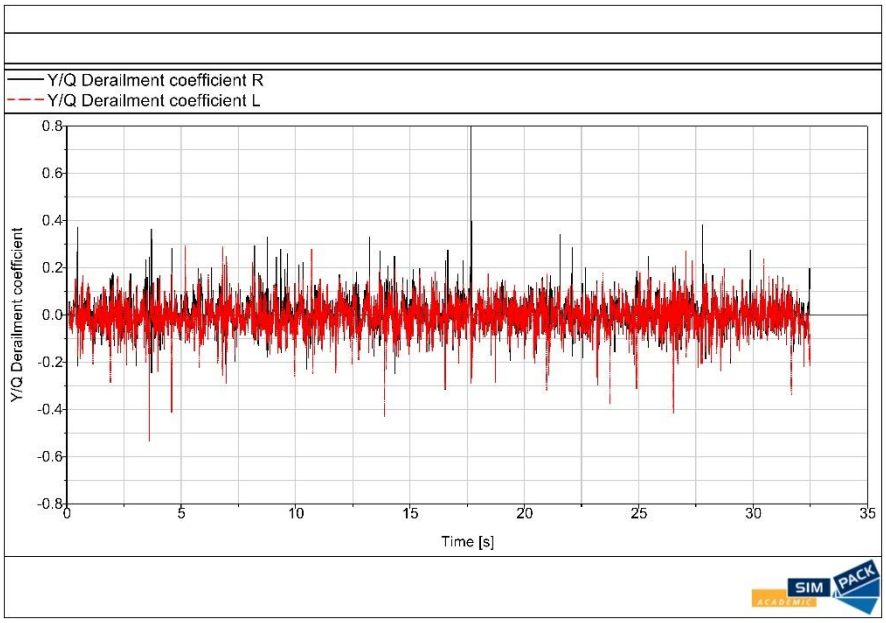


Figure A2. Derailment coefficient of the leading wheelset without fault in control system.

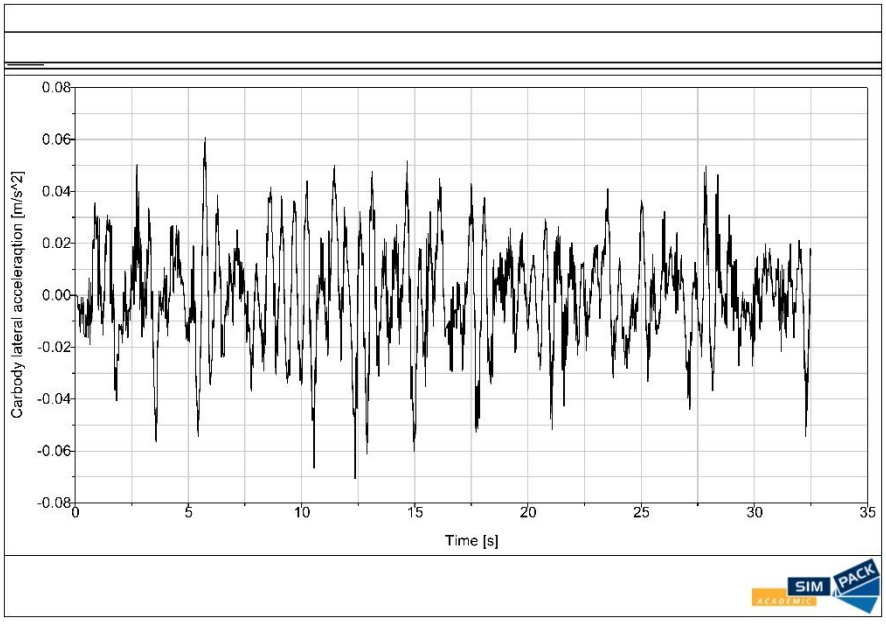


Figure A3. Lateral acceleration of carbody without fault in control system.

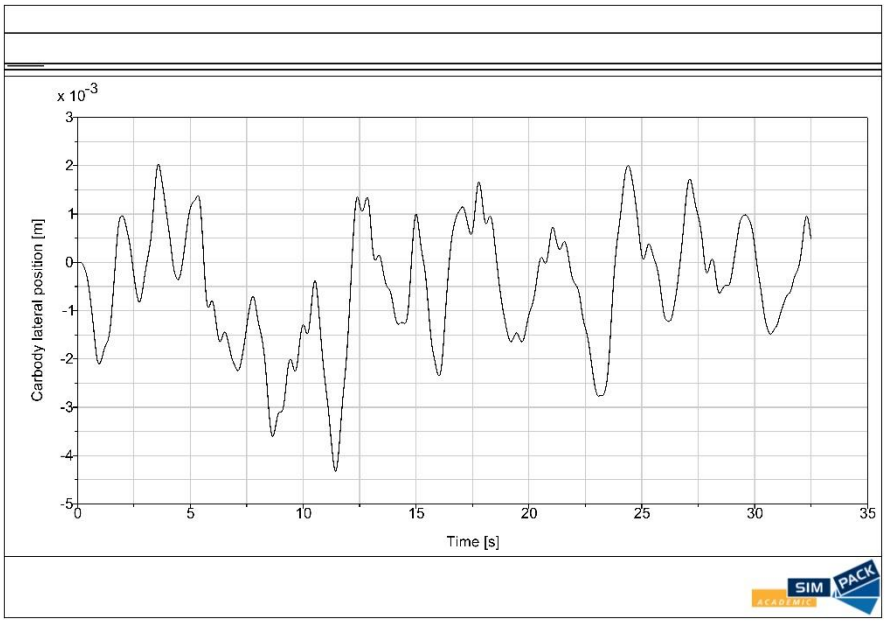


Figure A4. Lateral displacement of carbody without fault in control system.

Several critical actuator failure modes are simulated for the safety evaluation concerning the same running condition. The actuator failure modes include lock, free, zero force, max/min force and inversion. These fault configurations can be realized with the control models of the electromechanical actuators in the Matlab/Simulink environment. In this section, the fault is only applied to one actuator, the leading one in these cases. Single actuator failure is much more likely to happen than the failure of both actuators. The co-simulation results are analysed for each fault cases, especially from the safety and comfort perspectives. Regarding the simulation results, the actuator inversion fault should be categorized as a very serious fault and probably result in severe safety consequences during the operation. All the faults lead to the degradation of the comfort with the intensified acceleration and/or larger suspension deflection, whereas the faults related to lock, free, zero force and max/min force have very limited influence on the safety index, such as the derailment coefficient.

For the inversion fault case, the actuation system actually forms a ‘positive’ feedback loop instead of a normal ‘negative’ one. It means the vibration energy will be amplified by the active suspension system, whose main function should be to isolate the vibration. In this scenario, the actuation force fluctuates between the maximum and minimum threshold values of the control system, as shown in Figure A5. Even though the inversion fault is only applied to the leading bogie actuator, both leading and trailing actuators demonstrate the similar ‘Peak-to-peak Force’ feature. Due to the ‘positive’ feedback effect, the very high lateral wheel/rail forces take place continually for the wheelsets of the leading bogie as illustrated in Figure A6, which exceed the limit value of 60 kN in EN14363. Consequently, the derailment coefficient is extremely high compared with the reference value of 0.8 in EN14363, shown in Figure A7. In Figure A8, it can be seen that the wheelset in the trailing bogie without actuator fault also exhibits obvious wheel/rail lateral interactions. Furthermore, the lateral acceleration and displacement of the carbody exhibit frequent oscillations with very high peak values (See Fig. A9 and Fig. A10).

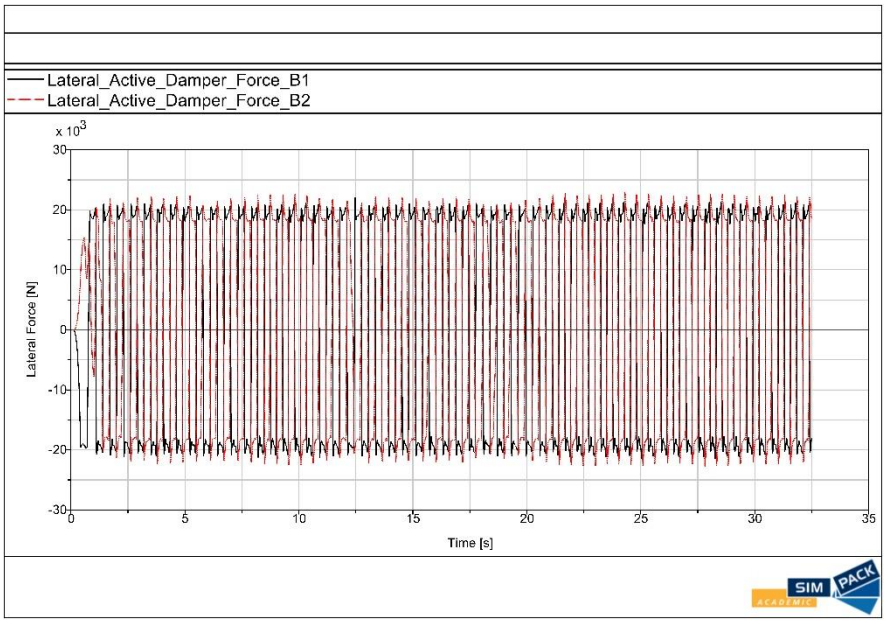


Figure A5. Actuator forces with inversion fault in actuation system.

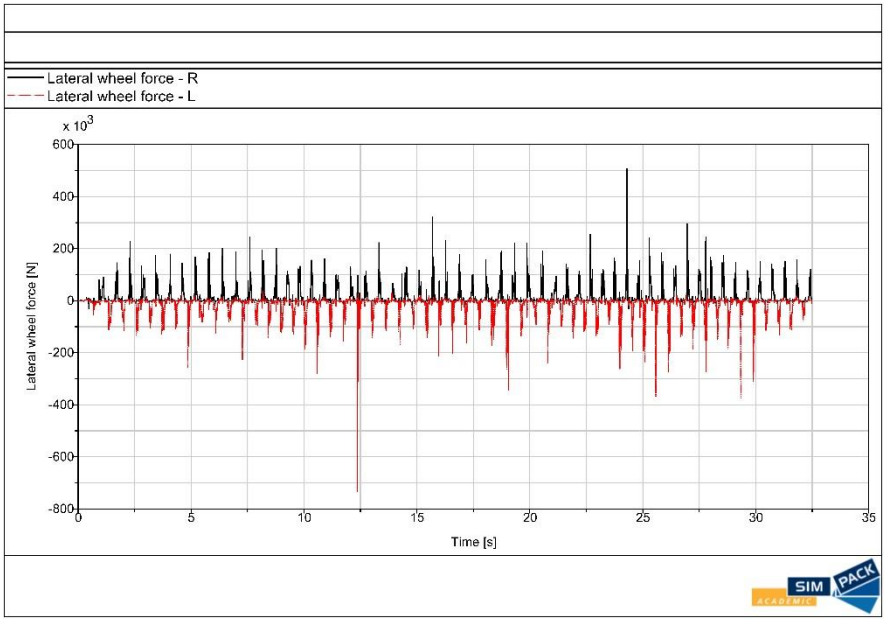


Figure A6. Lateral wheel/rail forces of the leading wheelset with inversion fault in actuation system.

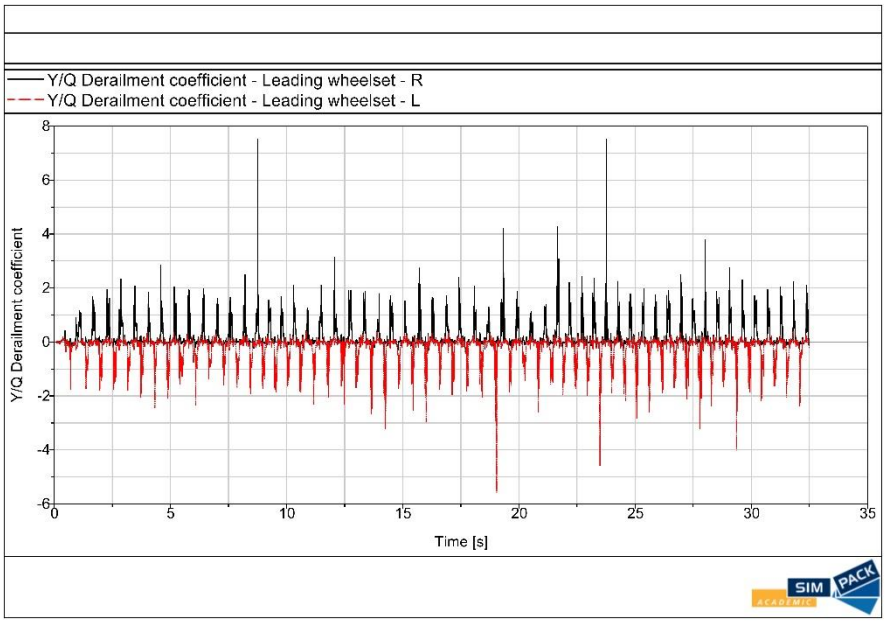


Figure A7. Derailment coefficient of the leading wheelset with inversion fault in actuation system.

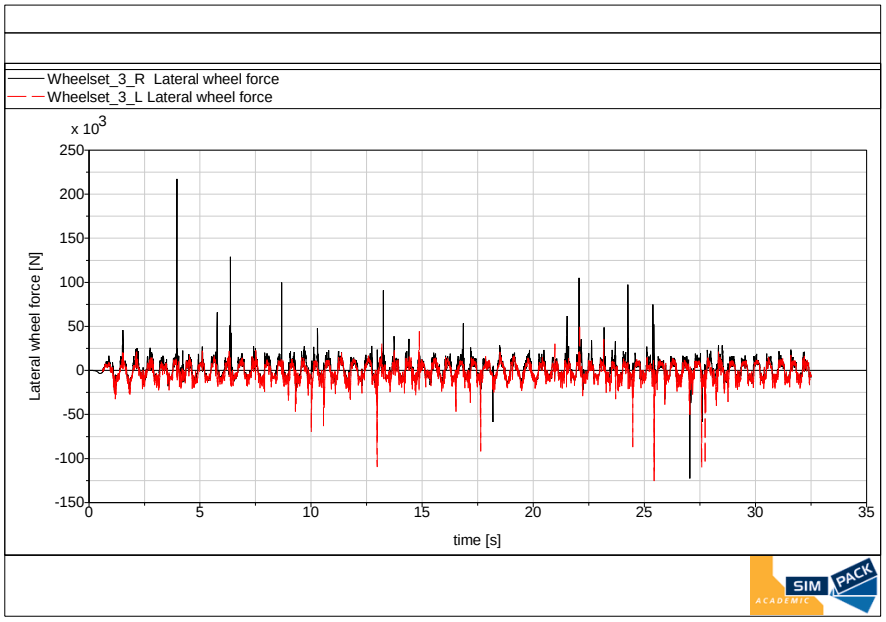


Figure A8. Wheel/rail lateral force of the wheelset of the trailing bogie without fault.

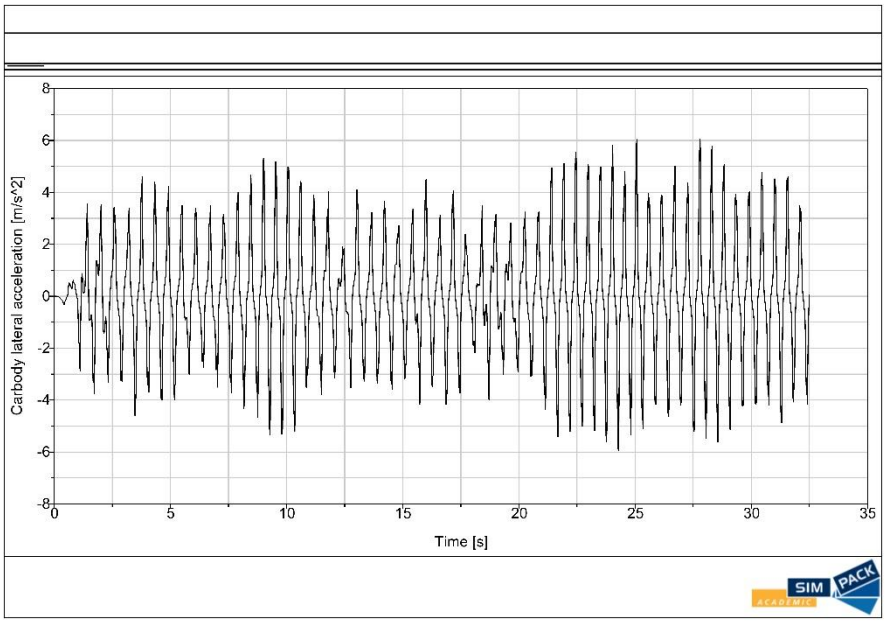


Figure A9. Lateral acceleration of carbody with inversion fault in actuation system.

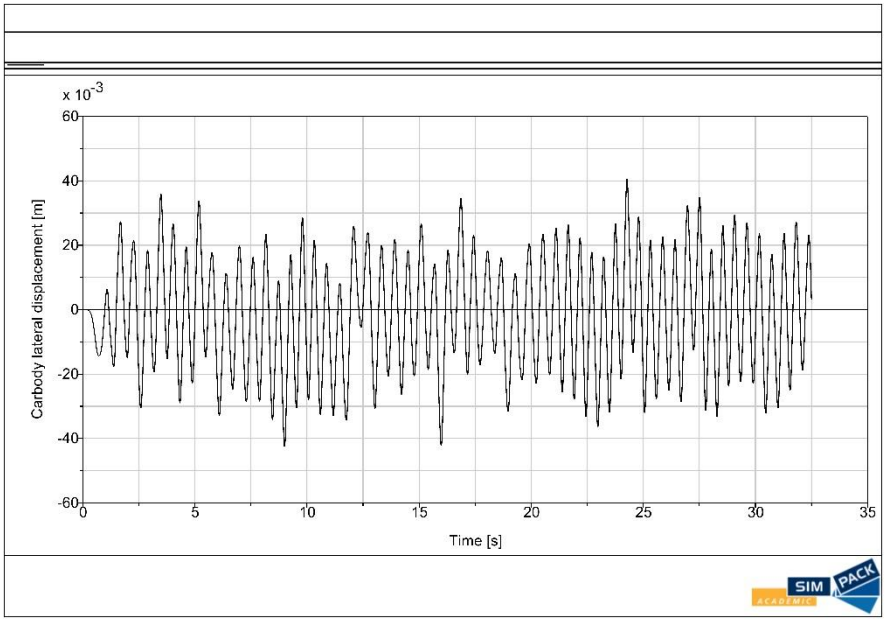


Figure A10. Lateral displacement of carbody with inversion fault in actuation system.

For the actuator locked case, the actuator cannot generate the active force according to the control command; however, the screw of the electromechanical actuator has certain stiffness and is still connected with the carbody and bogie frame. In this situation, the actuator functions as a passive spring between the carbody and bogie frame. In this simulation, the stiffness of the screw is 1 MN/m, which is higher than a normal secondary lateral stiffness value. Figure A11 and Figure A12

exhibit the lateral acceleration and displacement of the carbody. The carbody acceleration is higher than the normal condition with oscillations due to the increased stiffness. No abnormality is noticed in the derailment coefficient for this fault case (see Fig. A13).

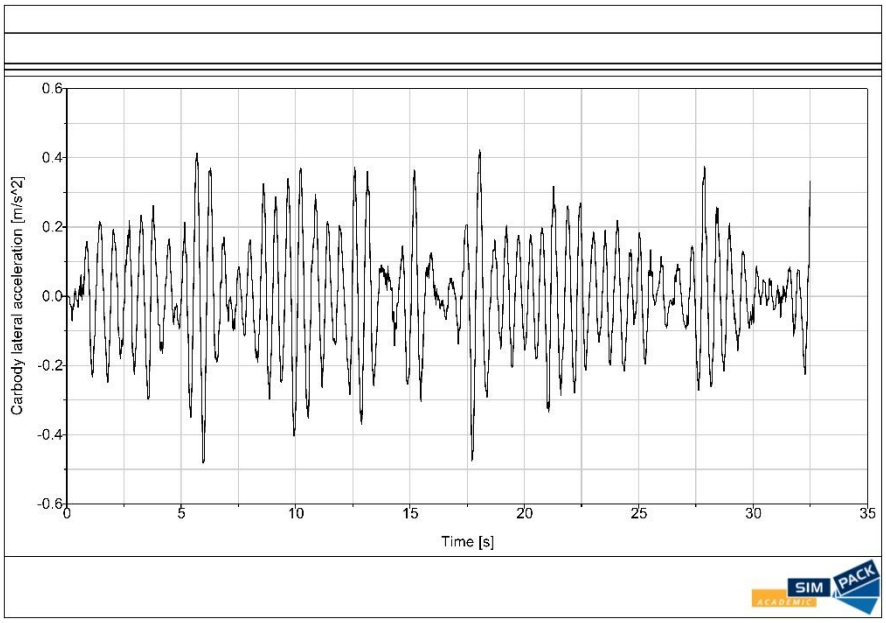


Figure A11. Lateral acceleration of carbody with locked fault in actuation system.

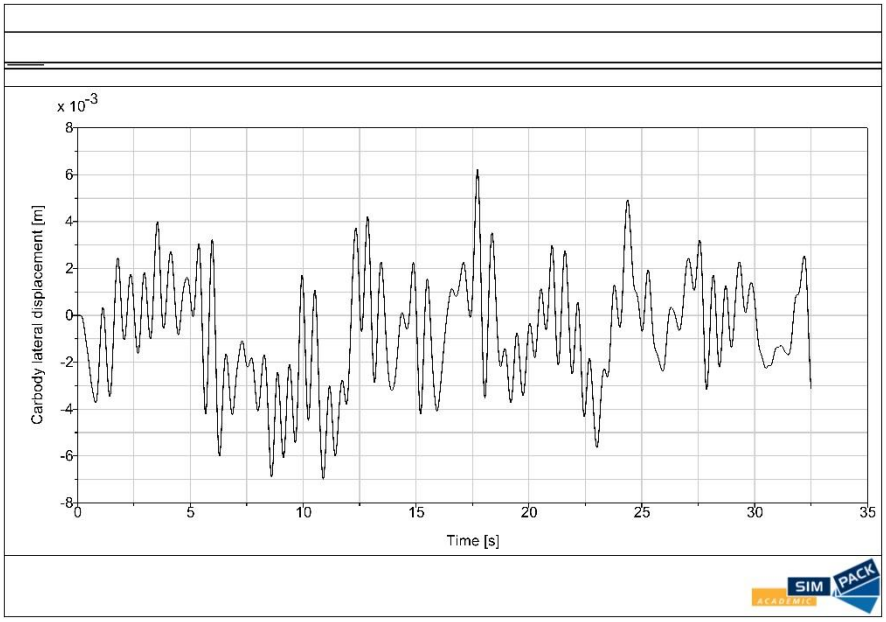


Figure A12. Lateral displacement of carbody with locked fault in actuation system.

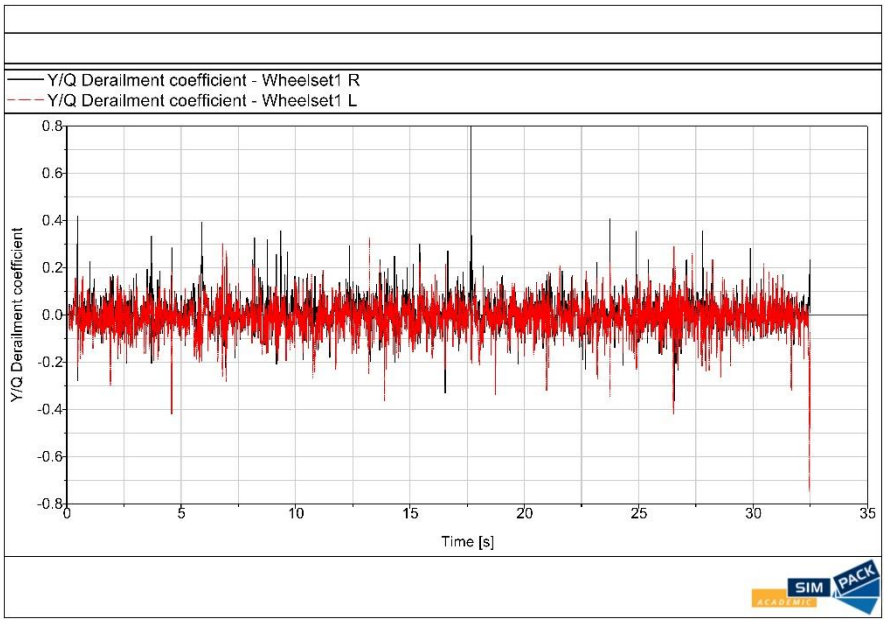


Figure A13. Derailment coefficient of leading wheelset with locked fault in actuation system.

For the free fault case, the actuator is physically disconnected from the carbody and bogie frame. There is no influence of the actuator on the dynamic behaviour of the vehicle. The actuator is modelled as it is removed from the system. Since almost no damping in the lateral direction can be provided by the secondary suspension, higher acceleration and large deflection of the suspension of the carbody can be noticed, as shown in Figure A14 and Figure A15. No abnormality is identified in the derailment coefficient for this fault case (see Fig. A16).

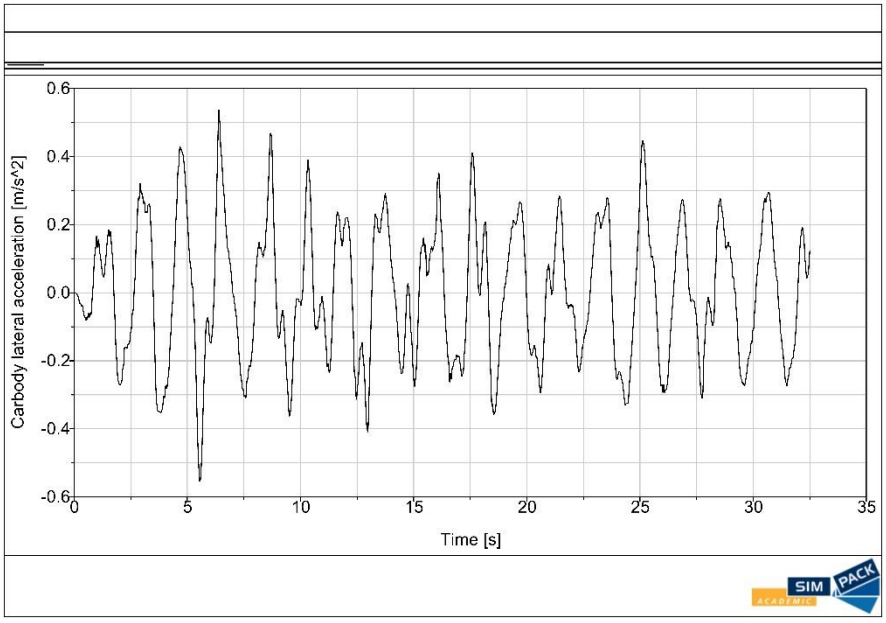


Figure A14. Lateral acceleration of carbody with free fault in actuation system.

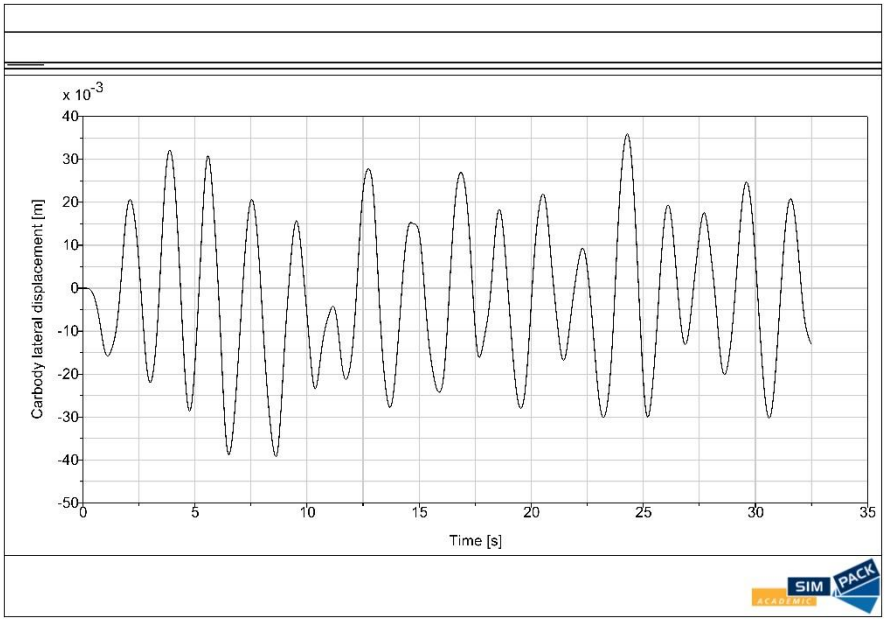


Figure A15. Lateral displacement of carbody with free fault in actuation system.

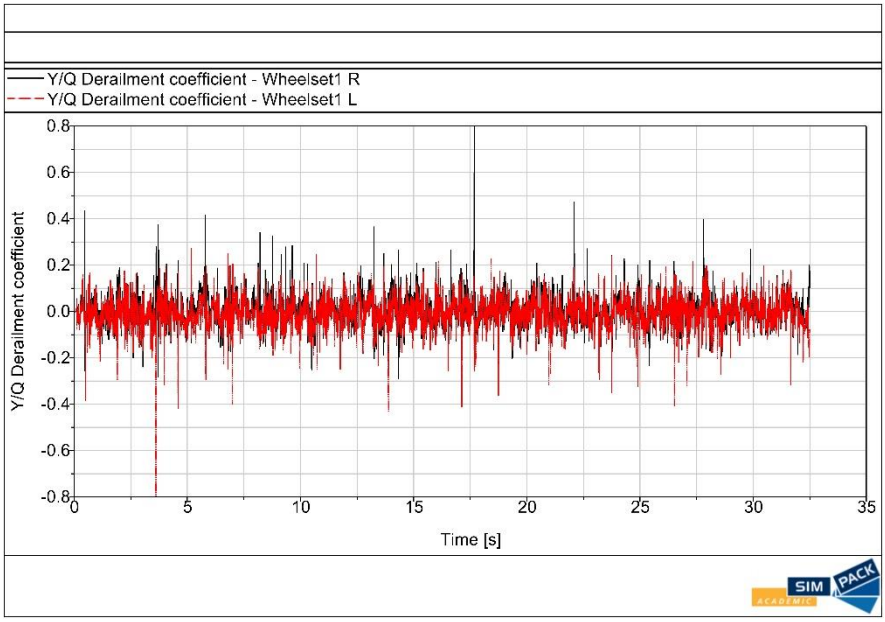


Figure A16. Lateral displacement of carbody with free fault in actuation system.

For the scenario of zero force input, the actuator cannot generate the desired force with the control command. Distinguished from the locked case, the actuation screw of actuator can still move freely with the rotor of the DC motor. In this way, the rotor and the screw form a mechanical feedback loop, which is necessary to consider its effect to the vehicle system. Figure A17 and Figure A18 exhibit the lateral acceleration and displacement of the carbody. The carbody acceleration is higher

than the normal condition with high-frequency oscillations due to the rotor motions. No abnormality is identified in the derailment coefficient for this fault case (see Fig. A19).

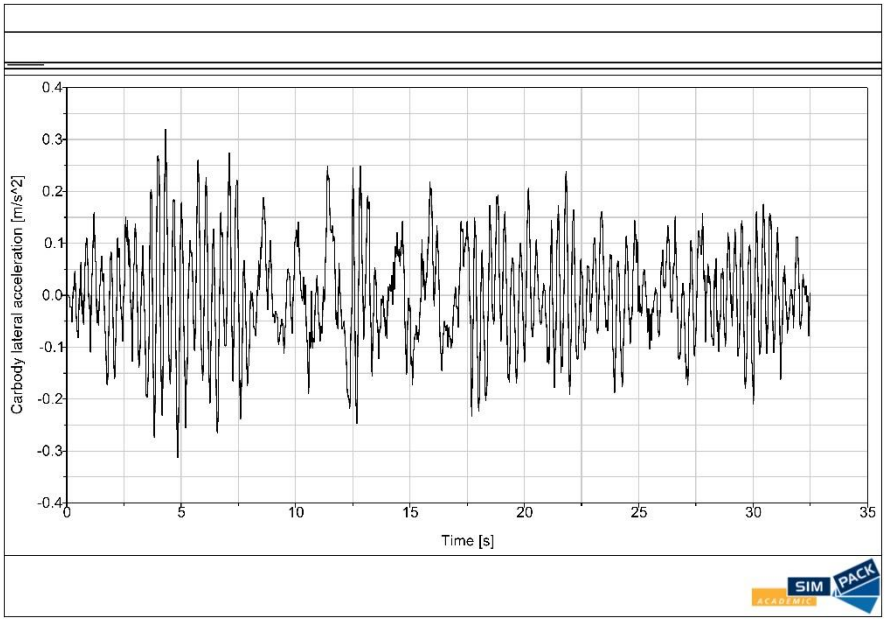


Figure A17. Lateral acceleration of carbody with zero-force fault in actuation system.

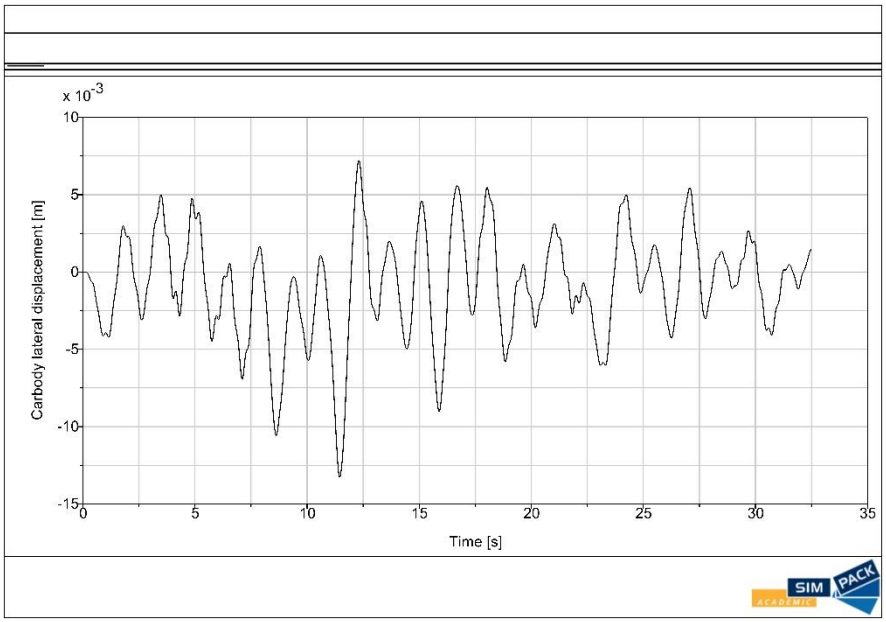


Figure A18. Lateral displacement of carbody with zero-force fault in actuation system.

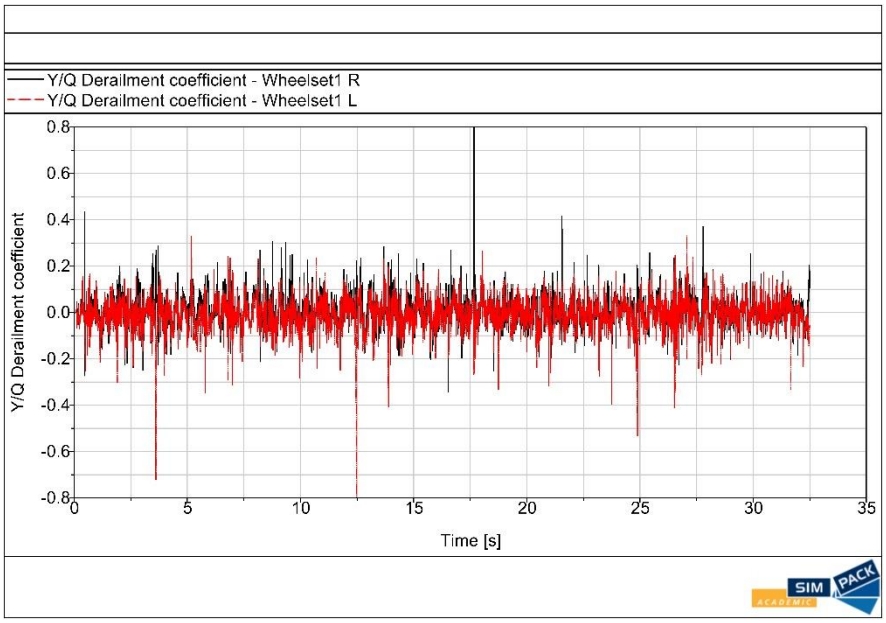


Figure A19. Derailment coefficient of leading wheelset with zero-force fault in actuation system.

For the fault case of Max/Min force, the excess force pushes the carbody laterally to one side of the bogie and hits the bumpstop. It leads to a large stiffness between the carbody and bogie frame, which is comparable with the locked case. Figure A20 and Figure A21 exhibit the lateral acceleration and displacement of the carbody. It can be noticed the carbody position deviates from the track centre line. The carbody acceleration is higher than the normal condition, because of the high contact stiffness by the bumpstop. No abnormality is identified in the derailment coefficient for this fault case (see Fig. A22).

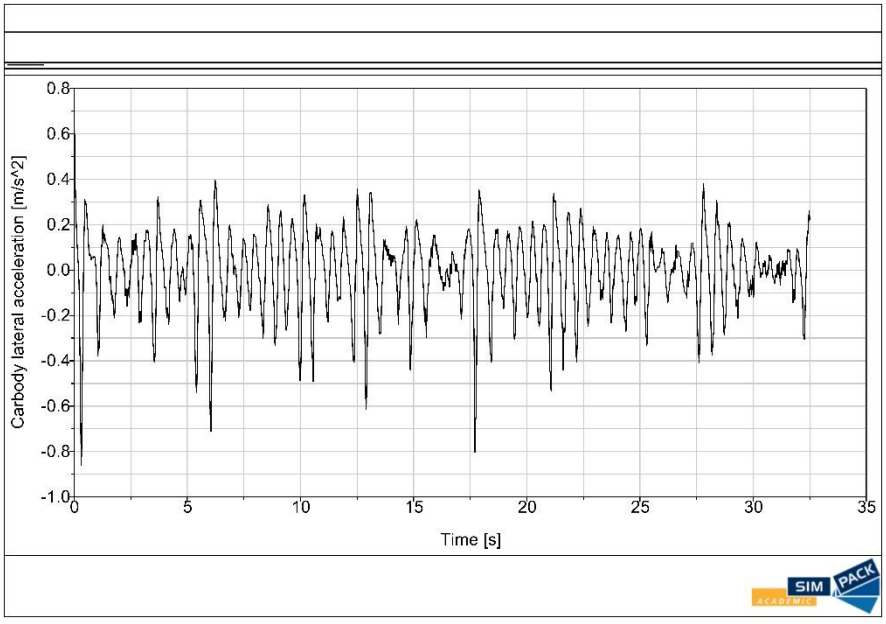


Figure A20. Lateral acceleration of carbody with Max/min force fault in actuation system.

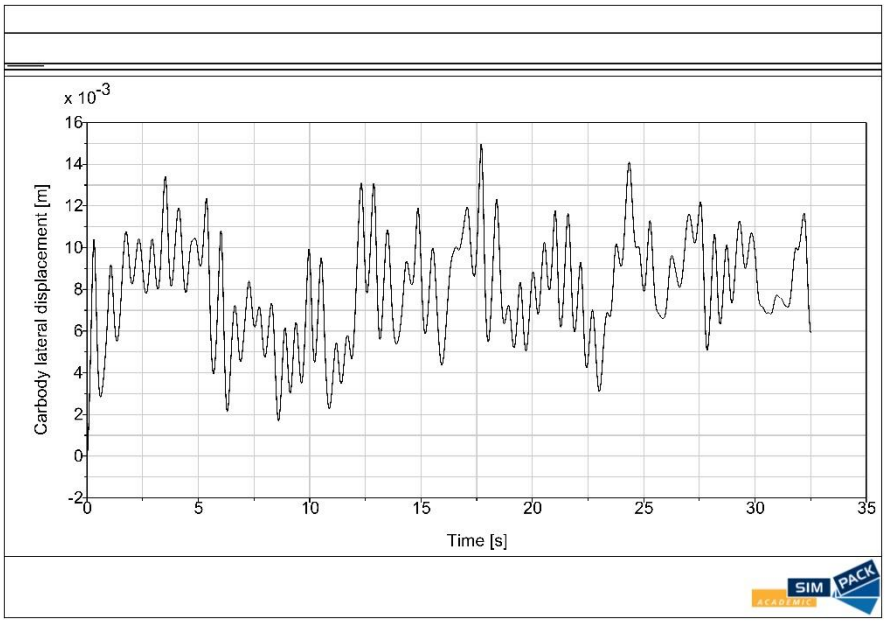


Figure A21. Lateral displacement of carbody with Max/min force fault in actuation system.

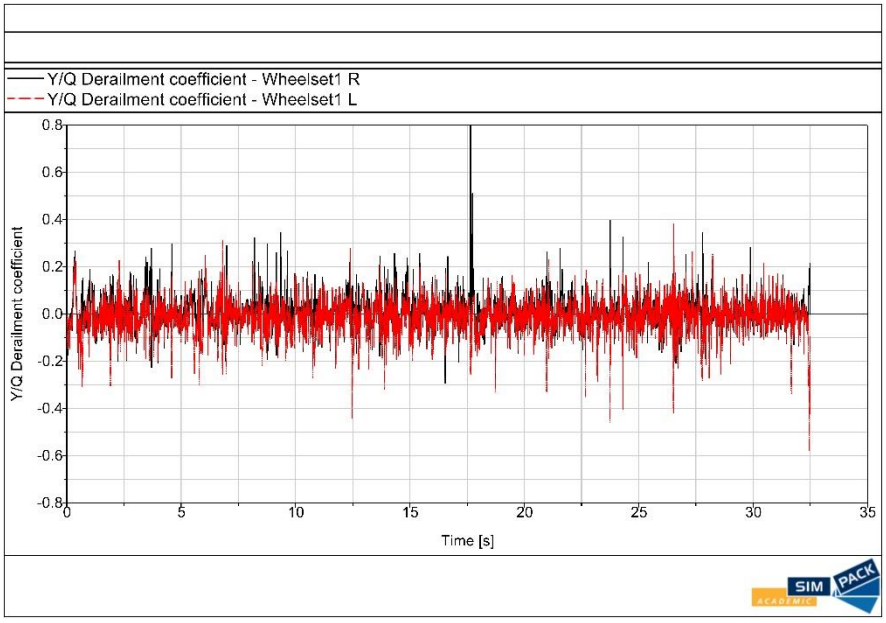


Figure A22. Derailment coefficient of leading wheelset with Max/min force fault in actuation system.

This section also includes the influences of the fault cases to the curving behaviours. It is found that the fault of the secondary lateral actuator does not constitute a direct impact to the curving

dynamics. It is not difficult to understand that the curve negotiation performance is mainly determined by the primary suspension. Figure A23 to Figure A25 demonstrate the dynamic behaviours for the actuator inversion fault during the negotiation of a small radius curve, which can be compared with the tangent track case mentioned above. In this curve negotiation case, the curve radius is 400 m and the cant is 100 mm. The speed is 80 km/h representing a cant deficiency situation. The actuator fault is applied on the leading actuator as well. In Figure A23, it can be seen that the oscillations of wheel/rail forces for the same axle are asymmetric, which is due to the lateral motion of the wheelset is confined in a small distance during the curve negation. This situation is also reflected in the derailment coefficient as shown in Figure A24. Both the derailment coefficient and the wheel/rail lateral force exceeds the limit values in EN 14363. Figure A25 represents the lateral displacement of the carbody. From the simulation results, it is found that the fault case of the secondary lateral actuator can be investigated independently without the redundant emphasises on various operational conditions.

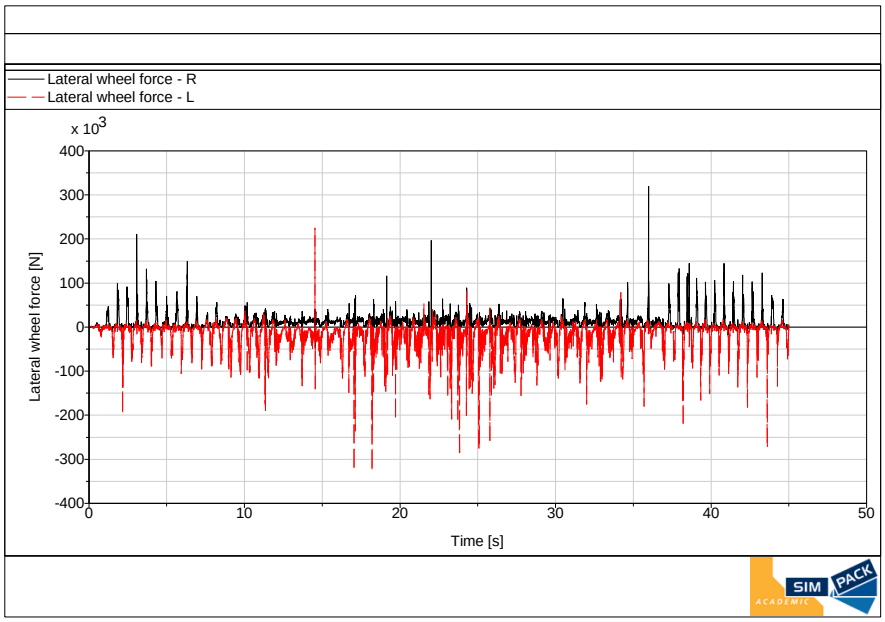


Figure A23. Lateral wheel/rail forces of the leading wheelset with inversion fault in actuation system.

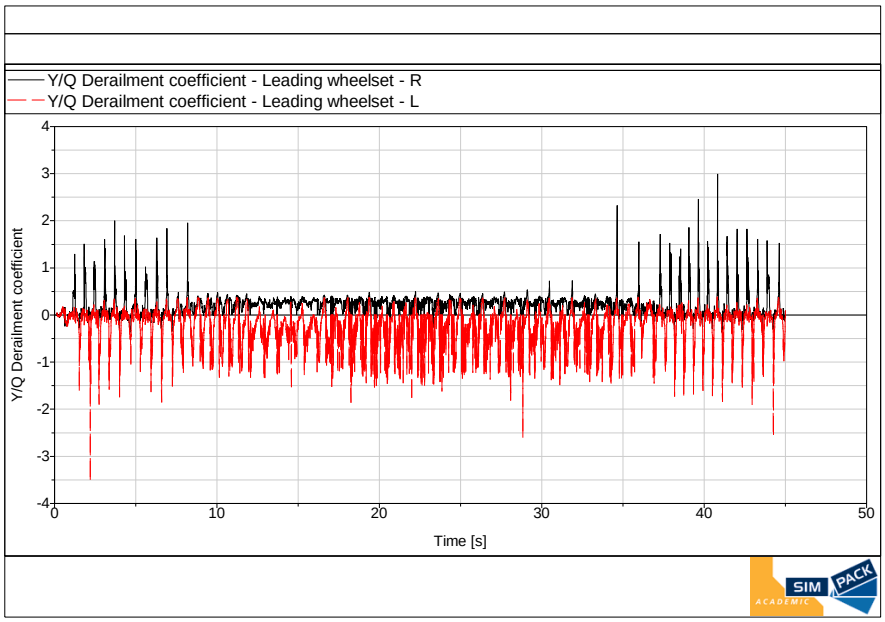


Figure A24. Derailment coefficient of the leading wheelset with inversion fault in actuation system.

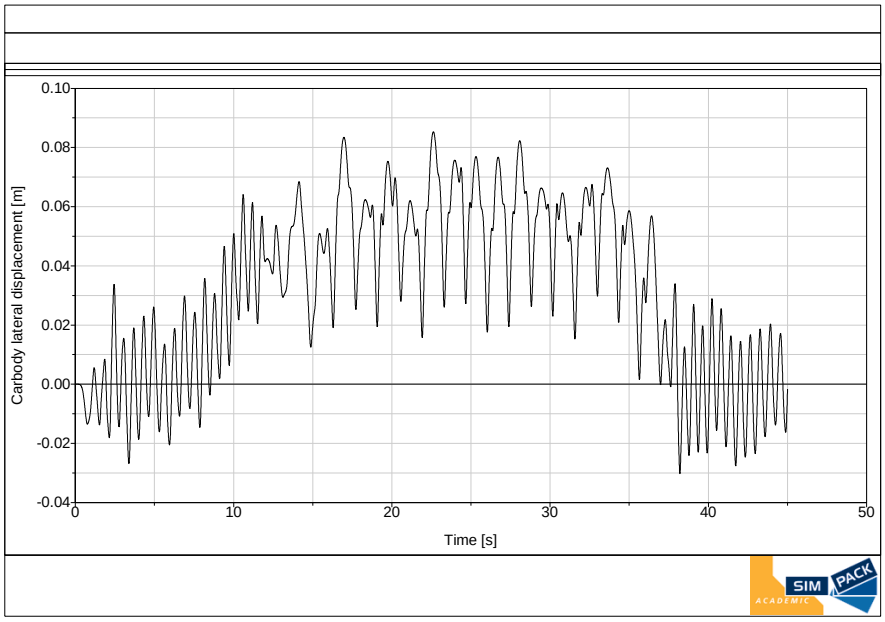


Figure A25. Lateral displacement of carbody with inversion fault in actuation system.

Summary of analysis

From the simulation results mentioned above, it is obvious that the actuator inversion fault should be distinguished from other faults in GASC analysis. It is not difficult to understand that the inversion fault can function as a 'positive' feedback control system and amplify the vehicle motion. The inversion fault does not only lead to the exceptional high-level vibration on the carbody, but more

importantly also cause serious safety problems including high derailment coefficients and large wheel/rail forces. The cause of this type of fault is more likely to attribute to the wrong installation of the actuation system, especially during the maintenance procedures. This issue will be in the focus of the GASC guideline. The rest of the faults contribute to the degradation of the passenger comfort, however, they may not lead to an obvious safety issue for the operation. These types of faults are not very critical for the reliability, because the operational safety could still be guaranteed. Since the fault in the actuator could be detected due to the comfort degradation perceived by the passengers, the decision-making and mitigation procedures can be implemented on the condition of enough safety margins.

Contract No. 777564

8.8 EXAMPLE: GENERIC APPLICATION SAFETY CASE FOR ACTIVE PRIMARY SUSPENSION WITH ELECTRO-HYDRAULIC ACTUATORS (EHAS)

Run2Rail T3.3: Authorisation Strategy

This is a draft document for discussion.

This document contains colour-coded text. The system of colour-coding is:

Orange italic text: This is guidance material for people completing this safety case template. Orange text describes the purpose of each section of the report. It is intended that orange text should be deleted by the safety case author.

Italic green text: This provides information on the content that should be provided in each section, sometimes simple examples are provide to clarify the nature of the content that is required. It is intended that italic green text is replaced by the correct content by the safety case author.

Black text: This is boilerplate text that will be needed in the final safety case. It is intended that black text be kept *as-is* in the safety case document.

Blue text: This provides exemplar context to illustrate the guidelines.

Red text: This is discussion text intended for the T3.3 project team during review of this document. Red text will not be included in the released version of this document.

Example: Generic Application Safety Case for Active Primary Suspension with Electro-hydraulic Actuators (EHAs)

Contents

Introduction

Background: purpose and scope

This document is an example of a Generic Application Safety Case (GASC) that provides evidence that an active primary suspension using electro-hydraulic actuators (EHAs) is safe.

Summary description of active suspension application

The active primary suspension considered in this document is aimed at providing the bogie with active steering capability, i.e. to actuate a steering angle of the wheelsets with respect to the bogie frame, so that the wheelset can take a nearly radial attitude in a curve, reducing unwanted creep forces and the related wear and damage effects. The active suspension is composed by two EHAs per wheelset. Each EHA is mounted in longitudinal direction between the bogie frame and one axle box of the wheelset. The two EHAs connected to the same wheelset are operated in displacement control to provide a relative displacement of the axle box relative to the bogie frame in longitudinal direction. The reference displacement for the two EHAs is equal in magnitude and has opposite direction, so that a yaw rotation of the wheelset with respect to the bogie frame is realised. The amount of this rotation is different for the leading and trailing wheelsets in the bogie, and is defined based on the yaw rate of the bogie measured by a gyroscope sensor and on the vehicle speed signal coming from the TCMS.

Brief description of safety approach

This document makes reference to the (example) GPSC for an electro-hydraulic actuator.

Figure 1 illustrates how in general the different safety cases may combine to provide the safety assurance and is also highlighting the relationship for this specific application of an active primary suspension system using EHAs.

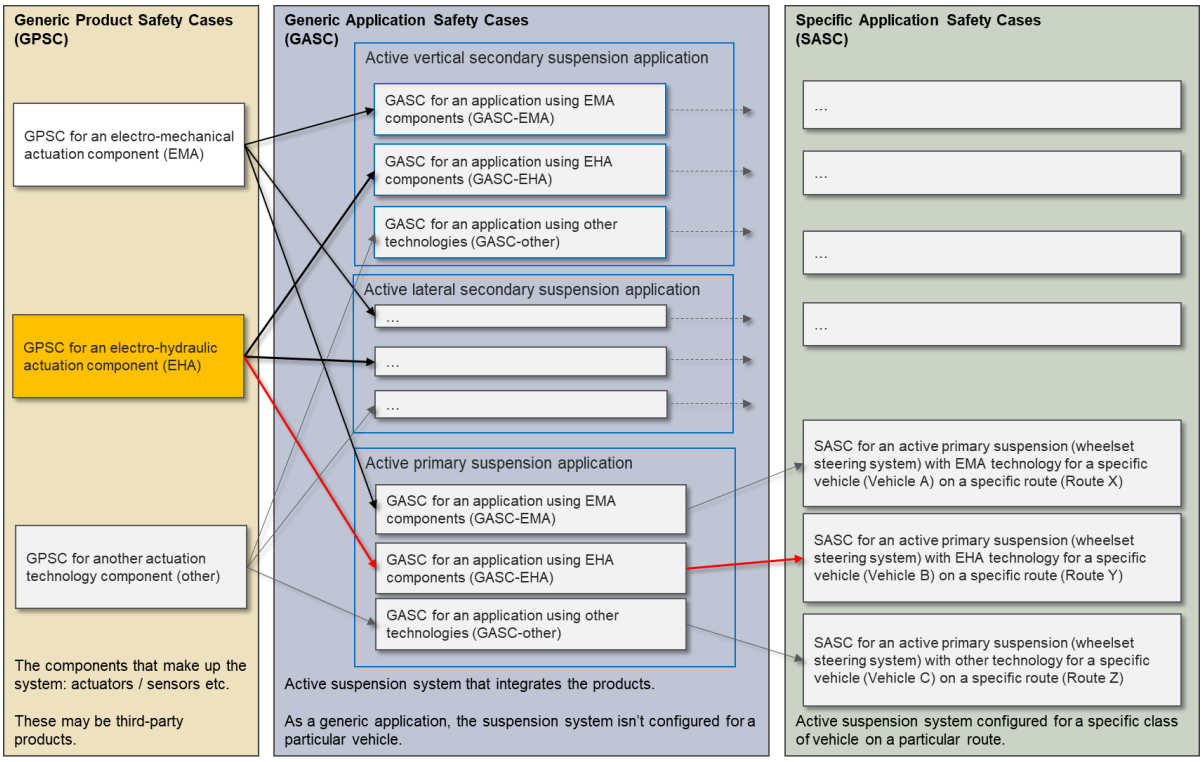


Figure 1 Relationship between Safety Case documents

This GASC focusses on the essential functionality of the active primary suspension utilising EHAs, although it might also rely upon other Generic Product Safety Cases (GPSCs) that deal with additional technologies to be incorporated, e.g. a track database system to provide "preview" information for the active control system, in this particular application this function is not used. This safety case identifies reasonably foreseeable safety hazards associated with the operation and maintenance of the generic application and describes the controls required to reduce the risk to an acceptable level. This safety case also shows that appropriate processes were applied in the design, development, testing and implementation of the system within the scope of a quality and safety management system.

Safety assurance strategy and method

The strategy for providing safety assurance is consistent with the approach described in the European Common Safety Method regulations [1]. *Figure 2* is reproduced from European legislation and shows the overall process for providing safety assurance for railway systems. The approach provides for three different methods of demonstrating risk acceptability, *viz*:

- codes of practice;
- similar reference system(s); and
- explicit risk estimation.

This GASC is based upon the third option, explicit risk estimation, but still involving codes of practice, in particular EN14363 [2]. Evidence will be provided that no combination of the EHA fault modes (as set out in the EHA GPSC) will create an unsafe running condition.

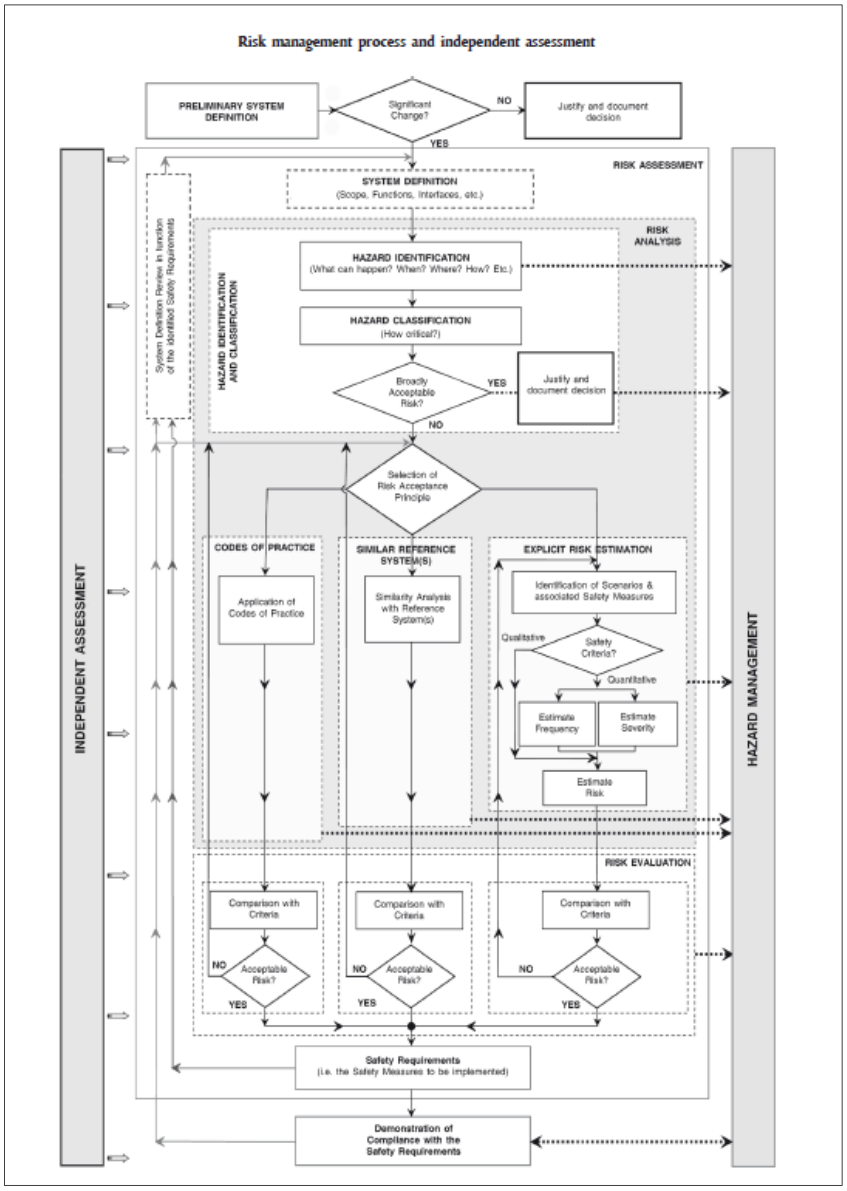


Figure 2 Overall approach to providing safety assurance shown in European Union [1]

The detailed demonstration of safety compliance within this overall strategy will be achieved through compliance with the European standard for demonstrating reliability, availability, maintainability, and safety for railway applications [3]. This standard requires a safety case to be developed that comprises:

- system description
- Quality Management Report (QMR);
- Safety Management Report (SMR); and
- Technical Safety Report (TSR).

This information is provided in the following sections.

System Description

Detailed active suspension description

The system description is shown in *Figure 3*. It utilises two electro-hydraulic actuators (EHAs) per wheelset (therefore a total of four EHAs per bogie), one on each side of the bogie. The actuators are mounted in longitudinal direction between the bogie frame and one axle box of the wheelset. Active control is achieved by measuring the bogie frame yaw rate at each bogie and processing these signals together with vehicle speed available from the TCMS to define a desired steering angle of each wheelset relative to the bogie frame. The angle is then actuated using as the reference displacement for the two actuators mounted on the two sides of the same wheelset opposite displacements having appropriate amplitude.

The objective of the active suspension is to reduce wear and RCF damage through the reduction of creep forces generated by the bogie in a curve, whilst ensuring running safety.

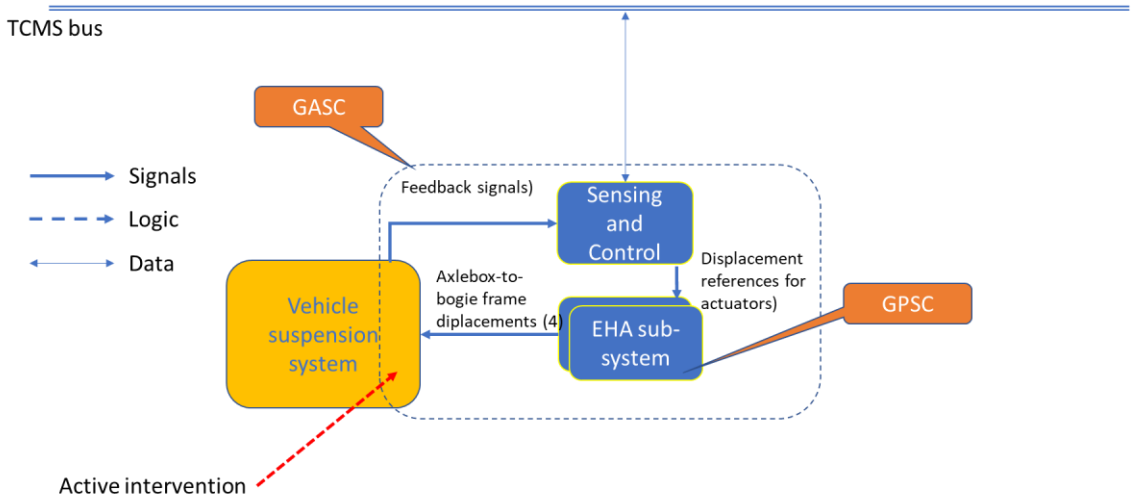


*Figure 3 Overall system diagram for active **primary** suspension*

Control functionality and diagram

Controller description.

The active steering system is realised by EHAs mounted in longitudinal direction between the bogie side frames and two axle boxes of each wheelset. The EHAs realising the active suspension are not redundant, however as each actuator provides about half of wheelset yaw, some functionality will remain if one actuator fails. Additionally, there is a passive primary suspension in parallel to the actuators, as shown in *Figure 4*.

The EHAs realise a longitudinal movement of the axle-boxes, producing a steering angle between the wheelsets and the bogie frame. The amount of the steering angle is defined based on the local curvature of the track according to the following expression:

$$\Delta \mathrm{L} = \frac{d}{R} \cdot a$$

where d represents the half wheelbase; a is the semi-gauge of left and right actuators and 1/R is the track curvature. Track curvature can be either estimated from sensors installed on the vehicle (e.g. one or more gyroscopes installed on some of the bogies) or can be obtained from a database of track curvature based on the position of the vehicle on the track obtained from a geo-referentiation system. In this document, the method used for curvature estimation is not considered as it depends on the specific application/implementation of the active primary suspension and instead the actual curvature value is used in the simulations, neglecting any estimation error. The examination of the effects on safety of errors in the curvature is mainly in the scope of a Specific Application Safety Case, depending on the actual implementation of curvature estimation in the considered application. In this GASC however, an inversion error is considered (see Section 5 and Appendix 1 of this document) as an extreme case in which a wrong sign of the curvature is obtained due to a fault in a sensor or in the control system, resulting in the inversion of the steering command with respect to the correct one.

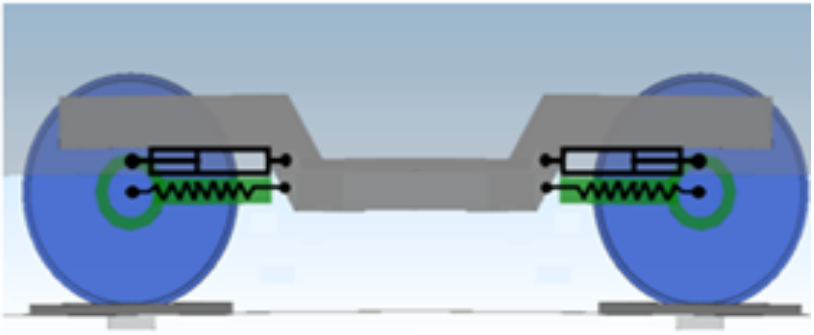


Figure 4 – Schematic side view of the bogie showing the arrangement of the active primary suspension with EHAs in parallel to a passive suspension

Quality Management Report

The Quality Management Report (QMR) provides information on the management and assurance procedures that were in place to achieve and demonstrate quality of the product. Information in the QMR is typically the same for all systems developed within the same organisation. Guidance on appropriate content for the QMR has been provide in the GASC template and has not been repeated in this document.

Quality Management System and Certification

Refer to GASC template for guidance regarding what is required

Organisational Structure

Refer to GASC template for guidance regarding what is required

Quality processes and assurance of processes

Refer to GASC template for guidance regarding what is required

Safety Management Report

This section describes the safety management techniques that were employed during the design, and where applicable development, of the generic product. This section should refer to the safety plan that was used for design and development activities.

Overall safety approach

This Safety Management Report provides a systematic description of the safety management techniques that were followed to demonstrate that the residual risk associated with the generic application is acceptable. The results of the analysis techniques are provided in the Technical Safety Report in Section 5.

The safety management approach includes the identification of fault modes that can occur in the active primary suspension with EHAs, and then an assessment their effect upon the system. The safety plan involves a hierarchical assessment approach adopted as part of the design and development process. Note that, as observed earlier, the effect of each fault mode upon safety risk depends upon the particular nature of the application and the manner in which the EHAs are to be used.

General safety (environment, electrical, maintenance, etc.)

(These aspects are addressed by the GPSC for an EHA.)

Functional safety

The individual EHA fault modes are assessed firstly using dynamic simulation based upon a well-established Multi-Body Software against the requirements of EN14363 and other relevant codes. This approach identifies the fault modes that may cause unsafe conditions and which need some mitigating action.

Fault modes which simulation has shown not to cause an unsafe condition are assessed by static/depot testing during initial commissioning in order to verify that the fault mode effect results from static tests are consistent with the simulation results. Track testing is used to validate the mitigation measures used to ensure the safety of fault modes that simulation has shown might otherwise be unsafe. Similarly, additional track tests may be specified where static/depot testing has not proved the safety of other EHA fault modes.

V-lifecycle diagram

Figure 5 shows the development of the active primary suspension system.

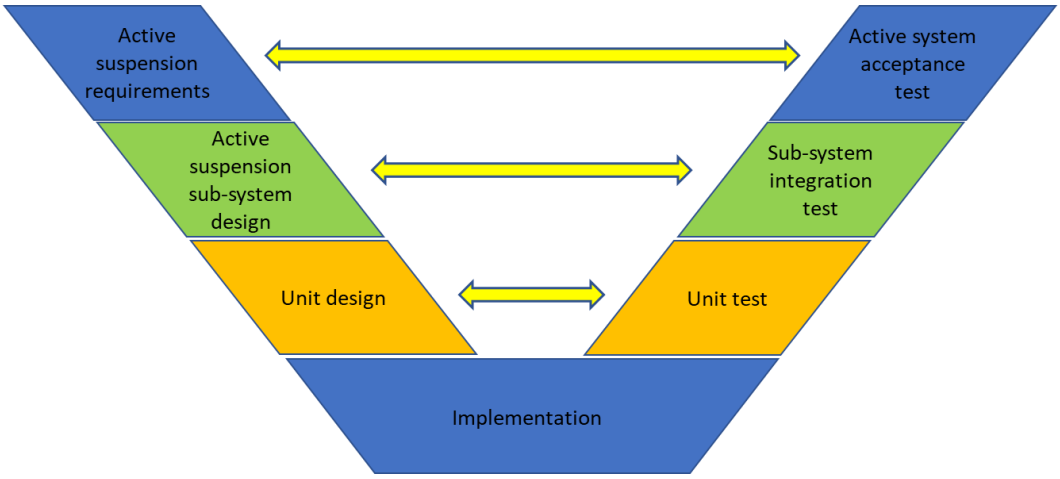


Figure 5 V diagram for active suspension system

Testing requirements

[A full GASC would describe in detail the overall approach involving simulation, laboratory (static) testing and track testing.]

Vehicle testing strategy

[A comprehensive statement setting out the track testing strategy should be added in a full GASC.]

Technical Safety Report

This Technical Safety Report provides the technical evidence that demonstrates correct application of the safety assurance techniques described in the SMR and that the residual safety risk of the system is acceptably low.

Review of Safety-Related documentation

For each document identify the author, checker and approver. Refer to the QMR to demonstrate that the staff have the competence necessary to perform their roles.

Analysis of fault mode effects

Provide a list of the safety analysis techniques described in the SMR. For each technique, provide the technical results. For example if an FMEA is stipulated in the SMR, then provide details of the FMEA, details of staff who were involved together with references to the QMR that describes staff expertise. Provide the results of the FMEA.

Initial filtering of fault modes is carried out via simulation to determine any that might affect upon safe operation. The model provided within the GPSC has been used in co-simulation with a Multi-Body Systems (MBS) dynamic model of the vehicle.

The hazard log shown in *Table 1* presents the safety hazards identified during the safety analysis based upon both the actuator model from the EHA GPSC and a detailed vehicle model in an MBS simulation package.

Table 1 Hazard list (AOA: Angle of Attack; WN: Wear Number)

Hazard ID	Hazard name (EMA fault mode)	Status	Other responsible party	Risk	Comments	Reference to other hazards
H001a	Zero force / free EHA in all corners of front bogie	Closed		None	Increase of AOA and WN	
H001b	Zero force / free EHA in leading outer corner of front bogie	Closed		None	Slight increase of AOA and WN	
H001c	Zero force / free EHA in leading inner corner of front bogie	Closed		None	Slight increase of AOA and WN	
H001d	Zero force / free EHA in trailing outer corner of front bogie	Closed		None	Slight increase of AOA and WN	
H001e	Zero force / free EHA in trailing inner corner of front bogie	Closed		None	Slight increase of AOA and WN	
H002	Semi-active EHA in all corners of front bogie	Closed		None	Increased AOA and WN	
H003	Force excess in all corners of front bogie	Closed		None	Large increase of AOA and WN	
H004	Random force in all corners of front bogie	Closed		None	Large increase of AOA and WN	
H005	Steering inversion on front bogie	Closed		None	Large increase of AOA and WN	

For each hazard listed in *Table 1*, the following *Table 2* to *Table 9* provide full technical comments related to their effect upon vehicle safety.

Table 2 Hazard 001a description

Hazard ID	H001a
Hazard name	Zero force / free EHA in all corners of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Increased levels of the safety relevant track shift force and derailment quote.
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Low, the assessment quantities defined by EN14363 for safety, track shift force and derailment quote, remain below their thresholds. Degraded performance in terms of wheel wear and track damage
Frequency	Infrequent (5×10^{-5}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 3 Hazard 001b description

Hazard ID	H001b
Hazard name	Zero force / free EHA in leading outer corner of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Slightly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.
Frequency	Extremely rare (1×10^{-6}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 4 Hazard 001c description

Hazard ID	H001c
Hazard name	Zero force / free EHA in leading inner corner of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Slightly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.
Frequency	Extremely rare (1×10^{-6} per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 5 Hazard 001d description

Hazard ID	H001d
Hazard name	Zero force / free EHA in trailing outer corner of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Slightly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.
Frequency	Extremely rare (1×10^{-6}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 6 Hazard 001e description

Hazard ID	H001e
Hazard name	Zero force / free EHA in trailing inner corner of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Slightly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.
Frequency	Extremely rare (1×10^{-6}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 7 Hazard 002 description

Hazard ID	H002
Hazard name	Semi-active EHA in all corners of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Degraded performance of the vehicle in terms of wheel wear and damage to the track, increased guiding forces on wheelsets and derailment coefficient but the value of assessment quantities defined by EN14363 for safety still below their thresholds.
Frequency	Infrequent (5×10^{-5}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 8 Hazard 003 description

Hazard ID	H003
Hazard name	Maximum force in all corners of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Highly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Highly degraded performance of the vehicle in terms of wheel wear and damage to the track, increased guiding forces on wheelsets and derailment coefficient but the value of assessment quantities defined by EN14363 for safety still below their thresholds.
Frequency	Infrequent (3×10^{-5}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 9 Hazard 004 description

Hazard ID	H004
Hazard name	Random force in all corners of front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Highly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Highly degraded performance of the vehicle in terms of wheel wear and damage to the track, increased guiding forces on wheelsets and derailment coefficient but the value of assessment quantities defined by EN14363 for safety still below their thresholds.
Frequency	Infrequent (5×10^{-5}per hour probability)
Risk	Not assigned because of Severity
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Table 10 Hazard 005 description

Hazard ID	H005
Hazard name	Steering inversion on front bogie
Status	Closed
Hazard cause	Refer to GPSC (Table 2)
Hazard consequence	Highly increased AOA and WN (increased wear and damage to the track) but not unsafe
Hazard source	Identified in the GPSC (Table2), analysed by simulation as part of GASC safety process
Severity	Highly degraded performance of the vehicle in terms of wheel wear and damage to the track, increased guiding forces on wheelsets and derailment coefficient but the value of assessment quantities defined by EN14363 for safety still below their thresholds..
Frequency	Infrequent because potential causes of inversion should be eliminated during commissioning. Software correctness needs to be assured. (4×10^{-5}per hour probability)
Risk	Low
Safety requirements	Inspection and maintenance manual (ref) …
Justification of risk acceptance	Not required
Interface hazard	Maintainer – safety-related tests on mechanical assembly
Reference to further analysis	Appendix 1 provides results of dynamic analysis
Comments	None
Proof of hazard closure	*Evidence of closure of the hazard can be found in Appendix 1.*
Date added	*Not needed for example GASC, but would be needed for a real SC*
Date closed	*Not needed for example, but would be needed for a real SC*
Change log	*Not needed for example, but would be needed for a real SC*
Reference to other hazards	Not applicable

Summary of dynamic simulations (move this, or repeat for initial screening)

Results of the fault mode analysis using Simpack/Simulink co-simulation are given in Appendix 1. All fault modes have been tested, although always on the leading bogie only. The weak coupling between the two bogies through secondary suspensions means however that the results obtained on the front bogie can be directly extended to faults occurring in the trailing bogie.

It shall be noted that some of the results obtained depend on the primary suspension stiffness assumed in the MBS simulation and also on the assumption that the bogie is equipped with (passive) yaw dampers. For instance, in case of zero-force type fault, the presence of a relatively high primary stiffness in longitudinal direction prevents the wheelset from undergoing an excessive angle of attack at narrow curves, whilst the presence of yaw dampers ensures the stable running of the bogie even in presence of the fault. The relationship between the stiffness and damping properties of bogie suspensions and failure mode effects shall be further investigated as part of a Specific Application Safety Case for an active primary suspension using EHAs.

Overall, the simulation cases considered show that in all fault modes the safety-related assessment quantities envisaged by the EN14363 standard remain below their respective thresholds when a severe curving condition is considered for the vehicle (curve radius R=250m, non-compensated lateral acceleration 0.65 m/s^2). For some fault modes however, the angle of attack and wear number increase significantly compared to the healthy case, showing that the fault would produce increased wheel wear and wear / damage to the track.

Regarding the conclusion on running safety, it is worth mentioning here that the safety assessment is performed using a single record of the derailment coefficient and track shift force, whilst the verification envisaged by EN14363 is performed comparing a statistical maximum of the assessment quantities with the respective thresholds, the statistical maxima being obtained through a statistical processing of at least 25 records from a line test (or simulation). In a real safety assessment case, more simulations would be required considering e.g. different track irregularity profiles and vehicle speeds / cant deficiencies to simulate a line test and then the results of these simulations should be processed statistically to derive a statistical maximum of the assessment quantities to be compared with the thresholds. This complete process is not performed here for the sake of simplicity but should be undertaken as part of a Specific Application Safety Case (SASC). It is also recommended that in a SASC other running conditions (e.g. negotiation of switches, stability at maximum running speed) are considered for a complete assessment of running safety.

Mitigation measures

Because of the conclusion that no fault mode would lead to an unsafe running condition, no mitigation measure is envisaged here, apart from correct implementation of inspection and maintenance procedures for the active primary suspension.

(Static test results)

[Needed for a complete GASC]

(Track test results)

[Needed for a complete GASC]

Operation with External Influences

Refer to the guidance in the GPSC template for the information that should be included.

Safety-related Application Conditions & Assumptions

Refer to the guidance in the GPSC template for the information that should be included.

Other Outstanding Safety Issues

Refer to the guidance in the GPSC template for the information that should be included.

Conclusion

Provide a statement summarising the safety case and giving the safety argument to demonstrate that the evidence provided by, or referred to, in this safety case makes a complete and correct argument for safety of the product for use within an active suspension system under all reasonably foreseeable conditions. Provide signature of the single authority responsible for safety of the system, and the independent safety advisor.

This document refers to the Generic Application Safety Case for an active primary suspension with no redundancy realising the active steering of the wheelsets in a curve. The use of Electro-Hydraulic Actuators (EHAs) is envisaged, and therefore this document makes use of the Generic Product Safety Case for an EHA.

A total of 8 fault modes was considered in the analysis. Each one was simulated using a multi-body systems model of the vehicle and the results are summarised in *Table 2* to *Table 9* whilst a more detailed description of results is provided in Appendix 1. Based on this analysis, it is possible to conclude that in all fault modes the safety-related assessment quantities envisaged by the EN14363 standard remain below their respective thresholds when a severe curving condition is considered for the vehicle (curve radius R=250m, non-compensated lateral acceleration 0.65 m/s^2). For some fault modes however, the angle of attack and wear number increase significantly compared to the healthy case, showing that the fault would produce increased wheel wear and wear / damage to the track.

It is worth recalling that the safety assessment is performed using a single record of the derailment coefficient and track shift force, whilst the verification envisaged by EN14363 should be performed comparing a statistical maximum of the assessment quantities with the respective thresholds, the statistical maxima being obtained through a statistical processing of at least 25 records from a line test (or simulation).

This complete process is not performed here for the sake of simplicity but should be undertaken as part of a Specific Application Safety Case (SASC). It is also recommended that in a SASC other running conditions (e.g. negotiation of switches, stability at maximum running speed) are considered for a complete assessment of running safety.

References

European Standard EN 50126-1:1999; Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Basic requirements and generic process.

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.

European Union; 2013. Official Journal of the European Union L 121; Legislation Volume 56; 03 May 2013.

List other documents that are required to support the safety argument. It is likely that very many references will be needed to provide the full suite of evidence necessary for the TSR.

List any related safety cases, such as safety cases for subsystems or components that are required as a part of the generic application.

Appendices

Appendix 1 Detailed simulation analysis of Fault Cases

A multi-body systems (MBS) model of a railway vehicle with active steering system is utilized to investigate the consequence of the failure modes in Table 1 of this document. The dynamics parameters of the Run2Rail conventional bogie vehicle are adopted in this example. The track irregularity of British Railway 'Track110' is utilized in this simulation task. For the condition of the simulation, the bogie vehicle negotiates a curve with radius R=250 m and 150 mm cant at 73 km/h, corresponding to a non-compensated lateral acceleration of 0.65 m/s^2. This combination of poor track quality and for the curve radii high speed is assumed to be the most challenging one for the vehicle considered in this example. However, it is possible that in a real safety assessment case more running conditions will need to be considered.

Case H001a: Zero force / free EHA in all corners of front bogie

To simulate this fault, the forces generated by the actuators in the front bogie are all set to zero. It is recalled here that due to the low inertia of EHA actuators and to the relatively slow speed of actuation required for wheelset steering, the case of zero force and free actuator produce the same effect which is zero force at the end effector of the actuator. The effect of this fault is the complete loss of steering effect due to the lack of steering forces, so that the bogie behaves as a passive one.

Figure 6 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

Based results shown in the figure, it is observed that the assessment quantities defined by EN14363 for safety remain below their respective threshold values. The results in Figure 6 also show that in the faulty configuration the angle of attack and the wear number of the leading wheelset are significantly increased with respect to the normal case. This is due to the lack of steering action implied by the fault considered. In conclusion, hazard H001a implies a degraded performance of the vehicle in terms of wheel wear and damage to the track, but still meets the requirements for a safe ride.

Regarding the conclusion on running safety, it is worth mentioning here that the safety assessment is performed using a single record of the derailment coefficient and track shift force, whilst the verification envisaged by EN14363 is performed comparing a statistical maximum of the assessment quantities with the respective thresholds, the statistical maxima being obtained through a statistical processing of at least 25 records from a line test (or simulation). In a real safety assessment case, more simulations would be required considering e.g. different track irregularity profiles and vehicle speeds / cant deficiencies to simulate a line test and then the results of these simulations should be processed statistically to derive a statistical maximum of the assessment quantities to be compared with the thresholds. This complete process is not performed here for the sake of simplicity.

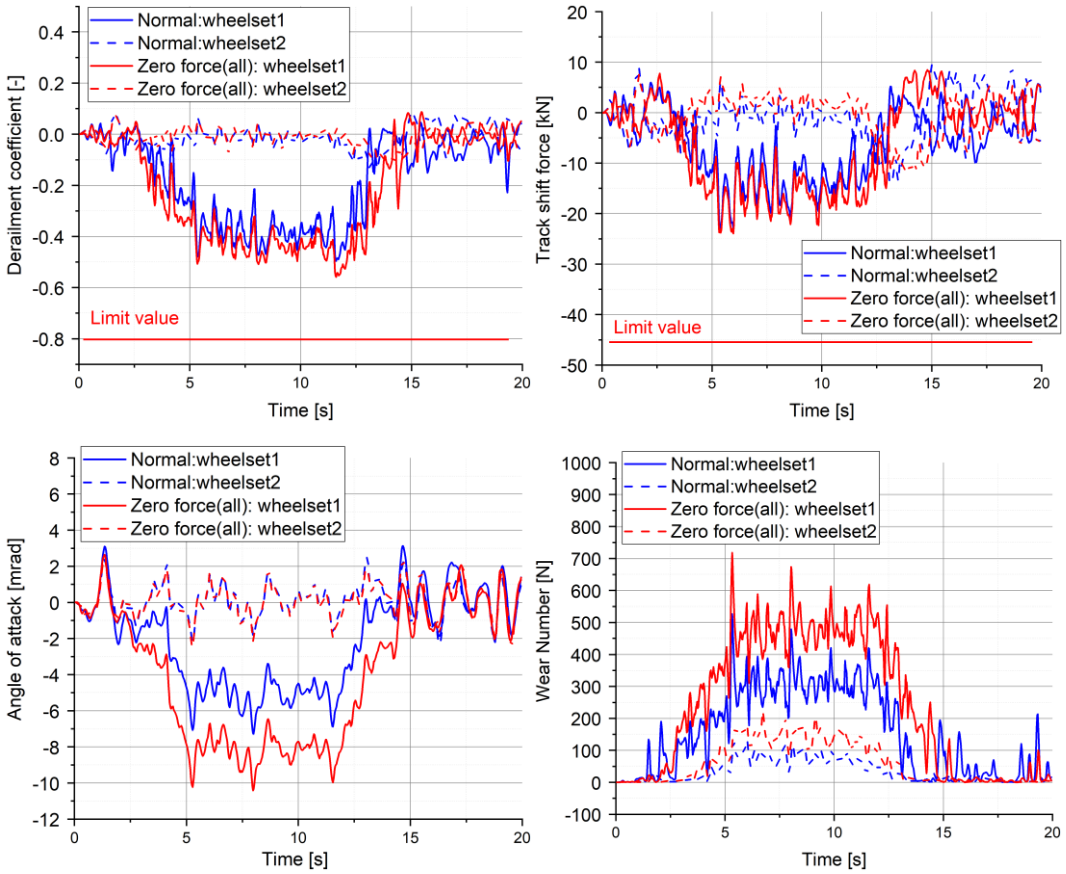


Figure 6: Case H001a: Zero force / free EHA in all corners of front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H001b: Zero force / free EHA in the leading outer corner of the front bogie

To simulate this fault, the force generated by the actuator in the leading outer corner of the front bogie is set to zero. The effect of this fault is a partial loss of steering effect due to the lack of steering force in one actuator, together with an un-symmetric application of steering on the two sides of the bogie and on the leading / trailing wheelsets.

Figure 7 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

Based results shown in the figure, it is observed that the fault considered here lead only to a minor increase of the safety-related assessment quantities and to a slight increase of the angle of attack and wear number. This is due to a degraded steering action caused by the fault considered. In conclusion, hazard H001b implies a slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.

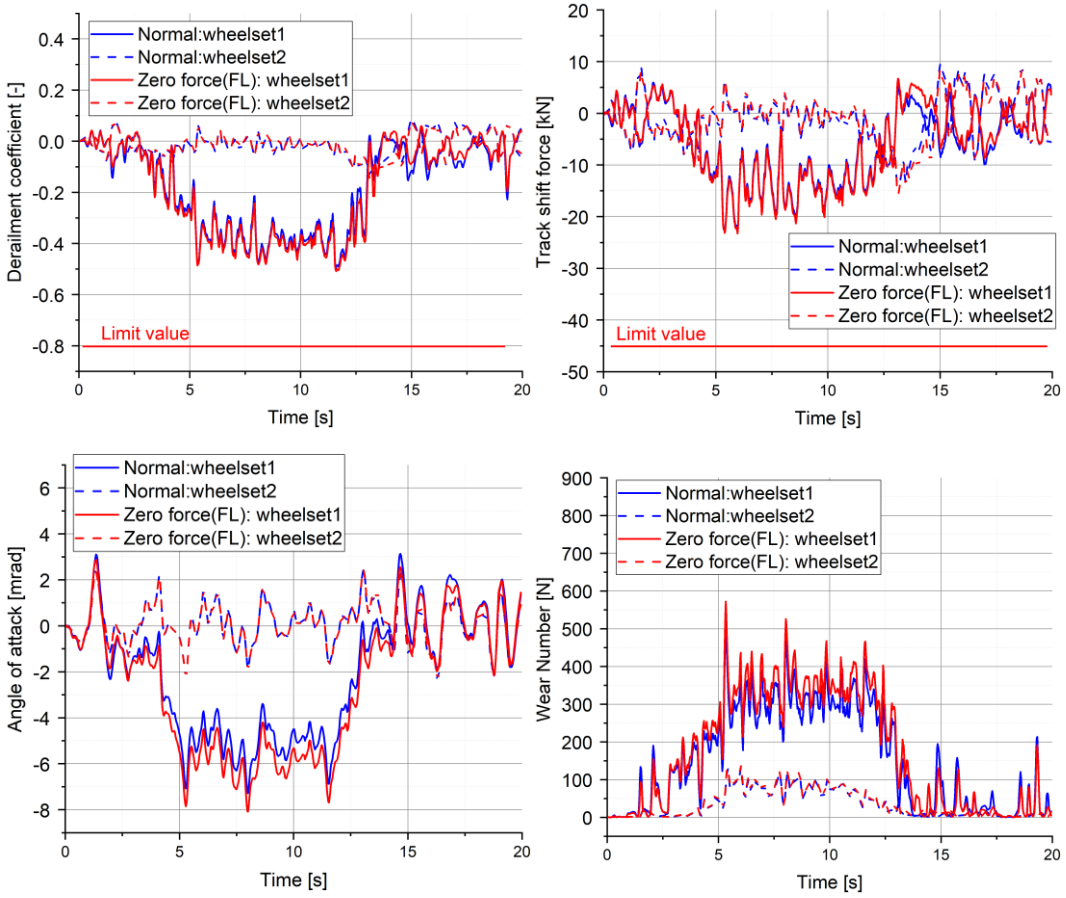


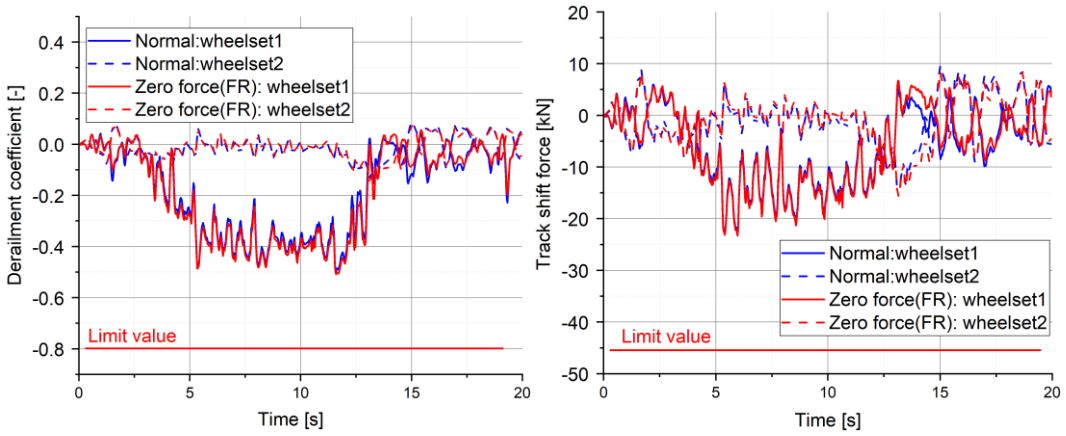
Figure 7: Case H001b: Zero force / free EHA in the leading outer corner of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H001c: Zero force / free EHA in the leading inner corner of the front bogie

To simulate this fault, the force generated by the actuator in the leading inner corner of the front bogie is set to zero. The effect of this fault is a partial loss of steering effect due to the lack of steering force in one actuator, together with an un-symmetric application of steering on the two sides of the bogie and on the leading / trailing wheelsets.

Figure 8 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

Based results shown in the figure, similar conclusions as in case H001b can be drawn: the fault considered causes a minor increase of the safety-related assessment quantities and a slight increase of the angle of attack and wear number. This is due to a degraded steering action caused by the fault considered. In conclusion, hazard H001c implies a slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.



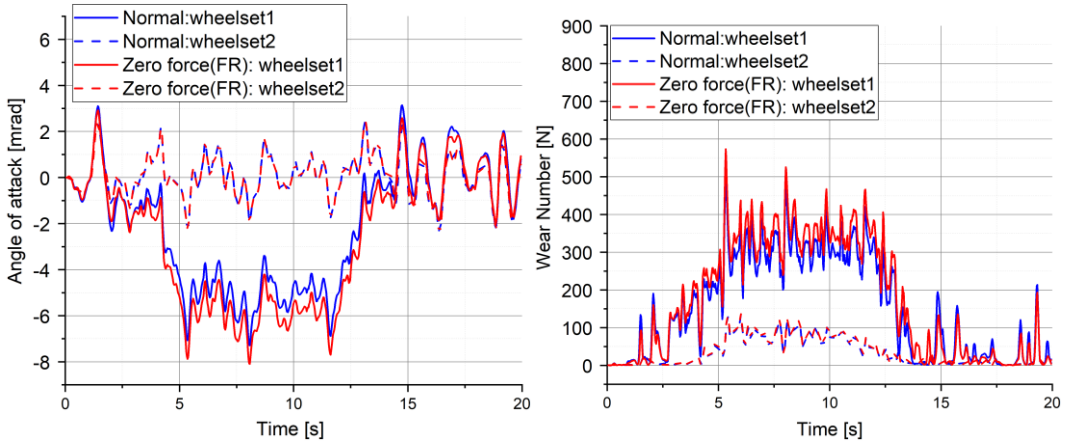


Figure 8: Case H001c: Zero force / free EHA in the leading inner corner of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H001d: Zero force / free EHA in the trailing outer corner of the front bogie

To simulate this fault, the force generated by the actuator in the trailing outer corner of the front bogie is set to zero. The effect of this fault is a partial loss of steering effect due to the lack of steering force in one actuator, together with an un-symmetric application of steering on the two sides of the bogie and on the leading / trailing wheelsets.

Figure 9 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

Based results shown in the figure, similar conclusions as in cases H001b and H001c can be drawn: the fault considered causes a minor increase of the safety-related assessment quantities and a slight increase of the angle of attack and wear number. This is due to a degraded steering action caused by the fault considered. In conclusion, hazard H001d implies a slightly degraded performance of the vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.

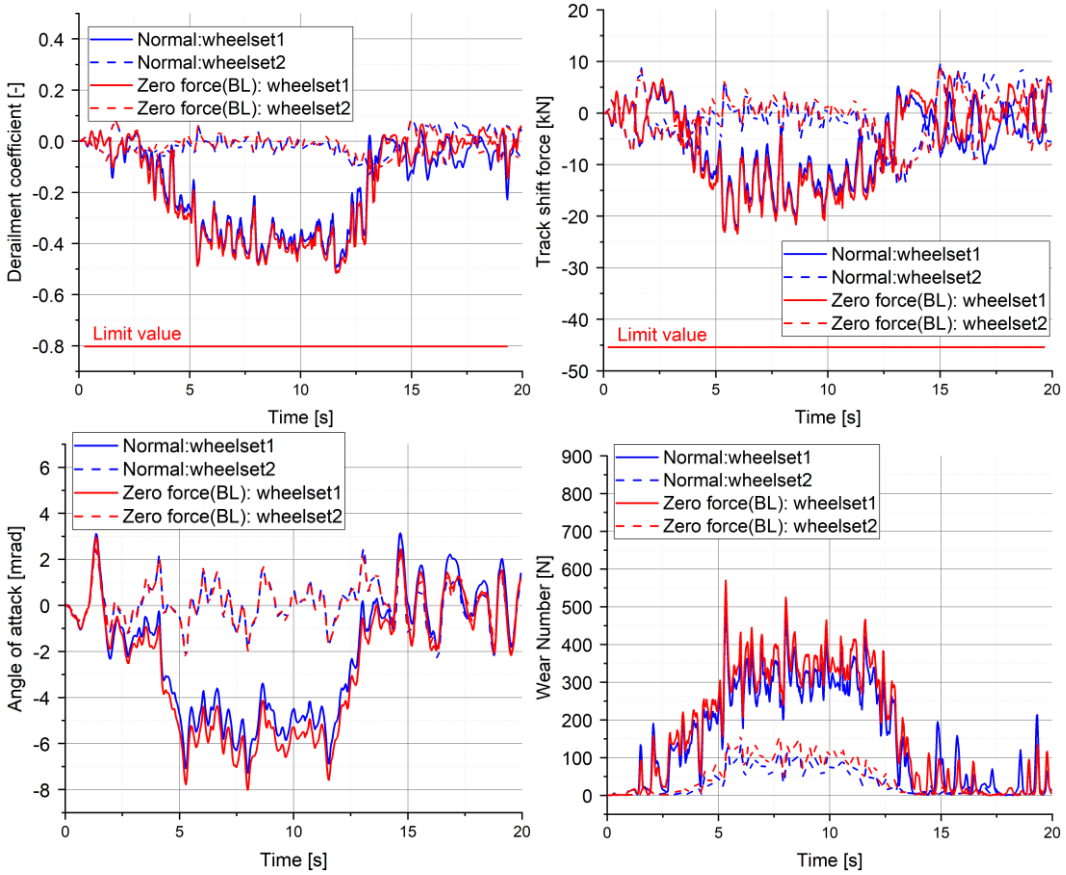


Figure 9: Case H001d: Zero force / free EHA in the trailing outer corner of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H001e: Zero force / free EHA in the trailing inner corner of the front bogie

To simulate this fault, the force generated by the actuator in the trailing inner corner of the front bogie is set to zero. The effect of this fault is a partial loss of steering effect due to the lack of steering force in one actuator, together with an un-symmetric application of steering on the two sides of the bogie and on the leading / trailing wheelsets.

Figure 10 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

Based results shown in the figure, similar conclusions as in cases H001b to H001d can be drawn: the fault considered causes a minor increase of the safety-related assessment quantities and a slight increase of the angle of attack and wear number. This is due to a degraded steering action caused by the fault considered. In conclusion, hazard H001e implies a slightly degraded performance of the

vehicle in terms of wheel wear and damage to the track, but has no significant impact on running safety.

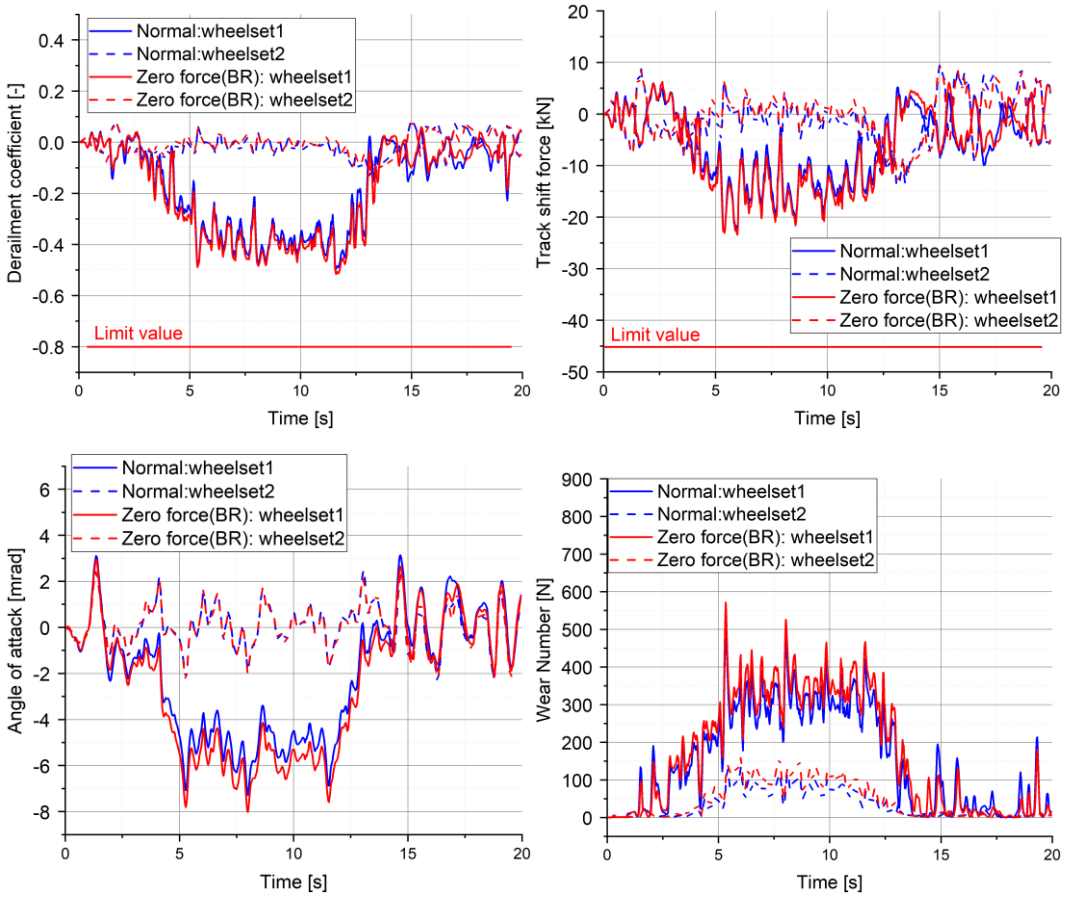


Figure 10: Case H001e: Zero force / free EHA in the trailing inner corner of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H002: Semi-active EHA in all corners of the front bogie

To simulate this fault, zero command is assumed for all actuators in the front bogie. This means the four actuators in the bogie are operated in passive mode and act as passive hydraulic devices, resulting in the loss of the steering effect.

Figure 11 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

The results in the figure show a significant increase of the derailment coefficient but this quantity still remains well below the threshold value of 0.8. The maximum value of the track shift force is only slightly increased compared to the healthy case. A quite large increase of the angle of attack and

wear number is also observed in this case compared to the healthy one, which is due to the lack of steering action from the steering system degraded to semi-active mode.

In conclusion, hazard H002 implies a degraded performance of the vehicle in terms of wheel wear and damage to the track, but still meets the requirements for a safe ride.

In the same way as for all other cases, in a real safety assessment case the conclusions regarding running safety shall be drawn based on a larger number of simulations and elaboration of a statistical maximum of the assessment quantities in line with the prescriptions of Standard EN 14363.

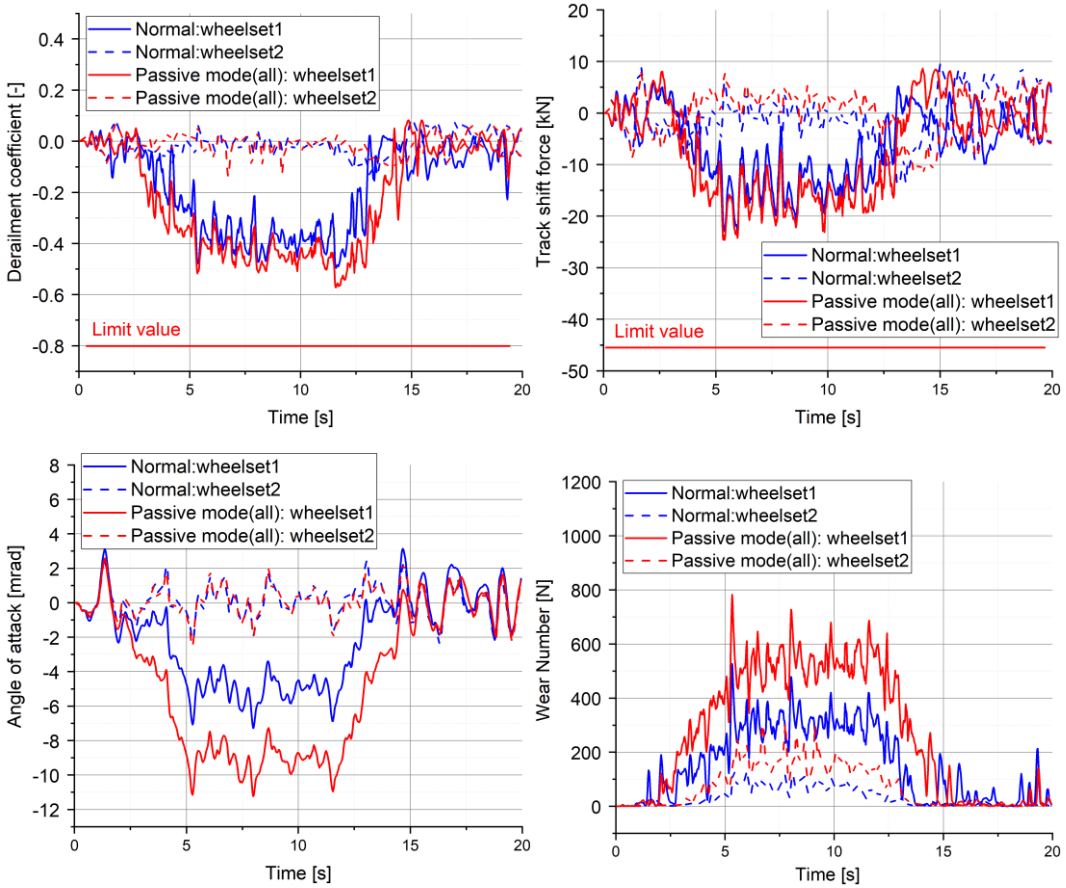


Figure 11: Case H002: Semi-active EHA in all corners of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H003: Force excess in all corners of the front bogie

In this case, the maximum force of 20 kN is applied on all actuators. The direction of the force is applied in a way that produces a worst case, i.e. the maximum force in each actuator points in the opposite direction than the one required to produce the correct steering of the wheelsets.

Figure 12 Case H003: Force excess in all corners of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Figure 12 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

The results in the figure show a significant increase of the derailment coefficient but this quantity still remains well below the threshold value of 0.8. The maximum value of the track shift force is only slightly increased compared to the healthy case. A large increase of the angle of attack and wear number is also observed in this case compared to the healthy one, which is due to inverse steering produced by the particularly unfavourable combination of forces applied on the actuators.

In conclusion, hazard H003 implies a highly degraded performance of the vehicle in terms of wheel wear and damage to the track, but still meets the requirements for a safe ride.

In the same way as for all other cases, in a real safety assessment case the conclusions regarding running safety shall be drawn based on a larger number of simulations and elaboration of a statistical maximum of the assessment quantities in line with the prescriptions of Standard EN 14363.

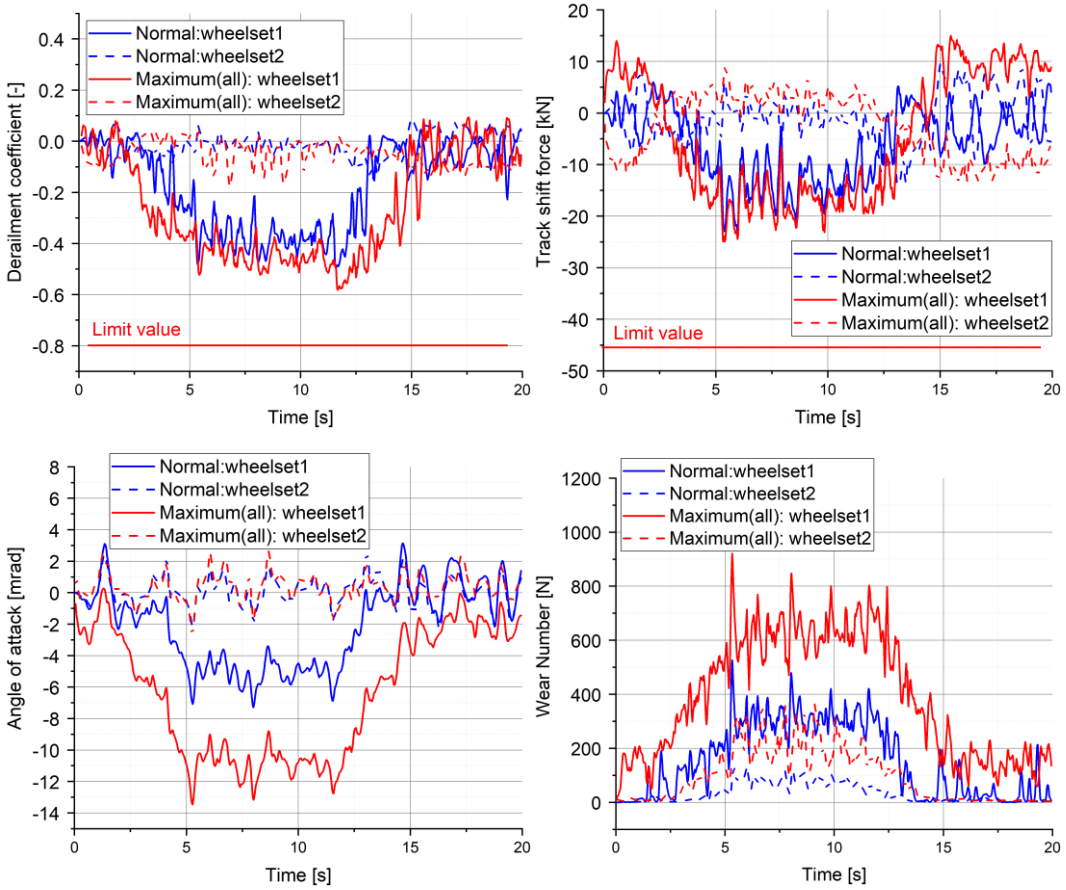


Figure 12 Case H003: Force excess in all corners of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H004: Random force in all corners of the front bogie

In this case, a random force with maximum value of 20 kN is applied on all actuators. The random signal representing the force applied by each actuator is obtained by generating a white random noise which is then passed through a low-pass filter with cut-off frequency 5 Hz to represent the pass band of the actuators. The random signal is finally normalised so that it takes values in the range +/- 20 kN. The direction of the force is depending on the sign of the random signal and therefore is changing randomly with time. The effect of this fault is that the direction and intensity of the forces generated by the actuators are not coherent with the desired steering action. As a result, large peaks of lateral wheel/rail contact force may arise on some wheels and the steering effect is lost.

Figure 13 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

The results in the figure show a significant increase of the derailment coefficient but this quantity still remains well below the threshold value of 0.8. The maximum value of the track shift force is only slightly increased compared to the healthy case. A large increase of the angle of attack and wear number is also observed in this case compared to the healthy one, which is due to the lack of steering effect.

In conclusion, hazard H004 implies a highly degraded performance of the vehicle in terms of wheel wear and damage to the track, but still meets the requirements for a safe ride.

In the same way as for all other cases, in a real safety assessment case the conclusions regarding running safety shall be drawn based on a larger number of simulations and elaboration of a statistical maximum of the assessment quantities in line with the prescriptions of Standard EN 14363. It is also recommended that other inputs are investigated to ensure that the used input represent an enough challenging case.

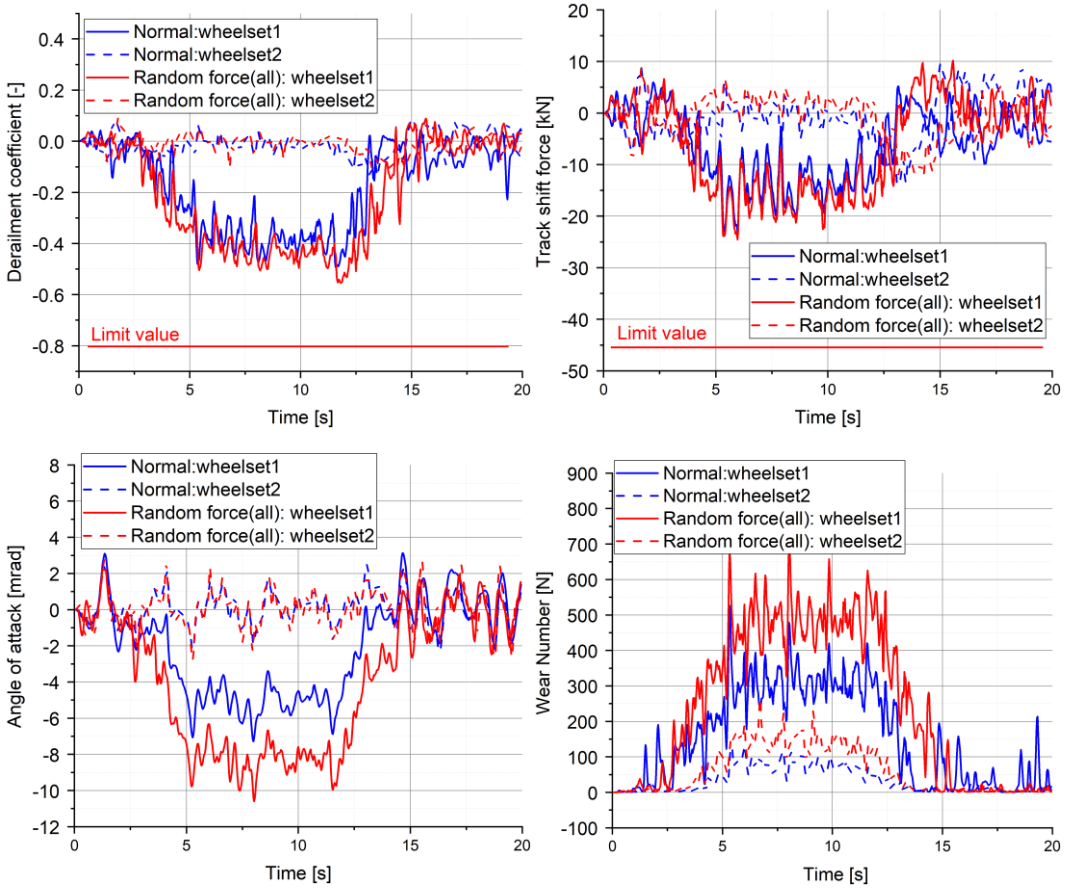


Figure 13: Case H004: Random force in all corners of the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Case H005: Steering inversion on the front bogie

In this case, steering inversion is simulated by deliberately changing the sign of the reference wheelset steering angle elaborated by the controller. As a result, the two wheelsets are steered by the correct amount (apart from the error in the feedback loop realised by the control system) but in a direction which is opposite to the correct one, resulting in an increased angle of attack, wear and large steady-state value of the lateral wheel/rail contact forces.

Figure 14 shows the time histories of the assessment quantities envisaged by the standard EN14363 for running safety (derailment coefficient and track shift force) for the two wheelsets of the front bogie and also the time history of the angle of attack and of the wear number (sum of outer and inner wheel) for the same two wheelsets. The lines in blue colour are for the normal condition of the steering system (no fault) whilst the red lines are for the considered faulty case. According to the prescriptions for data processing in EN 14363, all time histories shown in the figure are low-pass filtered with cut-off frequency 20Hz and then subjected to a sliding mean over a distance of 2 m travelled by the vehicle.

The results in the figure show a significant increase of the derailment coefficient but this quantity still remains well below the threshold value of 0.8. The maximum value of the track shift force is also increased compared to the healthy case, but remains well below the threshold. A large increase of the angle of attack and wear number is also observed in this case compared to the healthy one, which is due to the inversion of the steering action.

In conclusion, hazard H005 implies a highly degraded performance of the vehicle in terms of wheel wear and damage to the track, but still meets the requirements for a safe ride.

In the same way as for all other cases, in a real safety assessment case the conclusions regarding running safety shall be drawn based on a larger number of simulations and elaboration of a statistical maximum of the assessment quantities in line with the prescriptions of Standard EN 14363.

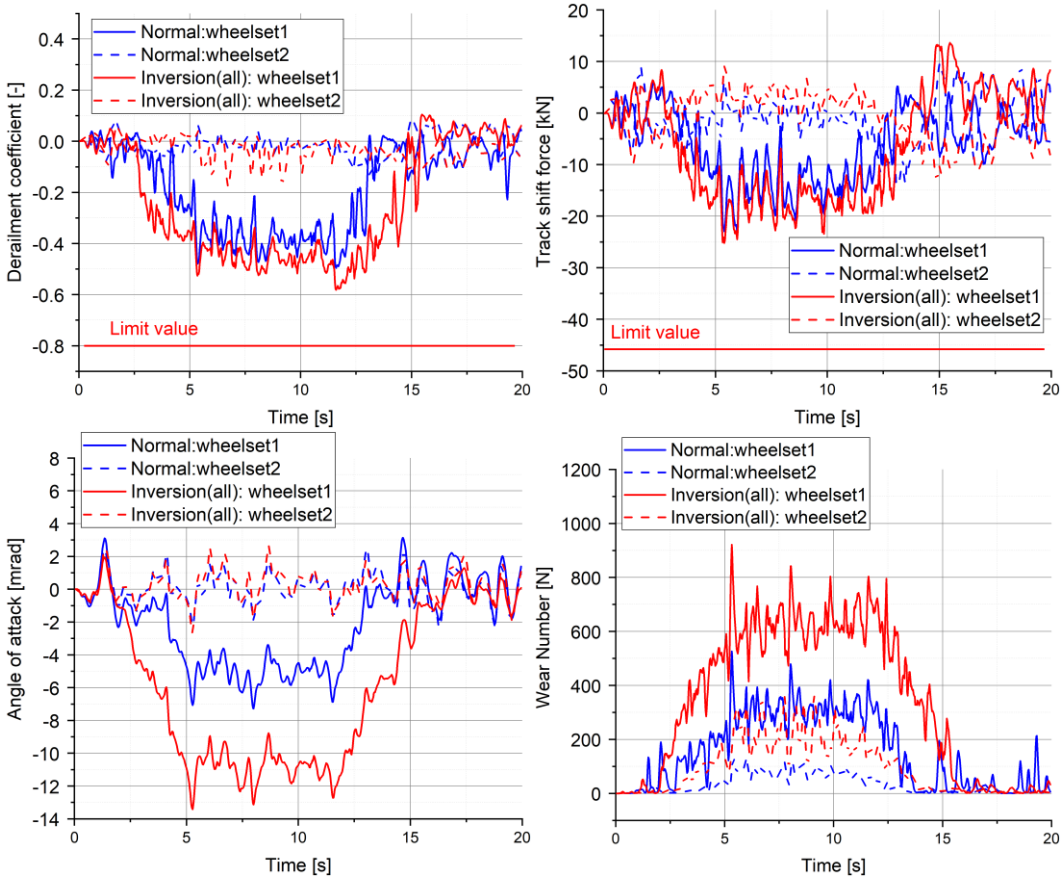


Figure 14 - Case H005: Steering inversion on the front bogie. Derailment coefficient (top left), Track shift force (Top right), Angle of attack (bottom left), wear number (bottom right).

Summary of analysis

Table 10 summarises the maximum values of the derailment coefficient, track shift forces, angle of attack and wear number obtained from multi-body systems simulation for the different fault modes considered. In the first line, the values for the active suspension in healthy state is reported as a term of comparison. In all fault modes, the derailment coefficient never exceeds 73% of the limit value 0,8 stated by standard EN14363. The maximum value of the filtered track shift forces obtained is approximately 55% of the threshold value foreseen by EN14363. Hence, there are significant safety margins for both derailment and track shift forces.

The analysis also shows that some fault modes, namely:

- zero force on all corners of the bogie;
- semi-active mode;
- force excess in all corners of the bogie;
- random force in all corners of the bogie;
- steering inversion;

produce a significant increase of the wheelsets' angle of attack and of the wear number so a significant degradation of vehicle performance in terms of wheel wear and wear / damage to the track is expected in case one of these faults occurs.

Table 10 – Summary of maximum values of the derailment coefficient, track shift forces, angle of attack and wear number for the healthy configuration of the vehicle and for all fault modes considered.

	Derailment Coefficient [-]	Track shift force [kN]	Angle of attack [mrad]	Wear number [N]
Normal case	0.497	23.019	7.282	526.102
Zero force (all corners)	0.559	23.934	10.420	717.605
Zero force (lead. outer)	0.508	23.262	8.087	571.759
Zero force (lead. inner)	0.509	23.324	8.090	573.029
Zero force (trail. outer)	0.516	23.482	8.001	569.494
Zero force (trail. inner)	0.516	23.445	8.012	571.154
Semi-active EHA in all corners	0.572	24.620	11.232	782.501
Force excess in all corners	0.582	24.949	13.427	921.293
Random force in all corners	0.555	24.539	10.603	701.728
Steering inversion	0.582	25.194	13.413	921.345