Safety Approval Process for Guided Transportation

Robert Bains
SINTEF Digital, Norway. E-mail: robert.bains@sintef.no

Thor Myklebust
SINTEF Digital, Norway. E-mail: thor.myklebust@sintef.no

Narve Lyngby
SINTEF Digital, Norway. E-mail: narve.lyngby@sintef.no

Efficient and well-defined Safety Approval Processes is important for Guided Transportation to be widely spread, ensure continuous improvements and to cover a significant part of societies' transportation needs. The current paper addresses the first steps of establishing a Safety Approval Process for Guided Transportation. We have evaluated relevant European regulations and current safety standards for different guided transportation domains. These domains include railway, metro, urban guided transport and hyperloop. The Safety Approval Process covers among others the process involved from concept to decommissioning, relevant stakeholders and the type of information required as part of the safety approval.

Keywords: Guided transportation, regulation, safety standards, Safety Approval Process.

1. Introduction

The railway domain, in Europe, is considered to have well-established Safety Approval Process but also well-established technology (excluding autonomous systems). Other domains covered by the 'Guided Transportation' term, such as for example Hyperloop, is significantly less mature. Despite the maturity of the Safety Approval Process within the railway domain, there may be possibility of improvement also within the railway domain. It is nevertheless foreseen that the other less mature domains included within the 'Guided Transportation' term may benefit from having a look at the established practices within the railway domain.

This paper is organized as follows: the remaining part of chapter 1 includes a definition of the 'Guided Transportation' term, presents the main stakeholders relevant for Guided Transportation and describes the delimitations made during this work. Chapter 2 presents the existing Safety Approval Processes within the domains covered by this paper. Chapter 3 covers technical aspects that may influence the choice of Safety Approval Processes. Chapter 4 compares the Safety Approval Processes for the different domains covered by this paper. Chapter 5 presents the Safety Approval Process proposed by the authors of this paper. Chapter 6 presents the conclusion and suggests topics for further research.

1.2 *Guided transportation*

Based on literature search (search through directives, regulations and standards) it appears that the term “guided transportation” is used several times but not always defining the term explicitly, possibly due being implicitly understood what the meaning of this term is, but also due to domain specific terms such as railway, metro etc. being used more commonly. A few definitions have however been found. The Modular Urban Transport Safety and Security Analysis (MODSafe) project, ref. Coineau D. (2012), defines the term 'Urban guided transport'. Furthermore, the same term has been defined by the IEC 62290-1:2014 which is a standard for urban guided transport (UGT) management and command/control systems:

"UGT is defined as a public transportation system in an urban environment with self-propelled vehicles and operated on a guideway, which is segregated from general road and pedestrian traffic."

The definition from Service Technique des Remontées Mécaniques et des Transports Guidé (STRMTG, national technical agency that is part of the French Environment, Energy and the Sea Ministry) has been the basis for the definition included in this paper STRMTG (2019):

"The “guided transport” terms mean public passenger transport systems whereby the vehicles follow a determined trajectory for all or part of their journey, with the exception of those which circulate exclusively on the national rail network.

These are, therefore, subways, trams, railways providing outside the national rail network a regular service or tourist journeys, and intermediate systems such as buses or trolley buses guided by rail or any other non-physical system (optical or magnetic guidance)."

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

It is found to be beneficial to redefine term for the scope of the work documented in this paper:

Guided Transportation means transport systems whereby the transport vehicles are physically guided (by e.g. rails or tubes) such as railway, metro, urban rail, trams and hyperloop but also transport vehicles guided by sensors such as automatic and autonomous systems. The term also covers safety related systems (external or internal of the transport vehicles) required to control the transport vehicles.

The term Guided Transportation has a quite wide definition in this paper. As a first step of suggesting a Safety Approval Process, a subset of the transportation domains included in the Guided Transportation term has been covered; see chapter 1.4 Delimitation for further description.

1.3 *Stakeholders*

Below we have mentioned the main stakeholders when approving guided transport constituents, products and systems in Europe.

DG Move, The Commission's Directorate-General for Mobility and Transport is responsible for EU policy on mobility and transport.

The Ministry of Transport in each EU/EEA (European Economic Area) country has often overall responsibility for the framework conditions for rail transport together with other transport sectors and the transport policy

European Union Railway Agency. Their mission is to make the railway system work better for society and to contribute to the effective functioning of a Single European Railway Area without frontiers. Their tasks are

- Promote a harmonized approach to railway safety
- Devise the technical and legal framework in order to enable removing technical barriers, and acting as the system authority for ERTMS and telematics applications
- Improve accessibility and use of railway system information
- Act as the European Authority under the 4th Railway Package issuing vehicle (type) authorizations and single safety certificates, while improving the competitive position of the railway sector.

The term "**Safety Authority**" is defined in EN 50126:2017, EN 50128:2011 and EN 50129:2018. The term "National Safety Authority" (NSA) is used (not defined) in (EU) 2015/1136 and (EU) No 402/2013. NSA refers to the stakeholder responsible for delivering the authorization for the operation of the safety-related system. Often, they also have the national responsibility for regulations and participate in the revision of regulations and in the development of new regulations.

The **manufacturer** role is defined and clarified mainly related to legal aspects in the "Blue guide 2016": The manufacturer is any natural or legal person who manufactures a product or has a product designed or manufactured, and places it on the market under his own name or trademark. The manufacturer is responsible for the conformity assessment of the product and is subject to a series of obligations including traceability requirements. When placing a product on the Union market, the responsibilities of a manufacturer are the same whether he is established outside the European Union or in a Member State. The manufacturer must cooperate with the competent national authorities in charge of market surveillance in case of a product presenting a risk or being non-compliant.

Assessor is defined in EN 50128:2011, EN 50129:2018 and EN 50126:2017. The role refers to the stakeholder(s) who evaluates the conformity of the process and the outcomes against the requirements of the standard, including SIL assignment.

EU directive 2017/797/EC. A **Notified Body** (NoBo) is an organization that has been nominated by the government of a member state and notified to the European Commission. The primary role of a NoBo is to provide services for conformity assessment of the conditions set out in the directives. This normally means assessing the manufacturers' conformity to the essential requirements listed in each directive. Conformity assessment can be inspection, quality assurance, type examination or design examination, or a combination of these. The benefit of NoBo certification is that, in principle, it is issued once and accepted everywhere within EU.

Assessment body (AsBo) is defined in (EU) 2015/1136 and (EU) No 402/2013. This is the stakeholder who carries out an independent assessment of the suitability of the applied risk management process concerning the proposed change and of its results.

The **proposer** is defined in (EU) 2015/1136 and (EU) No 402/2013. This is the stakeholder who proposes the change of the railway system and who is responsible for applying the regulation, including the assessment of the significance of the change.

The **Accreditation bodies**. Accreditation is a means of assessing, in the public interest, the technical competence and integrity of conformity assessment bodies. The idea of regulating accreditation at European level is twofold.

• a comprehensive European framework for accreditation provides the last level of public control in the European conformity assessment chain and is therefore an important element in ensuring product conformity

• it enhances the free movement of products and services across the EU by underpinning trust in their safety and compliance with other issues of public interest protection.

EU Decision commission 2010/713 "on modules for the procedures for assessment of conformity, suitability for use and EC verification to be used in the technical specifications for interoperability adopted under Directive 2008/57/EC of the European Parliament and of the Council" includes requirements and benefits by applying accreditation. E.g. copy from 2010/713: "When the manufacturer operates a certified quality management system certified by an accredited certification body, for the manufacturing of the relevant interoperability constituent, the NoBo shall take this into account in the assessment.". Testing laboratories, ISA, assessment body and NoBo can be accredited by accreditation bodies for their relevant work.

1.4 *Delimitation*

The work in this paper are based on the following delimitations:

- European safety standards and regulations are considered.
- Standards and regulations representing functional, technical and interoperability requirements are not considered.
- Security requirements are not considered.
- Railway, metro, urban guided transport and hyperloop are the subset of domains covered by the Guided Transportation term that are considered in this work.

2. Existing safety approval processes

The safety approval processes for several of the domains considered in this paper are defined by railway specific safety standards published by CENELEC: EN 50126:2017, EN 50128:2011 and EN 50129:2018. The current chapter addresses the safety approval process as defined by these safety standards, whereas sections 2.1-2.4 addresses the safety approval process for the specific domains considered in this paper.

A central aspect of the safety approval process is the determination of the actors to be involved and their tasks/responsibilities. Table 1 lists the main actors and includes a brief description of their responsibilities.

Table 1 Type of actors defined by the CENELEC railway specific safety standards EN 50126:2017, EN 50128:2011 and EN 50129:2018

Actor/Responsibility description
Assessor. The role is described in section 1.3 of this paper.
Independent Safety Assessor (ISA)/Safety Assessor. The actor who checks whether the system/product meets the specified safety requirements and forms a judgement as to whether the system/product is fit for its intended purpose in relation to safety.
Railway duty holder. The role is defined in EN 50126:2017 and EN 50129:2018. Refers to the actor with the overall accountability for operating a railway system within the legal framework. The responsibilities can be split between one or more bodies or entities.
Railway supplier. Term ("Supplier") defined in EN 50128:2011. Term used (not defined) in EN 50126:2017 and EN 50129:2018. Refers to the actor who designs and builds a railway control and protection system including the software or parts thereof.
Safety authority. The role is described in section 1.3 of this paper.

To summarize, regarding actors involved in the safety approval process, there are generally:

- a railway supplier that develops the systems to be given safety approval,
- a railway duty holder (with overall accountability for operating the railway system),
- ISA (the third party that checks whether requirements from safety standards are complied with), and
- the Safety Authority who may give the safety authorization based on the input from the ISA.

A central aspect of the Safety Approval Process is the production of safety documentation and documentation from the ISA and the Safety authority. A brief summary of the safety documentation required from the railway specific safety standards are provided below.

EN 50126:2017: Relatively large number of documents related to reliability, availability, maintainability and safety required to be produced, especially by the manufacturer. The standard specifies at which lifecycle phases the various document shall be produced and/or updated. Example of documents to be produced: system definition, safety plan, RAM Plan, risk assessment results, hazard log, RAMS system requirements specification, validation plan, validation report, verification plan, verification

report, safety case etc. Responsible of document production: railway duty holder and railway supplier.

EN 50128:2011: Relatively large number of documents related to software development required to be produced. The software documentation to be produced are related to the development lifecycles. The contents of the documents are dependent on the chosen set of techniques and measure applied during the software development. The allowed combinations of techniques and measures are regulated by the standard. Responsible of document production: Supplier. The standard further requires that a software assessment report is produced. The software assessment report documents the evaluation made by the assessor concerning the software development process and the developed software. Responsible of document production: Assessor.

EN 50129:2018: Safety case and large number of documents to be referenced from the safety case. The referenced documents shall be related to the system definition, quality management, safety management and the technical safety of the developed system. Several of the documents required to be produced according to EN 50126:2017 will be referenced in the safety case. Responsible of document production: railway supplier and railway duty holder. The standard further requires that a safety assessment report is produced. The safety assessment report includes the assessment results obtained by the ISA and is mainly based on the evidence that is obtained from the safety case and its referenced documents. Responsible of document production: ISA.

2.1 *Railway*

The railway domain is quite mature when it comes to safety approval processes. In addition to the safety approval of railway systems there are interoperability requirements, governed by the interoperability directive, (EU) 2016/797, and technical specifications of interoperability, that involves Notified Bodies in other to verify the compliance of these requirements. The scope of this paper is only on safety approval processes, and the conformity process related to verification of interoperability requirements is therefore left out of scope; see chapter 1.4 Delimitations.

The following railway specific safety standards, being mandatory standards (with the exception of EN 50129:2018) according to certain technical specifications of interoperability, are applied in conjunction with safety approval within the railway domain:

- EN 50126-1/2:2017, Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- EN 50128:2011, Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems
- EN 50129:2018, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.

The standards are written with the aim of covering the railway domain; however, the standards are also relevant for other domains, as described in section 2.2-2.3 of this paper.

In addition to the CENELEC railway specific safety standards, there is a safety regulation that railway signaling systems (control command signaling subsystems) need to comply with as part of the certification process according to the interoperability directive (EU) 2016/797 and technical specification for interoperability, (EU) 2016/919:

- (EU) 2015/1136, (EU) No 402/2013, common safety method for risk evaluation and assessment.

In practice this means that for several railway systems, both compliance with the safety standards and the common safety method regulations must be made, since several technical specifications for interoperability mandate the application of the common safety method risk assessment process. It shall be, noted however, that compliance with the common safety method can be met by demonstration of compliance with the safety standards.

The relevant actors defined by the CENELEC railway specific standards have been listed in Table 1. In addition, the common safety method for risk evaluation and assessment, (EU) 2015/1136 and (EU) No 402/2013, define central actors. Table 2 lists these central actors.

Table 2 Type of actors defined by (EU) 2015/1136 and (EU) No 402/2013

Actor/Responsibility description
Assessment body. The role is described in section 1.3 of this paper.
Proposer. The role is described in section 1.3 of this paper.

A brief summary of the safety documentation required from the common safety method for risk evaluation and assessment is provided below.

(EU) 2015/1136, (EU) No 402/2013: Risk management documentation including quality and safety procedures, hazard record, safety requirements, safety measures etc. The Common

Safety Method regulation includes requirements to some documentation to be issued but does not include a requirement to issue an aggregated safety document equivalent to the safety case, as required by EN 50129:2018. Responsible of document production: railway duty holder and railway supplier. The regulation further requires that a safety assessment report is produced. The safety assessment report includes the assessment results obtained concerning the applied risk management process and of its results.

To summarize, the safety standards and regulation for railway defines:

- the actors to be involved and their responsibilities (addressed directly above and in chapter 2),
- specific roles involved as part of the development (project manager, designer, verifier, validator etc.)
- the activities to be performed, and
- the documentation to be produced (addressed directly above and in chapter 2) including among others the safety case, risk management documentation, safety assessment report issued by the ISA/Assessment body, and document stating the approval by Safety Authority.

2.2 *Metro*

Metro systems are subject to national safety approval process and are not covered by approval processes defined on the European level. The safety approval processes may therefore potentially vary greatly for metro systems. The Norwegian national safety approval processes, ref. Forskrift om krav til sporvei, tunnelbane, forstadsbane m. m, however, require that the CENELEC safety standards EN 50126/50128/50129, as for the railway domain, are applied. In comparison, the Swedish national safety approval process does not require that specific standards are applied, ref. Transportstyrelsens föreskrifter om godkännande av spåranläggning eller fordon för tunnelbana och spårväg. However, the legislation and especially the CENELEC safety standards define what kind of documentation must be prepared. According to the author's experience the CENELEC safety standards, even though not mandated though national safety processes, are applied as part of the safety approval processes for metro systems. The CENELEC safety standards therefore in practice define the Safety Approval Process for European countries.

The Common Method Safety regulation (EU) 402/2013 amended by (EU) 2015/1136, which is applied in the railway domain, has in general not been applied for Metro in European countries.

In addition to the CENELEC railway specific safety standards, that are central for safety approval, there are a few other standards that provide guidelines. The IEEE standard for Communications-Based Train Control (CBTC) includes requirements related to safety. The IEEE 1474.1:2004, which is part of the IEEE standard for CBTC, includes requirements to safety management, hazard identification, risk assessment process, quantitative safety performance requirements and basic safety design principles. The other parts of the IEEE standard for CBTC does not include safety requirements.

2.3 *Urban guided transport*

Urban guided transport is governed by the IEC 62290 standard series. It is stated however in IEC 62290-1:2014 that the standard series is a recommendation for those transport authorities wishing to introduce interoperable, interchangeable and compatible equipment. The standards state that trains of transport undertakings (e.g. underground/metro, tram, regional and suburban operators) are covered by the 'Urban guided transport' term even if they are operated under specific railway regulations, as long as they also are designated to operate on urban guided transport management and command/control system infrastructure.

Regarding the Safety Approval Process of urban guided transport reference is provided in IEC 62290-1:2014 to the IEC equivalents (IEC 62278/62279/62425) of the railway specific safety standards EN 50126, EN 50128 and EN 50129. The standard IEC 62290-1:2014 further defines five grades of automation (GOA0-GOA4) for the systems. IEC 62278/62279/62425) is defined for all grades of automation except for the lowest grade (GOA0, On-sight train operation).

2.4 *Hyperloop*

Hyperloop is so far not covered by approval processes defined on the European level. The hyperloop tube including magnetic levitation has similarities with railways while the pod that is situated in low air pressure has similarities with aviation. As a result, the approval process foreseen will be based on relevant regulations and guidelines for the railway domain and the aviation domain. In addition, it is expected that generic safety standards like IEC 61508 will be applied. However, the hyperloop system has some major differences as well, especially the vacuum in a tube. So special adaptations are foreseen.

Standardization of design is a challenge for hyperloop. Several companies are working on the hyperloop concept, with different ideas.

3. Technical aspects

The Safety Approval Process may potentially be coupled to aspects related to the technical implementation and the operating environment. The following chapter therefore addresses the typical technical aspects of the different forms of guided transport in order to investigate whether there are specifics from those that should be addressed by the proposed Safety Approval Process.

A short summary of typical characteristics of the selected forms of guided transport is presented in the following.

Traction
Similar for railway, metro and guided transport is that the traction is made between wheel and rail using electric or diesel electric propulsion system. Hyperloop on the other hand is using electromagnet propulsion and vacuum in combination with vacuumed tube.

Interoperability
Trains are moving across national borders on a cross boarder network of rails. A large effort has due to this been made to increase interoperability within the railway domain. Interoperability might also be an aspect for hyperloop. However, the extent is not yet clear, and the Delft report (Delft Hyperloop, 2019)) states that "*To increase interoperability, it is important that there will be a single European standard. However, it is necessary that this does not happen too early in the process, as multiple techniques have to be developed first in order to research their potentials*". Interoperability is not an aspect for metro.

Traffic condition
Common for railway, metro and hyperloop is that the movement is restricted to enclosed infrastructure; rail network for railway and metro, and vacuum tube network for hyperloop. Possible obstacles are mostly restricted to other trains on the track for railway and metro, crossings for railway and other pods in tube for hyperloop. Urban guided transport, however, are moving in an urban environment, and need to cope with surrounding environment, i.e. other vehicles, pedestrians etc.

Speed
There are large differences in operating speed for the different domains. Whilst trams, as an example of urban guided transport, is moving at speeds between 5 and 20 km/h, hyperloop may move at speeds above 1200 km/h. Metro is normally operating up to 80 km/h and railway up to 160 km/h for freight and about 500 km/h for high speed passenger transport.

Navigation
In many ways, physically guided transport is simpler than sensor guided transport. Its path is confined to the rail/tube network, and it can only go in two directions. Sensor guided transport combines a variety of sensors to perceive its surroundings, such as radar, Lidar, sonar, GPS, odometry and inertial measurement units. Advanced control systems interpret sensory information to identify appropriate navigation paths, as well as obstacles and relevant signage.

Positioning
In lack of precise positioning systems, trains are usually separated by dividing the track into section, so called blocks. In normal circumstances, only one train is permitted in each block at a time. This principle forms the basis of most railway safety systems. Blocks can either be fixed (block limits are fixed along the line) or moving blocks (ends of blocks defined relative to moving trains).

The most usual system to determine if a section is occupied is by use of track circuit. An alternative train detection system is the use of axle counters, counting the number of axles arriving and leaving a block section.

Over the last decade, important efforts have been made regarding satellite-based positioning systems, in order to adapt them to civilian applications (e.g. pedestrian and vehicle navigation). The development of Galileo (Europe) and BeiDou (China) are examples (Otegui, et. al. 2017).

Automation technology
For automated train operation within the railway domain, the movement of a train and the control commands are not indicated by signals on the track but are issued via data communication between the train and trackside communications equipment. All of these systems operate similarly:

- In fully automated mode, trains are driven by the automatic train control (ATC) in combination with control and protection of the line by interlockings.
- On board the train, the Automatic Train Operation (ATO) system replaces the driver and controls the train's speed.
- The ATO computer is monitored and, if necessary, corrected by the Automatic Train Protection (ATP) system.

Levels of automation
The level of automation is considered to affect the depth and the degree that human factors are required be addressed in the safety documentation. Higher degree of automation will

lead to lower reliance of humans during the operation phase whereas lower degree of automation will lead to higher reliance of humans during the operation phase. Even though the exact documentation covering human factors is expected to differ between systems with high degree compared to low degree of autonomation, the Safety Approval Process and the type of documentation is not expected to differ for the different degree of automation levels.

The various grades of automation range from driver-assisting functions for control of the brakes and automatic speed control of the vehicle.

IEC 62290-1 (2014) has defined five Grades of Automation (GoA) which are applicable for railway, metro and urban guided transport. The GoA's are defined according to basic functions of train operation and split in operational responsibilities whether it is for humans or the system itself. Hyperloop is still a new mode of transportation and no similar levels of automation has yet been defined.

Additionally, Table 3 shows the status of the different guided transportation domains related to the GoAs. Dark grey color reflects the technological status of the domain, whilst the light grey color reflects where the domain is likely to develop. Table 3 also shows how mature the regulation within the domain related to the different GoAs.

Table 3 Maturity of the regulation within the domains related to the different GoAs

GoA level:	0	1	2	3	4
Railway		x	x	x	x
Metro		x	x	x	x
Hyperloop					
Urban guided	x	x	x	x	x

4. Comparison of Safety Approval Processes for Guided transportation

In practice the Safety Approval Processes of railway, metro and urban guided transport are represented by railway safety standards EN 50126, EN 50128 and EN 50129 which means that the Safety Approval Processes for these modes of guided transportation are to a large degree the same. For urban guided transport, the IEC equivalents (IEC 62278/62279/62425) of these standards are applicable. These standards present quite detailed requirements to the activities to be performed during the different lifecycle phases, the documentation to be produced during the lifecycle phases and the manner the documents shall be collected and structured in a safety case. The standards require further that an independent third party (ISA/safety assessor/assessor) checks compliance with these standards. The railway domain in EU must further demonstrate compliance with the common method safety regulation (EU) 402/2013 amended by (EU) 2015/1136 which presents less detailed requirements with respect to activities and documentation to be produced compared to the requirements from the CENELEC standards. Compliance with the CENELEC standards is also considered being an appropriate means of demonstrating compliance with the risk management process set out in the common method safety regulation.

For Hyperloop, the Safety Approval Process is not established yet and it is an open topic for further investigation. CEN and CENELEC has started a project in 2020 to ensure that standards are established. Several countries have already shown their interest in this project. It is expected that existing railway standards and some aviation standards can be a basis for further development and adaptation to Hyperloop.

The next chapter proposes a Safety Approval Process for the forms of Guided Transportation considered in this paper.

5. Proposed Safety Approval Process for Guided transportation

The CENELEC safety standards have been mandatory within the railway domain for many years. The authors of this paper have also several years of experience as ISAs, assessing compliance against the requirements from these safety standards. These safety standards include quite detailed requirements to the activities and documentation to be produced and require that the safety documentation is collected in a top-level document, denoted safety case. It is the view of the authors that the advantage of standardizing the activities to be performed and the documentation to be produced in such level of details is that a minimum level of quality of the performed activities and produced documentation can be achieved to a greater degree. Such level of details also facilitates the achievement of consistency across different projects (different systems, different actors etc.) in terms of the activities performed and documentation produced. In contrast, the common method safety regulation, (EU) 2015/1136 and (EU) No 402/2013, provides much larger degrees of freedom regarding the activities to be performed and the documentation to be produced. In this, case the quality of performed activities and produced documentation is more reliant on the competence of the actors involved; those performing the activities and producing documentation but also the Assessment body.

It is proposed in this paper that the safety documentation for railway, metro, hyperloop and urban guided transport is collected in a safety

case. Collecting the safety documentation in a safety case, is not currently only practiced within railway, metro and urban guided transport, but also practiced within the road vehicles domain (see standard ISO 26262) and within defense (see standard Def Stan 00-56).

The proposed Safety Approval Process for development of new products and system is briefly described in the following manner:

- Development should be performed according to the requirements of EN 50126:2017. We propose an agnostic approach regarding lifecycles. In the waterfall paper by Royce (1970) h states " I believe in this concept, but the implementation described above is risky and invites failure". EN 50128:2011 states in chapter 5.3.2.14 "Where any alternative lifecycle or documentation structure is adopted it shall be established that it meets all the objectives and requirements of this European Standard.". New lifecycles for the safety domain has also been developed See Hanssen et al (2018) .This agnostic approach has also been followed in UL 4600:2019draft.
- Software development could be performed according to requirements of EN 50128:2011 with some adaptations. Missing and weak points like AI (Artificial Intelligence), OTA (Over The Air) deployment and distributed development should be included. We propose an agnostic approach regarding lifecycles. The standard itself states that it does not mandate the use of a particular software development lifecycle. We propose that the roles described in the standard could be relaxed as long as the requirements are complied with. Our proposition is to follow a goal based approach and to open the possibility for the suppliers/manufacturers to follow modern software development processes.
- Relevant testing and assessment bodies like testing laboratories, ISA and NoBo could be accredited to ensure both effective and trustworthy certifications.
- Collection of safety documentation within a safety case. Hierarchical structuring of safety documentation. The safety documentation structured in an agile safety case (see Myklebust T. et al 2018) together with a re-use of documentation/information approach. An agile safety case improves the process by inserting information when available, includes all relevant agile practices relevant for the project and is aligned with an agile and DevOps approach.
- Assessment of safety documentation collected in a safety case by an ISA and software documentation by an assessor.

There exist already frameworks for taking care of cyber security, e.g. the NIST framework (NIST 2020) and the IEC 62443 standard series. All parts of the series have not been finalized. We are aware of the ongoing EN TS/TR 50701:2019draft work by CENELEC. This document could preferably include only adaptations of NIST and the IEC 62443 series to guided transportation.

6. Conclusion

We have proposed the initial steps of a Safety Approval Process for the main forms of Guided Transportation including the following: railway, metro, urban guided transport and Hyperloop. The proposed Safety Approval Process is based on requirements and the authors' experience from the railway domain but with a few suggestions of modifications (related to the rigidity of required activities, roles and documentation). The railway domain is chosen due to its well-established Safety Approval Process but also well-established technology.

Further research is needed in order to refine (increasing level of details) and to validate the proposed safety approval process.

References

Coineau D. (2012, August). MODSAFE Glossary, D10.5, v.13.

Commission Notice - The 'Blue Guide' on the implementation of EU products rules 2016.

Delft Hyperloop (2019, June). The Future of Hyperloop.

Forskrift om krav til sporvei, tunnelbane, forstadsbane m.m (kravforskriften), FOR-2014-12-10-1572.

Myklebust T. and Stålhane T. (2018). The Agile Safety Case, Springer, ISBN 978-3-319-70264-3

NIST Cybersecurity framework edition 1.1 (2020)

Otegui J., et. al. (2017). A Survey of Train Positioning Solutions, IEEE Sensors Journal, Vol. 17, No. 20, October 15, 2017, pp. 6788-6797

Transportstyrelsens föreskrifter om godkännande av spåranläggning eller fordon för tunnelbana och spårväg. TSFS 2010:115.

Website for Service Technique des Remontées Mécaniques et des Transports Guidés (STRMTG), www.strmtg.developpement-durable.gouv.fr/en/urban-guided-transport-in-france-r25.html, visited 2019-08-13.

W. Royce. Managing the development of large software systems (1970)

G. K. Hanssen, T. Stålhane and T. Myklebust. SafeScrum – Agile Development of Safety-Critical Software. Springer December 2018.