Safety Case Design Structure for Satellite Based Localisation in Railways

Hansjörg Manz, Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder
Technische Universität Braunschweig; Institute for Traffic Safety and Automation Engineering
Langer Kamp 8, 38106 Braunschweig, Germany
h.manz@tu-bs.de; e.schnieder@tu-bs.de

ABSTRACT
Satellite based localisation systems (GNSS) – GPS, GLONASS and future Galileo – are widely used for non safety relevant applications in transport like passenger information or tracking and tracing of goods providing large economical and operational benefits. In all four domains of transport – road, rail, aviation and maritime – the usage of satellite based localisation for safety relevant applications – for example automatic driving and train control – would bring even more benefits but requires a certification. To apply satellite based localisation systems in safety relevant applications, the domain specific certification regulations have to be respected. In this paper, these regulations are analysed with a specific focus on the application of satellite based localisation systems in railways. This work is done within the project GaLoROI which has the target to develop a certifiable satellite based localisation unit for railways.

KEYWORDS: GNSS, safety case, certification, railways

1 INTRODUCTION
For the application of satellite based localisation in railways, a certification according to the railway specific normative background is necessary. Therefore the certification process has to be compliant with the current normative background. Because of their importance within the certification process for safety relevant applications the necessary documents are analysed in this paper. A specific focus will be laid on the different parties involved in the process. These parties – e.g. manufacturer and assessor – have different responsibilities which are derived including the documents they use. The target of this analysis is to clarify the design of the safety case including all documents to be used. This shall ease the work for all parties in the certification process and structure the normative background of the certification together with the clarification of the roles and responsibilities of the involved parties. This will ensure that all documents and requirements are included and that the structure of the safety case can be correctly understood by all involved parties. This structure will enable a general understanding and help to easily accomplish all necessary processes and requirements adequately. The involved parties shall only receive information relevant for them.

The safety case as an important part of the certification process is created by the manufacturer and assessed by the safety assessor to officially prove that the product has been developed according to the respective current normative framework. The safety case and its approval is currently done for every specific application and structured according to the background of the manufacturer and assessor. The target of this paper is a clear structured certification process usable in the railway domain. In this paper this will be done on the base of the application of satellite based localisation in the railway domain but it shall be applicable for other products or devices to be certified as well.
As base of this paper, the certification process for satellite based localisation systems in transportation will be introduced in chapter 2 focusing on the generic certification of satellite based localisation systems on the one hand and the domain specific certification on the other hand. Following, the normative framework of certification in railways will be introduced in chapter 3. Based on this, the structure of the certification and relevant normative documents are focused. In chapter 4, the safety case design structure is introduced. This includes the requirements on safety case modelling, the structure of the safety case as well as certification relevant properties, characteristics and applications. Chapter 5 finishes this paper with a conclusion.

2 CERTIFICATION FOR GNSS IN TRANSPORTATION

Currently many applications in transport use satellite based localisation systems like GPS or GLONASS. This is mostly restricted to information purposes, safety relevant applications are not possible because of the missing certification of satellite based localisation systems. To foster safety relevant applications in transport, a certification for these applications using satellite based localisation systems or for the satellite based localisation system itself is necessary. In subchapter 2.1, an introduction to safety relevant applications for Galileo is given. In subchapter 2.2, the general certification for Galileo will be introduced; in subchapter 2.3 the application specific certification will be focused.

2.1 Galileo for safety relevant applications

For satellite based localisation, generally all GNSS can be used. The systems currently in operation are GPS operated by the US-American military and GLONASS operated by the Russian military. The European system Galileo and the Chinese system COMPASS are currently under development. COMPASS is developed and will be operated by the Chinese military. Galileo is the only civil developed GNSS and has therefore a focus on civil requirements which have been included into the development phase as specifications of a part of the five Galileo services. Within Galileo, the five services “Open Service” (OS), “Commercial Service” (CS), “Safety of Life” (SoL), “Public Regulated Service” (PRS) as well as “Search and Rescue” (SAR) are planned. Out of these services, the Safety of Life service is designed to provide a specifically defined safe localisation [European Comission/European Space Agency 2002]. To use the according localisation results for safety relevant purposes, a certification is necessary. Furthermore, liability has to be regarded in the safety relevant context specific for each domain [Schnieder 2009].

The certification can be either done for the satellite based localisation system in general or specifically for an application in a certain domain.

2.2 Generic certification of satellite based localisation systems

The generic certification of a satellite based localisation system like Galileo would have the advantage that any application could use the signals of Galileo according to the specifications which are then guaranteed. This would require that Galileo – which will be mainly referred in this paper – is certified based on its specifications. These are defined in [European Comission/European Space Agency 2002] and specify for example an horizontal accuracy of 4 metres and a vertical accuracy of 8 metres for 95% of all localisation fixes. One of the first projects dealing with the certification of Galileo was GALCERT [Seybold 2007]. This project implemented “a certification scheme […] that covered both the validation of Galileo signals in space against the SRD (System Requirements Document) […] and the Galileo services against the present MRD (Mission Requirements Document)” [Seybold 2007]. With the combination of the knowledge of certification procedures, relevant documents for certification purposes and requirements for the notified body GALCERT provided an overall Galileo certification process. This process followed the idea of certifying Galileo as a whole by a certification authority including the in-orbit validation (IOV) and the validation of the full operational capability (FOC) followed by the validation of the technical evaluation leading to a certification supported by a formal evaluation. For this
certification process, the full operational capability of Galileo was necessary and planned for 2012 which did not happen. The elements of the Galileo certification plan presented in GALCERT are the certification process, the development plan, a roadmap and a life cycle model [Seybold 2007].

As the development of Galileo is delayed and the introduction of its Safety of Life (SoL) Service is questioned, the usage of EGNOS is promoted. In addition to satellite based localisation systems, satellite based augmentation systems (SBAS) are used to increase accuracy. Those systems are for example the Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay Service (EGNOS). SBAS use geostationary satellites to increase the accuracy of GNSS.

EGNOS is a project of the European Space Agency (ESA), the European Union (EU) and Eurocontrol which is the European Organisation for the Safety of Air Navigation. This already shows the strong focus of EGNOS on aviation.

The Safety of Life Service (SoL) of EGNOS is currently the only adequate service for safety relevant satellite based localisation. It was set operational in March 2011 [GPS World 2011]. With currently no generic certification of EGNOS SoL planned and the delay of Galileo SoL, the certification needs to be done for EGNOS SoL. To achieve this, the current approach is to certify EGNOS SoL for specific applications which are referred to in subchapter 2.3.

2.3 Domain specific certification of satellite based localisation systems

After EGNOS SoL was set operational, the first applications certified for this service are in aviation. The first aircraft landings with EGNOS SoL as localisation device have been performed at Pau airport in Southern France [GPS World 2011]. For this purpose EGNOS SoL has been certified by air navigation providers. This approach is not only a domain specific certification but even a specific certification for certain airports. The certification for applications of Galileo and EGNOS has to be in line with domain specific requirements, norms, regulations and laws [Schnieder 2009].

For the application of EGNOS in other domains then aviation, it has to be certified in their specific context according to its specific regulations. For this certification, the domain specific processes have to be regarded. One of the first approaches to do so was the GAUSS basic project for automotive, aviation and railways [GAUSS Basisprojekt 2010]. The main result of the project was the comparable structure of the certification processes in these three domains. In all focused domains the involved parties are the manufacturer, the assessor and a governmental authority. The process for the railway domain, which is focused in this paper, has been adapted to the current state of the art and the requirements of the project GaLoROI in accordance to EN 50126 [EN 1999] and EN 50129 [EN 2003].

In all product certifications the valid laws in the country where the certification takes place have to be followed. Other relevant documents are internal documents of the operator and the state of the art. All relevant documents are detailed in chapter 3.

In the following chapters of this paper the focus will be on the certification of satellite based localisation specific for the railway domain. A generic certification of satellite based localisation for several domains is currently not regarded as realistic option because the completion of the development of Galileo cannot be estimated. Furthermore, no generic certification of Galileo or EGNOS seems to be carried out currently.

3 NORMATIVE FRAMEWORK OF CERTIFICATION IN RAILWAYS

As analysed in chapter 2, a domain specific certification is a necessary base for the safety relevant application of satellite based localisation systems in railways. To enable this, the normative documents in the railway domain are analysed. The certification process in railways in Europe is based on international and national laws and standards. For a good understanding and structure the normative context of certification in railways will be analysed in detail in this chapter.
To get an overview and a basic understanding, the certification process in railways is structured according the involved parties in subchapter 3.1. In 3.2, the relevant normative documents are analysed.

3.1 Certification process

The certification process in railways is performed by three players. These are the manufacturer, the assessor and the railway authority. This certification process is shown in Fig. 1 according to [EN 2003] and [GAUSS Basisprojekt 2010].

The central element of the certification process in railways is the safety case. It has to be created by the manufacturer and assessed by the assessor to prove the compliance of the developed product with the standards and the legislative background which are explained in subchapter 3.2.

For a detailed understanding of the certification process it is structured into its functions according to the specific responsibilities [Hänsel 2008]. The manufacturer is responsible for the development process. The design of a product or system starts with the requirements of the operator to the product which provides important advices to the design process supported by the permanent verification and validation of the development where the assessor and the responsible authority can participate to enable a smooth safety assessment and approval. An efficient certification after the development is as well fostered by the information of the railway authority that a new product is developed, a confirmation of the railway authority that no circumstances are known that might lead to a denial of approval during the whole process is aspired. During the development process the safety assessment is done leading to a safety case which is handed in to the assessor. The assessor should accompany the development process as base for a fast assessment of the safety case. The accordingly resulting assessment report is handed in to the railway authority. It first provides the generic product approval followed by the specific product approval. After this, the product can be delivered to the operator.

Figure 1: Certification Process in Railways [EN 2003; GAUSS Basisprojekt 2010]
3.2 Relevant normative documents

In this subchapter the relevant normative documents during the development and certification of a product or system in railways are focused. These documents are strongly influenced by European harmonisation [Schnieder 2009]. This process is necessary because a national restricted legislation is outdated and obstructs border crossing traffic as well as Europe-wide certification.

The European and national normative background can be structured in detail as shown in Fig. 2. The mandatory documents are the European and national constitution, national laws, national regulations, EU-decisions, EU-regulations and EU-directives. In this context it is of special importance that European regulations are directly binding for the members of the European Union, whereas directives have to be ratified by the member states. Decisions are binding in all of their parts as well, only if special parties are addressed it is only relevant for those [European Union 2008].

Because of the European harmonisation, national documents have lost importance. European normative documents refer mainly to interoperability and safety targets. The most relevant are [European Commission 2012]:

- Directive 2008/57/EC on the interoperability of the rail system within the Community
- Regulation 2009/352/EC on the adoption of a common safety method on risk evaluation and assessment
- 2010/409/EC Decision on Common Safety Targets
- 2012/88/EU Decision on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system

The not binding parts of the European normative background are technical standards, specifications and documents of the manufacturer as well as requirements of the operator. The most relevant standards are EN 50126 [EN 1999], EN 50128 [EN 2001] and EN 50129 [EN 2003]. EN 50126 is of special importance because it describes the lifecycle which is relevant for the development process. EN 50129 structures the certification process itself.

Normative documents vary from time to time. Until the last decade of the 20th century, only national laws were binding in railways. In the first decade of the 21st century the European Commission started to set up international laws which are now in the second decade of the 21st century solely binding.
Standards are in a process of changes as well. EN 50128 [EN 2001] which structures the certification process has been changed recently. The new version is [EN 2012] which is not widely used yet.

4 SAFETY CASE DESIGN STRUCTURE

The safety case is the central part of the certification process in railways; therefore its structure is important for a successful certification. The structure of the certification process in railways needs to be well understood by all involved parties; therefore an adequate modelling is necessary. According to [Schnieder 2010] this modelling can be done in different ways. The level of formalisation can be informal, semiformal or formal. An informal mean of description is the natural language; a semiformal mean of description can be a message sequent chart and a formal mean of description petri nets or programming languages. If the mean of description is formal, a structured analysis of the context with less risk of misunderstanding is possible. The Institute for Traffic Safety and Automation Engineering of TU Braunschweig (iVA), which is responsible for assessment of the safety case in the project GaLoROI, has already a broad knowledge concerning modelling and formal description. Formal means of description should always be the preferred method because they allow the linguistic work and certification with a low level of misunderstandings. In the last years, an intelligent glossary was developed in the Institute for Traffic Safety and Automation Engineering [Dr. Stein 2012]. This glossary allows structuring terms with their definitions, relations and varieties they belong to. This glossary is based on the intensive work in the Institute in the last years mainly focusing on formal description.

An example for the use of the intelligent glossary in the context of satellite based localisation is the term “integrity” which has been chosen because of its diverse meanings [Manz et al. 2009]. In aerospace “integrity” is used to define the “ability of a system to provide a warning to the user that an error whatever the source might lead to the failure of the system to meet certain margins of accuracy within a given time to alarm.” [European Comission/European Space Agency 2002] In railways, the word “train integrity” only means that a train stays complete with the initial number of carriages. Such kind of misunderstandings shall be prevented by clearly defining the safety case and the according structure in this chapter.

An approach to model the safety case design structure shall be introduced. Therefore, in subchapter 4.1 the requirements on safety case modelling are introduced. Based on this, an outline on the structure of the safety case will be given in subchapter 4.2. This will be followed by the certification relevant properties and characteristics focused in subchapter 4.3, according applications are regarded in subchapter 4.4.

4.1 Requirements on safety case modelling

The safety case shall be modelled comprehensive for all involved parties to allow creating an usable structure. This process and structure has to comply with the normative background. The development of a technical system in railways according the valid standardisation and laws is necessary [Hänsel 2008], therefore the structure of the safety case needs to be modelled adaptable to later changes of the normative background.

To allow the modelling of the safety case structure the requirements to the means of description, methods and tools have to be defined. This is currently done within the project GaLoROI where the safety case of the localisation unit is performed accompanying the development. Some requirements to the safety case modelling are:

- Show relevant input documents
- Show relevant output documents
- Structure the safety case
- Relevant processes
- Clarify responsibilities
These requirements are an important base for the structured modelling of the safety case in GaLoROI and beyond.

4.2 Structure of the safety case

As shown in Figure 1, the involved parties in the certification of a system are the operator, the manufacturer, the assessor and the railway authority. The operator sets the requirement to the system which is produced by the manufacturer. After the assessor confirms the safety of the system according the normative background and the state of the art, the railway authority provides the product approval necessary for the service of the system performed by the operator. Within this process, the safety of the system is proven by a safety case. Therefore the basic structure of the safety case is a central part of the certification process and specified in EN 50129 [EN 2003] which has to be followed. Therefore the safety case has to consist of six parts [EN 2003]:

1. Definition of System
2. Quality Management Report
4. Technical Safety Report
5. Related Safety Cases
6. Conclusion

In the first part (Definition of System), the system for which the safety case is performed has to be defined in detail including its basic functions. The used software and hardware needs to be explained including necessary documents and system requirements which shall be done methodological with according tools [Bikker/Schroeder 2002].

The second part (Quality Management Report) and third part (Safety Management Report) of the safety case are standard documents of the manufacturer. In these documents it has to be proven that a quality and safety management system is in use. Most manufacturers are today certified according EN ISO 9001 which is a simple prove for this. The safety management report includes the safety life-cycle known as V-model.

The fourth part (Technical Safety Report) is the central part of the safety case. In this document the system architecture is described based on the requirements and the definition of the system. A reference to existing system architectures and specifications is possible. Furthermore, interfaces have to be defined as well as how system and safety requirements shall be fulfilled. Hardware and software functionality and the assurance of the correct function of the system as well as testing procedures are, among others, part of the technical safety report.

The fifth part (related safety cases) relates to other safety cases where the main system depends on. This might by a device or a safe computer which is part of the system.

The sixth part (conclusion) summarises the proof of the previous chapters.

The documents for the safety case have to be created by the manufacturer and in part by its suppliers. The documents and processes shall be shown specifically for each involved party. In the project INESS, funded as well by the European Commission as FP 7 project, the Goal Structured Notation (GSN) was introduced [von Buxhoeveden/Trog 2012]. GSN is a user interface for the structure of the safety case and has a direct link to a document management system. This allows a direct and structured access to all required documents.

The approach in GaLoROI shall be one step further. Here not only the documents produced within the safety case are structured. Beyond that, all normative documents which are needed as input are structured. In this structure, a hazard analysis of EGNOS SoL and railway RAMS should be included [Lu et al. 2012].
4.3 Certification relevant properties and characteristics

During the certification of a technical system a large number of properties and characteristics have to be derived and clearly structured, especially if the certification takes place under safety relevant aspects. The according modelling of the normative background [Hänsel 2008; Schnieder et al. 2009] is an important base for the later system approval for regular operations.

The quality is an important property of a safety relevant system. It can detail aspects like measurement deviation and errors [Wegener et al. 2011]. These quantities of technological quality are the base for a reference measurement system [DemoOrt 2009; Wegener et al. 2010] which has the ability to analyse and evaluate the quality of satellite based localisation system [Grasso Toro et al. 2012]. In this paper, the modelling is done for applications of satellite based localisation in the railway domain.

4.4 Applications

GaLoROI is a project funded by the European Galileo Supervising Authority (GSA) within the Seventh Framework Programme (FP7) of the European Commission. This project has the target to develop a certifiable satellite based localisation unit for railways. To reach this target, the normative context of railways has been analysed in this paper. This is done to have a good base for certification within the project and to structure the safety case for later projects and products.

In this subchapter applications of the railway domain requiring safety relevant localisation because of their high requirements on accuracy, availability, safety and reliability are introduced. These applications can be allocated to the categories train control, track maintenance und railway station. Applications of the category train control are e.g.:

- Speed and distance supervision
- Level crossings
- Stand still detection
- Collision warning

Applications of the category track maintenance are e.g.:

- Protection of track workers
- Control of track laying machinery
- Automation of civil engineering works

These applications can be analysed according their requirements which will be structured according to the attribute hierarchy introduced in [Schnieder 2010]. The concept of the attribute hierarchy breaks down the application into its attributes. These attributes are properties, characteristics, values and quantities with their units. In Fig. 3, an example of the attribute hierarchy is shown for “Speed and distance supervision”. The safety relevant application of satellite based localisation systems in railways is shown with its properties relevant for safe localisations which are accuracy, availability and safety. This attribute hierarchy can of course be extended.

This attribute hierarchy shall be used for all applications in railways and other modes of transport requiring a safe localisation to derive their requirements on localisation. These requirements will be matched with the specifications of GNSS and their augmentation systems to certify the used localisation unit.

![Attribute Hierarchy Example](image)

Figure 3: Requirements of applications according to [Schnieder 2010]
5 CONCLUSION

In this paper, the certification of GNSS in transport with a focus on railway applications was introduced. Due to no generic certification for GNSS available, the necessity of a railway specific certification for satellite based applications in this domain was shown. For certifications in railways a safety case is necessary. Therefore a structure for the safety case was introduced in this paper. This structure is very clear because it follows European standardisation. The challenges in this case are the diverse interpretations of this structure by involved parties. A single interpretation fostered in the project GaLoROI will be an important base for a certification of applications of satellite based localisation for railways in Europe.

As base for this certification the requirements of safety relevant applications to localisation have to be clarified. A possibility to do so has been introduced in this paper.

6 ACKNOWLEDGEMENT

The authors thank the European Galileo Supervising Authority (GSA) for funding the European research project GaLoROI within the Seventh Framework Programme (FP7) which made this work possible.

REFERENCES


Schnieder et al. 2009 Schnieder, Eckehard; Becker, Uwe; Hänsel, Frank; Manz, Hansjörg; Poliak, Ján; Schröder, Jürgen; Zhou, Yong: Entwicklung einer Methodik zur Zertifizierung von Ortungseinrichtungen unter sicherheitsrelevanten Aspekten. ZEUS - Projektabschlussbericht, Braunschweig, 2009.


