An Authorisation Framework for Actively-Controlled Running Gear

Roger GOODALL[2], Riccardo LICCIARDELLO[1], Rickard PERSSON[3], Peter HUGHES[2]

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

Abstract

A Shift2Rail funded research project called RUN2Rail has investigated a range of new technologies for railway rolling stock. The project included a task on the use of active suspensions, and one of the subtasks was to propose a strategy supporting the authorisation by safety authorities for highly innovative mechatronic vehicles to be placed on the market. The incorporation of electronics and control into suspension systems is still at an early stage, so this paper provides a framework for a practical and efficient authorisation strategy, primarily based upon existing European regulations and standards but in general applicable worldwide.

Keywords: safety, suspensions, control, electronics, active suspension

1. Introduction

Active or “mechatronic” suspensions have now been on the research and development agenda for railways for a number of decades. They employ sensors, electronics and actuators in addition to well-established passive suspension components such as springs, dampers and mechanical linkages, and they can offer performance improvements that are not possible with purely passive solutions [1]. However, apart from extensive use of active tilting solutions which can enable higher speed through curves, their widespread use remains elusive.

The design of an active suspension requires a combination of engineering skills, including the following:

- Control technology (actuators and sensors)
- Control systems theory
- Electronics and software
- Vehicle dynamics
- Systems engineering

For this reason, the process whereby a safety authority authorises a vehicle incorporating all the corresponding systems to be placed on the market (the authorisation process) and ultimately put in service by an operator needs to accommodate this disparate range of disciplines and their associated design approaches.

A key requirement is 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. Given the technical complexity of vehicles and methods, another key requirement is for safety assessors (e.g., in the EU, the Notified Bodies) and authorities to be able to rely on clear criteria, easily related to their current way of working, otherwise the uptake of the now fairly mature technology could be slower than envisaged. It is therefore essential to develop an approach that can provide the basis for future authorisation of advanced active suspension systems.

This paper presents a framework supporting the authorisation process (the authorisation framework)

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

2. Background

2.1 Regulation and Standardisation

The existing regulatory framework for vehicle authorisation in Europe revolves around the Interoperability Directive [2] and the Safety Directive [3]. The former defines the authorisation process and the Technical Specifications for Interoperability (TSIs) with which authorised systems (including vehicles) must comply, the latter introduces the Common Safety Methods (CSM) [4] which include the CSM for Risk Assessment (RA), used for example to assess the safe integration of systems (including those making up a vehicle). Moreover, any significant change to the railway system, such as the introduction of a new (and particularly novel) vehicle, must be assessed by the vehicle's operator according to the CSM RA to ensure that the associated risks are kept acceptable throughout the vehicle's lifetime.

The CSM RA allows the acceptability of risks to be demonstrated using one of the following methods:

- demonstration of compliance with relevant codes of practice;
- comparison with a reference system;
- an explicit risk-based approach; or
- a combination of the above approaches.

According to the current regulations, this method may be used to demonstrate the safe integration of components in a vehicle (e.g., active suspension components), but not to prove the safe integration of the vehicle in the network for which it is intended. For example, to prove the safe integration of components making up an active suspension system, it is possible to make a comparison with an existing reference system. In this way, a dedicated technical specification or standard is not needed. For vehicle-network integration this approach is not allowed. Only a rule-based approach (i.e., conformity with the TSI and with the mandatory standards referred to therein) is allowed. The key technical document for vehicle-network integration as regards running dynamic behaviour is thus the specific TSI, e.g., for locomotives and passenger rolling stock the TSI "Loc&Pas" [5].

The TSI sets specific requirements in its clause 4.2.3.4.2. It relies heavily on standard EN 14363 "Testing and Simulation for the acceptance of running characteristics of railway vehicles" [6]. It also contains "additional requirements when active systems are used", which essentially consist of demonstrating that the risk associated to failures in such systems, which have the credible potential to lead directly to fatalities, is controlled to an acceptable level. Of course the CSM RA can play a key role to this end.

Standard EN 14363 is founded on experimental tests (fixed site and on-track tests), and also acknowledges an increasing contribution from virtual methods (e.g. Multi-Body Simulation MBS). It requires several assessment quantities to lie within specified limits for authorisation to be granted. They are related to wheel-rail interaction forces (for example the ratio of lateral to vertical wheel loads Y/Q, the sum of the lateral wheelset forces) and accelerations (e.g., vertical and lateral accelerations in specified points of the running gear) to be assessed over lengths of the order of tens of kilometres of track with specified characteristics, considering their statistical variability to determine "quasi-worst-case values". Conformity with EN 14363 "closes out" the risk related to the "running dynamic behaviour" requirements of the TSI for vehicles with no active systems, and this is taken to ensure the acceptability of such risks as well as the safe integration of vehicle and network.

The standard, however, is still not tailored to new vehicles with active secondary and/or primary suspension components. For active secondary suspensions, on-track tests may have to be repeated, perhaps for every fault or combination of faults that might lead to an unsafe failure mode, leading to a high burden even if there is only one mode that needs to be tested. For active primary suspensions, the proliferation of test requirements could become even more burdensome. Furthermore, for active systems, there may be failure modes which are simply not safe to test on track, for example, a sudden wrong-side failure of software which could cause an immediate derailment. In such cases, on-track testing would not be helpful as the cause of the failure may not be related to the running of the train at that time.

In order for vehicles with active systems in the running gear to be authorised, two possibilities, to be used as alternatives or in combination, are:

- "EN 14363 route": the EN 14363 running safety limits are always complied with, even in the presence of faults (possible for example 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 failure mode and such systems have a relatively low performance;
- "TSI active systems route": it is acknowledged that the failure modes would cause EN 14363 running safety limits to be exceeded, and the assessment is focussed on demonstrating that they are "highly improbable", making the best possible use of virtual methods.

The latest version of the standard EN 14363 [6] would also support the second route, as it contains an opening for risk-based assessment in its clause 5.2.2 specifically dedicated to faults: *"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."*

Safe operation may be achieved by some form of redundancy, e.g. triplication, so that a fault in a single channel does not lead to an unsafe failure. Note that in this case, if one channel fails, mitigation may require reducing the speed or stopping, which raises the question of the reliability of operation[1].

Consistently with the above considerations, the proposed authorisation strategy adopts a risk-based approach founded on the series of standards EN 5012x, which are suggested by the European Union Agency for Railway in its guide [8] on possible tools supporting the CSM RA. EN50126, 50128 and 50129 deal with railway safety cases where electronics and software are a key part of the system, which therefore are very relevant to active suspension systems. These are focussed upon signalling applications, and are not usually an important part of the conventional running dynamics assessment process. EN50129 in particular supports the principle of establishing multiple related safety cases [9], stating that the following three different types of safety case can be considered:

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

Fig. 1 is a diagram from European Standard EN50126-2:2007 [10] showing how the various safety cases can be used together. Fig. 2 which follows later is a re-drawing of this diagram that is better focussed upon active suspensions.

[1] Operational reliability is not considered in this paper, but some thoughts are presented elsewhere [7]

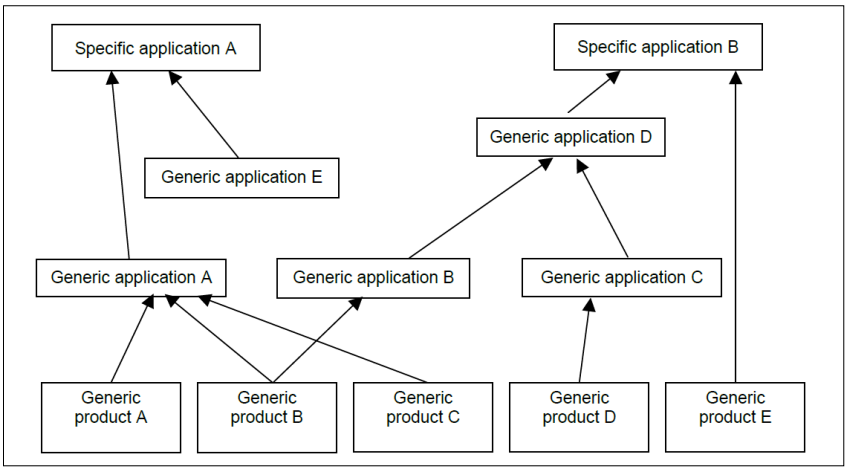

Figure 1: The combination of numerous safety cases for different specific applications (EN 50126-2:2007).

The authorisation framework develops GPSC, GASC, SASC for active suspension systems according to EN 5012x which include, in the safety case itself, assessment of conformity with EN 14363 as required.

2.2 Types of active suspension

From a number of discussions within the RUN2Rail project, three active suspension types have emerged that are expected to be distinct in terms of their safety authorisation implications:

Type 1 – Active Secondary Suspensions It is expected that most active secondary suspensions (including tilting) could be authorised using existing standards (principally EN 14363). Although faults in either vertical or lateral active secondary suspensions are likely to degrade ride quality, they can readily be designed so as not cause effects such as unsafe instability, excessive wheel loads or derailment. There may be implications for gauging, but generally existing methods should still be relevant.

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. The constraints associated with a mechanical back-up and/or limited force capability from the actuators may limit the performance of an active primary suspension. For example, a mechanical backup consisting of passive springs in parallel with the actuators may require impractically large higher-force actuators needed to overcome the spring reactions as well as to provide the necessary wheel or wheelset steering. Limited force capability may not achieve what is needed for the required performance in terms of steering angles.

Type 3 – Active Primary Suspensions with functional redundancy Since the reliability of a single "channel" of active control will not be sufficient, some form of functional redundancy is required to decrease the probability of unsafe operation in the event of faults within the active system. Of course, the existing standards for stability, derailment and wheel loads (EN 14363) would still be directly relevant, but compliance would not prove the safe integration of the vehicle within the network. An explicit risk-based authorisation methodology is needed to meet the specified integrity levels defined for the associated hazards.

2.3 Proposed authorisation framework

The RUN2Rail project decided to adopt the GPSC, GASC and SASC approach, and Fig. 2 presents a modular framework of Safety Case documents: this is a re-drawing of the EN50126 diagram in Fig. 1

with the wording made directly relevant to active suspensions of different types. This shows how a particular active suspension application may utilize a choice of actuation technology, also how a particular actuation technology may be applied to a variety of active suspension applications. The highlighted arrows and boxes show the possible relationship diagram for the ~~illustrative~~ lateral secondary suspension example employing Electro-Mechanical Actuation described in Sect 4. Other possibilities for using the EMA technology are also shown by the dash-dot lines.

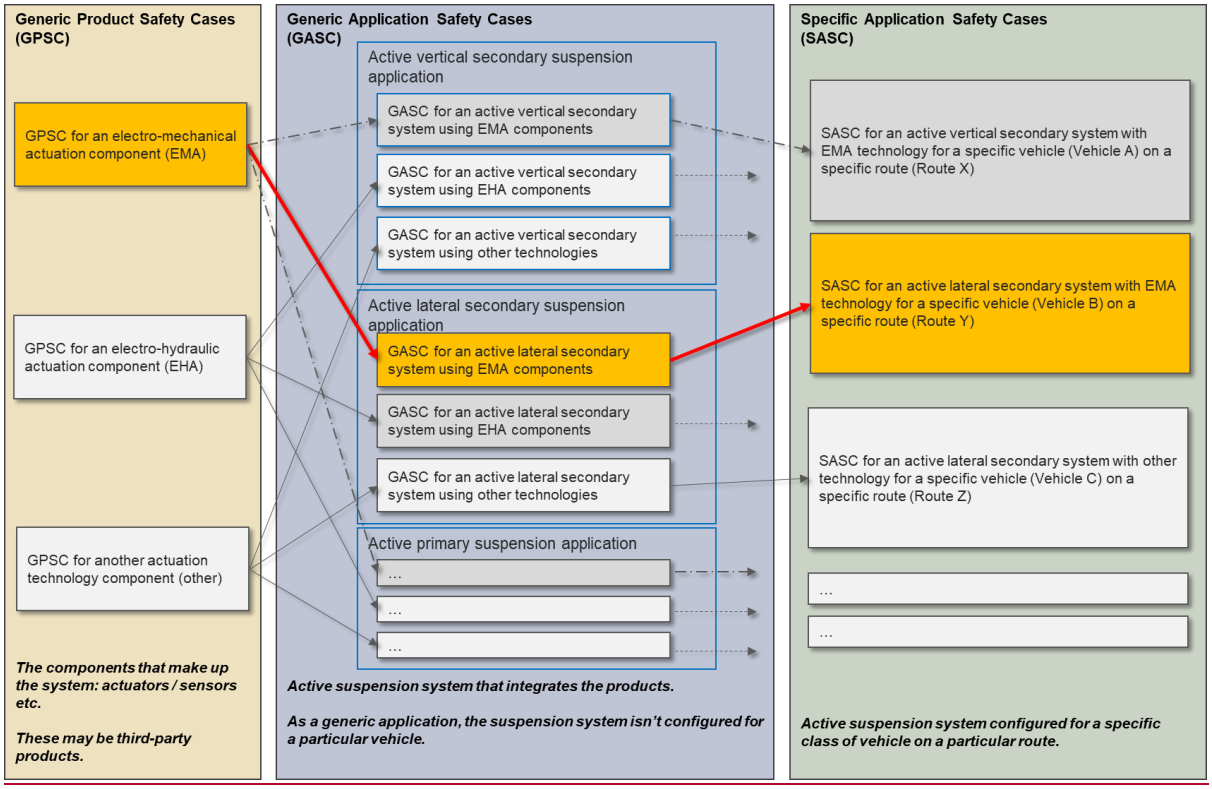

Figure 2: ~~Active suspension s~~Specific version of diagram from European Standard EN 50126-2:2007 for active suspensions~~.~~

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

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

Specific application safety cases (SASCs) are illustrated in the right-hand panel: these describe how a generic application is configured for and safely integrated with a specific vehicle with given network

characteristics. The SASC will show how the application conditions of the GASC have been met for a specific vehicle. As such, an SASC will normally contain a number of checklists showing that the application has been configured and installed correctly, for example an SASC will show that a specific installation of the application for a specific vehicle was fitted by a competent (named) fitter and show the licence details of the fitter. The SASC will also show that the process to fit and test the wiring was correctly followed and include the fitting and inspection checklists that were completed when the application was installed. To prove safe vehicle-network integration, the SASC will also investigate compliance with EN 14363 running safety limit values in the different fault states, whether it is always ensured (e.g. through mechanical backups) or whether exceedances may occur but are highly improbable.

3. Templates and guidelines

Three templates have been developed within the RUN2Rail project for the GPSC, GASC and SASC. These templates contain colour-coded text, where the system of colour-coding is 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 provided 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.

Each safety case has the section headings required by the CSM: Introduction, System Description, Quality Management Report, Safety Management Report (the safety process), Technical Safety Report (the safety analysis), Conclusion plus relevant references and appendices. The guidance provided by the orange, green and black text is different for the GPSC, GASC and SASC templates.

4. Illustrative example

This example is intended to suggest how a Generic Product Safety Case for an electro-mechanical actuation product (EMA) could be used for a variety of active suspension applications, and specifically discusses the Generic Application Safety Case for an active lateral secondary suspension. It does not claim to be complete, rather it contains some typical and/or indicative information in order to help illustrate some of the detail that would be provided within the authorisation framework.

4.1 The GPSC

4.1.1 EMA technology overview

The EMA actuation system in Fig 3 shows an input force demand (an electronic signal) and an output control force that would be applied to the vehicle dynamic system in order to provide “active intervention”.

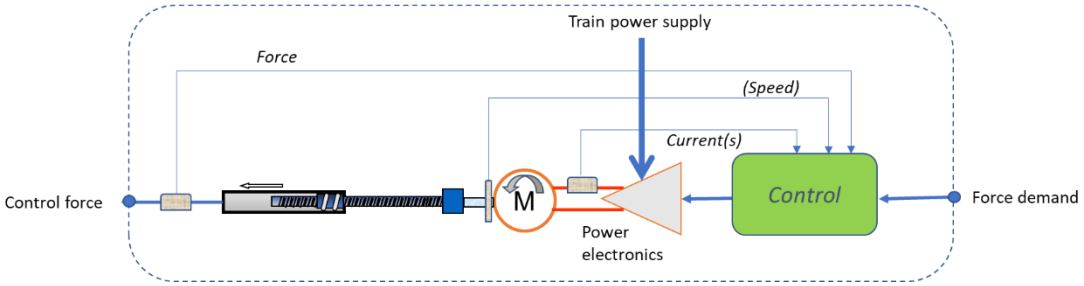

Figure 3: EMA diagram.

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

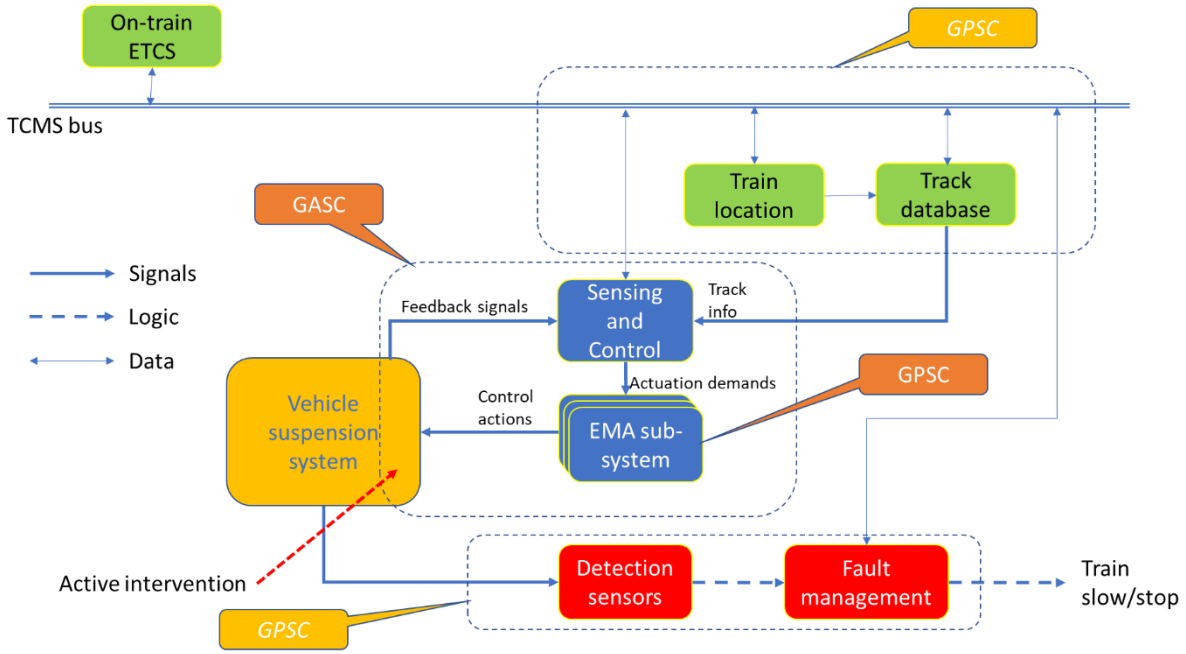

Figure 4: Generic Active Suspension diagram.

This scheme 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 shown at the top of the figure. The object of the GPSC in this case would be the device that provides track information signals and data to the sensing and control unit feeding the EMA sub-system. In a typical European architecture, this would involve interfacing with the Train Control and Management System (TCMS) bus, for example to extract location information from the odometry system comprised in the on-board signalling equipment, typically the European Train Control System (ETCS).

As drawn, there is also 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; this is indicated at the bottom of the figure but again may not be a necessary system requirement.

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

4.1.2 Sub-systems and fault modes

Table 1 lists broadly representative sub-systems for a typical EMA. Each sub-system will generally comprise a number of components[2], which may also include quality assurance documentation. The second column lists the type of documentation that might constitute the approach to safety, and the third column gives broadly representative sub-system failure probabilities.

Table 1 EMA sub-systems

Subsystem	Approach to demonstrate safety	Failure probability
Electric motor	Initial supplier's Quality Control (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 and software design document Independent bench test Regular maintenance checks	$10x10^{-6}$ /h (but Safety Integrity Level (SIL) 4 components available ($<10^{-9}$ /h)
Cabling	Pre-installation test	$4x10^{-6}$ /h (value for a databus)

Faults in the various components can create or contribute to a variety of EMA faults that may lead to unsafe failures within an active suspension application, and Table *2~~Table 2~~* identifies these causalities. The failure probabilities from Table 1 are copied to the column headings, and the corresponding

[2] The following NASA definitions are used to describe the various elements of a suspension system:

- System: an integrated set of elements that accomplish a defined objective. What is to be created.
- Subsystem: a system in its own right, except it normally will not provide a useful function on its own, it must be integrated with other subsystems (or systems) to make a system.
- Components: elements that make up a subsystem or system.
- Parts: elements on the lowest level of the hierarchy.

probabilities of faults leading to each fault (state) can be derived from the combination of relevant sub-system failure probabilities. Again, these are not definitive, rather typical combinations are suggested to illustrate the general principle.

Table 2 Relationships between component faults and EMA subsystem fault states

Fault state			**Component**					
		Motor	Power amp	Mechanics	Sensors	Control electronics	Cabling	Failure probability
	Per hour	$20x10^{-6}$	$20x10^{-6}$	$0.025x10^{-6}$	$10x10^{-6}$	$10x10^{-6}$	$4x10^{-6}$	
H001	Locked	×	×	✓	×	×	×	$0.025x10^{-6}$
H002	Free	×	×	✓	×	×	×	$0.025x10^{-6}$
H003	Zero force	✓	✓	×	✓	✓	✓	To be calculated
H004	Force excess	×	×	×	✓	✓	✓	To be calculated
H005	Inversion	×	×	×	Perhaps checked in testing	✓	×	$14x10^{-6}$
H006	Random force	×	×	×	✓	✓	×	$14x10^{-6}$
H007	Pulse force	×	✓	×	✓	✓	×	To be calculated

The fault states are explained as follows.

- Locked: This is a purely mechanical fault, arising principally from a catastrophic degradation of the nut which essentially jams it onto the screw, something that will normally only arise if the maintenance checks of the mechanism (too much free play, loss of lubrication) are neglected.
- Free: This fault would be caused by a mechanical breakage within the screw/nut assembly and is distinct from “Zero force” described below.
- Zero force: This will arise from failure of the motor to be energised, and in contrast to the “Free” state the motor inertia will still be connected to the output which will affect the system dynamics.
- Force excess: In contrast with the “Locked” state, this will be due to a motor controller failure, with demand for a higher than expected force from the actuator.
- Inversion: A faulty sensor connection or a software function could result in the opposite polarity of force being demanded.
- Random force: This would arise due to a partial sensor failure or an intermittent wiring problem.
- Pulse force: Similar to “Random force”.

It is useful to note that modern power amplifiers have several self-protection functions that disable them, in particular over-current and under- or over-voltage. This would lead to the “Zero force” fault state, and this choice of component may be a significant mitigation for some fault effects.

4.2 The GASC

4.2.1 Technology overview

A Generic Application Safety Case (GASC) for an active lateral secondary suspension application utilising EMAs would have a more specific version of Fig. 4, as shown in Fig. 5. Various features have been removed and more relevant “Feedback signals” and “Control actions” added . As an example, it considers two EMAs connected laterally (horizontally) in parallel with the secondary (airspring) suspension, one on each bogie of a passenger coach. 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).

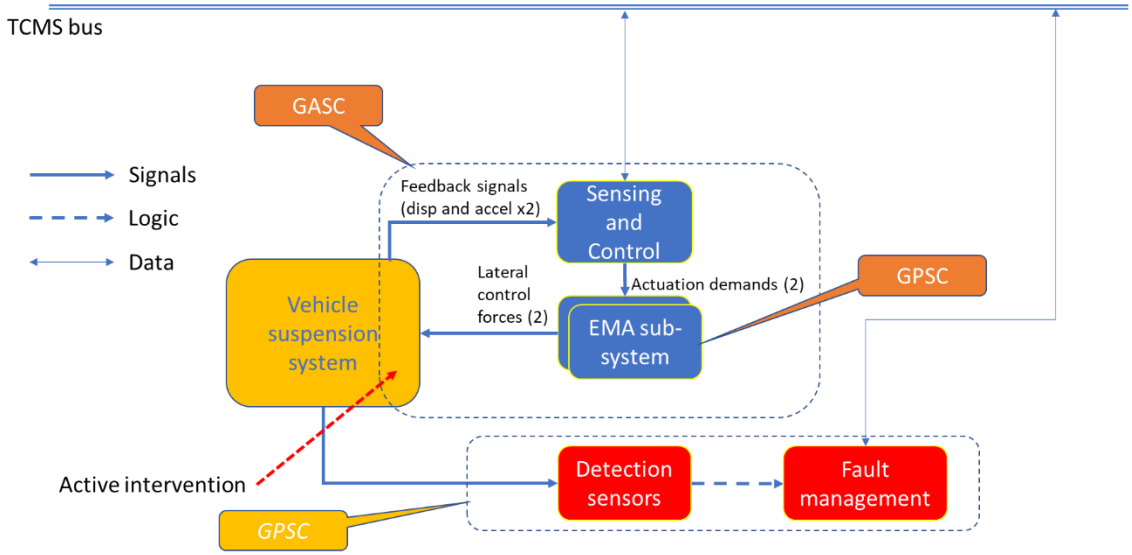

Figure 5: Overall system diagram for active lateral secondary suspension using EMAs.

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

4.2.2 Fault assessment

The hazard list shown in Table 3~~Table 3~~ presents the safety hazards identified during the safety analysis that shows the effect of the GPSC faults upon the overall suspension system. The safety analysis will be based upon both the actuator model from the EMA GPSC and a detailed vehicle model in a Multi-Body Simulation (MBS) package. Because there are two EMAs in this particular application the single H001 fault state becomes two, one for each EMA. In this case the rows might be very similar, but listing separately is essential.

Table 3 Hazard list

Hazard ID	Hazard name (EMA fault state)	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 the table a full set of tables would be required to provide technical comments related to their effect upon vehicle safety. For this paper only two of the tables are included to illustrate the principles. The “Hazard Consequence” rows indicate that Table 4 identifies a safe fault effect, whereas Table 5 identifies a potentially unsafe fault.

Table 4 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 2), 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 ($0.025x10^{-6}$ 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	*State where evidence of closure of the hazard can be found, in many cases the evidence will be another part of the Technical Safety Report (TSR).*
Date added	*Not needed for example GASC, but would be needed for a real Safety Case*
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 005a description

Hazard ID	H005a
Hazard name	Leading EMA force inversion.
Status	Closed
Hazard cause	Refer to GPSC (Table2)
Hazard consequence	Transient exceedances of EN 14363 Y/Q limits and high lateral forces on the track
Hazard source	Identified in the GPSC (Table 4), 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

Obviously, for a real vehicle authorisation much more information would be required. The purpose of the paper is to introduce a generally-applicable authorisation process, and the example has been included to drill down a little into the detail that would underpin the framework described in Section 3.

5. Conclusion

The documentation for the Authorisation Strategy that has been developed as part of the RUN2Rail project is illustrated in Figure 6. It covers the following:

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

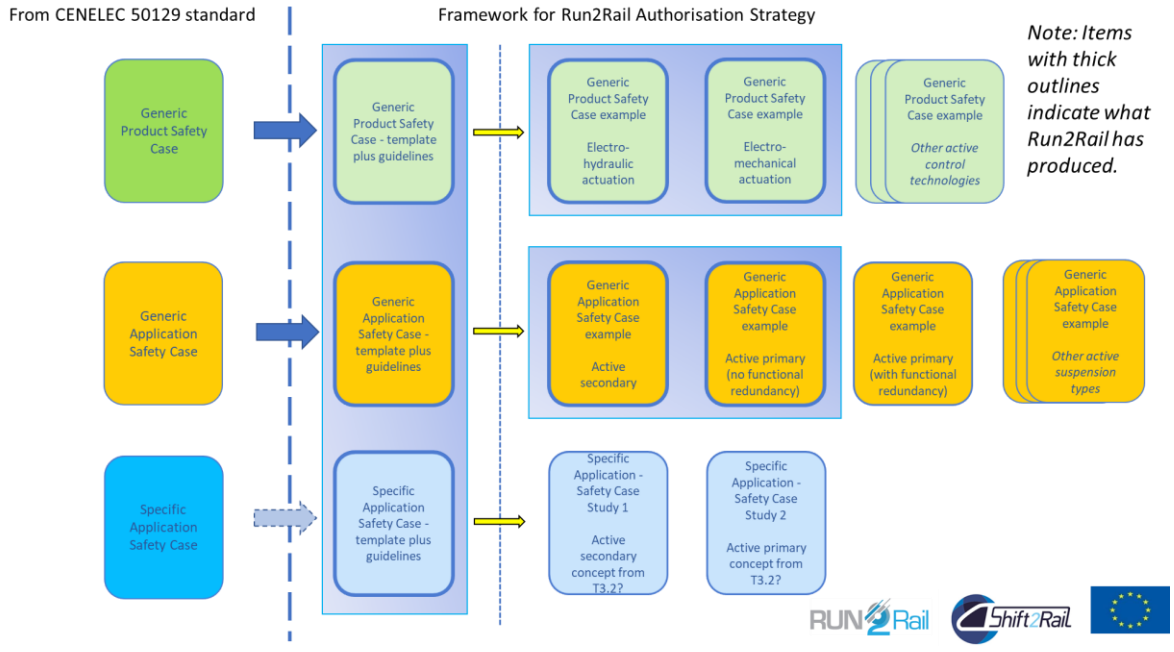

Figure 6: Authorisation strategy framework

The combination of documents and illustrative examples provide potential industry exploiters with a valuable starting point for a full safety case submission. In particular it enables re-use of pre-existing safety cases, and provides pro-forma documents (the templates) for writing new safety cases.

The work has focussed only upon the Safety aspect of the RAMS process. In particular, as mentioned in Section 3, it does not deal with operational reliability, and in practice additional functional redundancy may be required to deliver the required level, i.e. in addition to that required to assure safe operation.

Acknowledgment

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 777564. The paper reflects only the authors' view and the Joint Undertaking is not responsible for any use that may be made of the information it contains.
The authors acknowledge support from all the members of the project partners who have provided important advice.

References

[1] Bruni, S, Goodall, RM, Mei, TX, Tsunashima, H (2007) Control and Monitoring for Railway Vehicle Dynamics, Vehicle System Dynamics, 45(7-8), pp.743-779, ISSN: 0042-3114. DOI: 10.1080/00423110701426690
[2] Directive (EU) 2016/797 of the European Parliament and Council, 11 May 2016, Interoperability of the rail system within the European Union
[3] Directive (EU) 2016/798 of the European Parliament and Council, 11 May 2016, Railway Safety
[4] Commission Implementing Regulation (EU) No 402/2013, Common Safety Method for Risk Evaluation and Assessment
[5] Commission Regulation (EU) No 1302/2014, Nov 2014, technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union
[6] EN 14363:2016+A1:2018. Railway applications. Testing and Simulation for the acceptance of running characteristics of railway vehicles. Running Behaviour and stationary tests.
[7] Goodall, RM, Dixon, R, Dwyer, VM (2006) Operational Reliability Calculations for Critical Systems. In Zhang Zhang, (ed) Proceedings of 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS) 2006, Beijing, China, pp.771-776.
[8] European Railway Agency (2009). Collection of examples of risk assessment and of some possible tools supporting the CSM Regulation.
[9] European Standard EN 50129:2018; Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling
[10] 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