Working Paper #2:

Safety Assurance Considerations – Blending Transit and Automotive Safety Analysis Methodologies

To the

National Highway Cooperative Research Program (NCHRP)

On project

20-102 (02): Impacts of Laws and Regulations on CV and AV Technology Introduction in Transit Operations

March 2017

From

Kimley-Horn – Douglas Gettman, Ph.D.

Texas Southern University – J. Sam Lott, Principal Investigator

Cambridge Systematics – Tom Harrington, AICP

Table of Contents

List of Appendices

List of Figures

List of Tables

March 2017 Revisions

The following changes have been made to the October 2016 version of this Working Paper #2. This superseding version also has had other minor editorial changes made throughout the document that do not affect meaning.

1. **Forward** – A wholly new insertion of a Forward which will be included in all subsequent Working Papers.
2. **Chapter 1** – Revision and Purpose of the Study has been revised to match other working papers.
3. **Chapter 4** – Addition of text identifying importance of ASCE-21 with respect to MIL Std 882E.
4. **Chapter 4** – Insertion of explanations of ASCE-21 identification of unacceptable hazardous conditions for Automatic Train Control systems.
5. **Chapter 4** – Include in footnote 13 the fact that IEC 62278 is identical to EN50126
6. **Chapter 4** – Addition of new subsection – Enhancement of System Safety Assurance Process through EN50126 Safety Case Approach
7. **Chapter 5** – Rewording of footnote 18 to identify "current industry discussions"
8. **Chapter 6** – Addition of new subsection at the end of the chapter -- Recommended Research Projects on AV Transit Safety.

Acknowledgements

A special contribution to the content of the working paper was made by members of the ASCE-21 Automated People Mover Standard Committee's Safety Working Group. Materials and graphical information prepared during the ASCE-21's Safety Group normal deliberations was made available for the author's use. Contributors to the information on transit system safety methodologies in the main body of the working paper, and specifically to Appendix C were:

Sue Cox – Safetywright Inc.

Michael Kingsley – Rockwell Automation

Cindy Sugimoto – Lea + Elliott, Inc.

These contributors are greatly appreciated, and should be noted that the use of their information does not necessarily indicate that they are in complete agreement with the contents herein.

Foreword

This working paper uses the following terminology and focus of its content in a manner consistent with all the associated working papers of the NCHRP 20-102(02) project.

Definition of Automated Vehicle (AV) Transit – The "system" comprising AV Transit includes:

1) Driving automation system(s) and technology per SAE J3016[1]
   a) Other vehicle systems and components which provide driver assistance such as lane departure warning when a human driver is performing the dynamic driving task (DDT) from inside the vehicle or from a remote location; and
2) Other monitoring, supervisory control and passenger safety systems, technologies and facilities necessary for public transit service, such as precision docking, automated door operation, and dispatch functions.

Definition of Transit Vehicle Operator – The typical term used to identify the person operating a transit vehicle is the "vehicle operator". However, under SAE J3016 definitions and terminology, a human "driver" is the person who manually exercises in-vehicle braking, accelerating, steering, and transmission gear selection input devices to operate a vehicle. Considering the SAE standard's intent to define terms for driving automation systems only, the term vehicle driver is specified. In the working papers, the terms vehicle driver and vehicle operator may be used interchangeably, depending on the context and point of emphasis. Likewise, the terms "remote driver" (per SAE J3016) and "remote operator" will likewise be used interchangeably.

Definition of Transit Operating Agency – Transit operating agencies can be any type of public, governmental or non-profit entity, such as transit authorities created with certain governmental responsibilities; municipal, county and state government public transportation departments; medical/educational institutions; and local management authorities/districts.

Focused Nature of the Working Papers – Each working paper has a focused purpose and is not intended to provide a comprehensive set of steps, actions or preparations encompassing the full evolution of AV Transit technology applications in public transit service. Some aspects of this project's research have focused more on the ultimate operating conditions when AV technology is fully mature to understand the long term, ultimate state of automated transit technology, policy and regulations.

Conclusions on AV Transit in the Final Report – The Final Report will address information on the probable benefits and impacts of AV Transit, as well as articulate a roadmap of further research activities that technology, policy and regulations should follow over the next few decades.

[1] SAE J3016 is the Society of Automotive Engineers Standard titled – Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles; revised September 30, 2016.

1. Introduction to Automated Roadway Vehicle Transit Safety

Major advances in robotics, artificial intelligence, sensors, and processing technology are driving the automotive industry toward fully automated vehicles (AV) operating along all types of roadway systems. These advances offer significant opportunities to improve transit services by reducing cost, extending reach, and improving safety of transit vehicles.

A common theme within the evolving AV industry has been the challenges of providing a safe design for all operating environments within the generally-understood goal of exceeding the comparative safety of human-operated vehicles.

The historical development of safety analysis methodologies within the transit industry and within the automotive industry have followed different paths. This working paper defines these two general methodologies considering the recently announced safety program initiatives of the National Highway Traffic Safety Administration (NHTSA) and the Federal Transit Administration (FTA), and discusses the potential for a new blended approach to provide safety assurance for AV transit applications.

Introduction to Safety Analysis

The field of analyzing safety on a system level has been an evolving area of science, engineering and technology for the past 100 years. This engineering field has matured within the military/avionics/aerospace industry starting in the World War II era.

Designing for such complex systems is in the field generally classified as **systems engineering**. Within this broad field, the analysis of operational conditions, system failures and the related safety concerns inherently involves a specialized sub-field called **safety and reliability engineering** that analyzes system Reliability, Availability, Maintainability and Safety (RAMS).

In the discussion of the methodologies for safety analysis that follow, there is a distinction made between **safety certification** and **safety assurance**. *Safety certification* typically is provided through an approach called **Functional Safety** that is integral to the design process of various components,

The levels of automation referenced herein are taken from – the Society of Automotive Engineers in SAE J3016.

- **Level 0** – the human driver does everything.
- **Level 1** – an automated system on the vehicle can *sometimes assist* the human driver conduct *some parts of* the driving task.
- **Level 2** – an automated system on the vehicle can *conduct* some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task.
- **Level 3** – an automated system can both conduct some parts of the driving task and monitor the driving environment *in some instances*, but the human driver must be ready to take back control when the automated system requests.
- **Level 4** – an automated system can conduct the driving task and monitor the driving environment, and the human need not take back control, but the automated system can operate only in certain environments and under certain conditions.
- **Level 5** – the automated system can perform all driving tasks, under all conditions that a human driver could perform them.

NOTE: These levels of driving automation will be referred to in this document as **L1**, **L2**, **L3**, **L4** and **L5**.

assemblies and subsystems/systems which are typically a product supplied by a manufacturer. In comparison, *safety assurance* describes a process of safety management tasks and responsibilities built on a foundation of a structured analysis of hazards and the associated assessment of risk.

Safety certification has liability/legal connotations involving the supply of a product(s), whereas safety assurance is a responsibility of the owner/operator of the system in which these products are operating.

The discussions that follow compare the ways that both the automotive industry and the transit industry have approached the process of analyzing a system's failure and/or possible operation within a hazardous situation, and assessing the resulting risks and public safety implications such that safety can be assured. Each chapter describes the sources of the methodologies, and the differences between the focus and approach with vehicle-focused safety analysis versus a system-focused safety analysis.

Ultimately, the introduction of AV technology into transit service requires both transit operating agencies and responsible government entities to become part of the process of determining safety assurance. The automated vehicles are themselves manufactured products, and the supply of these vehicles follows a different process of safety analysis.

Purpose and Organization of the NCHRP 20-102(02) Study

This project identifies a roadmap of activities to be performed by industry groups, legislatures, the federal government, and others that will facilitate automated roadway transit operations. The project is focused on the potential barriers imposed by operating authority policies, agency regulations, and governmental laws relative to the transit environment. Without adjustment, the combination of new technology with old rules could result in undue delays and restrictions to deployment, which reduces the cumulative societal benefits that could have accrued if automated systems technology was implemented earlier.

The project consists of five tasks:

1. Development of a technology baseline for the current state of the practice in AV transit
2. Identification of issues and impacts on transit vehicle driver and associated staff
3. Identification of government regulations and laws impacting AV adoption in transit
4. Development of an implementation plan to address the challenges identified in Tasks 1-3
5. Preparation of a final report consolidating Tasks 1-4

We have organized the five tasks to produce six working papers, and an implementation roadmap for transit automation in the final report. The Working Paper #1 provides an overview of the deployment scenarios for AV technology in transit applications.

Working paper #2 provides a foundation of technical information concerning safety from which subsequent considerations of operating agency policy and governmental safety regulations can be addressed.

Working Papers #3 Workforce Deployment and #4 Operating Agency Policy address the implications of automating roadway transit vehicles with respect to local operating agency issues, including labor relations and training, broad operating planning and policy, and response to governmental laws and regulations.

Working Paper #5 addresses issues and possible changes to the federal and state governmental laws and regulations over public transit that should be researched, as well as issues and possible changes that may be required in vehicle designs to effectively comply with regulations. Finally, Working Paper #6 addresses the preliminary timeline for deployment of progressive transit automation in overall consideration of technology, policy and regulatory changes that will be required.

Then in the final report for the project, an assessment is discussed of the overall benefits and impacts of AV technology on public transit, and a proposed "roadmap" for further research will be described.

Working Paper #2 Contents

The content of this paper is organized to first discuss the new USDOT initiatives in transportation safety in Chapter 2, then followed in Chapters 3 and 4 with an initial framework of vehicle-focused and system-focused safety analyses that will be necessary for AV transit. The discussion in Chapter 5 then addresses a blended approach for both vehicle-focused and system-focused methodologies.

It is noteworthy that safety analyses which focus on the driving automation systems and the other vehicle safety features and systems address only part of the safety realm of transit operations. The greatest contribution of this working paper to the overall pursuit of AV transit systems may be the proposed blending of the different vehicle-focused and system-focused methodologies. For AV transit systems to be successful, the automation technology needs to be able to address the broader role of a transit vehicle's human operator beyond just "driving the bus".

2. USDOT Safety Initiatives

The U.S. Department of Transportation has been actively pursuing technical and policy aspects of safety for automated and connected roadway vehicles over several years. During the authoring of this working paper, NHTSA released specific policy statements and guidance related to automated driving systems. This guidance is summarized and the implications specifically with respect to the safety analysis for public transit applications is discussed in this section.

NHTSA Federal Policy Guidelines for Automated Vehicles

In September of 2016 the National Highway Traffic Safety Administration (NHTSA) of the U.S. Department of Transportation released a major policy document titled Federal Automated Vehicles Policy – Accelerating the Next Revolution in Roadway Safety.[2] The document is described in the Executive Summary as follows (the acronym HAV meaning "highly automated vehicles"):

> *… this Policy sets out an ambitious approach to accelerate the HAV revolution. The remarkable speed with which increasingly complex HAVs are evolving challenges DOT to take new approaches that ensure these technologies are safely introduced (i.e., do not introduce significant new safety risks), provide safety benefits today, and achieve their full safety potential in the future. To meet this challenge, we must rapidly build our expertise and knowledge to keep pace with developments, expand our regulatory capability, and increase our speed of execution.*
>
> *This Policy is an important early step in that effort. We are issuing this Policy as agency guidance rather than in a rulemaking in order to speed the delivery of an initial regulatory framework and best practices to guide manufacturers and other entities in the safe design, development, testing, and deployment of HAVs.*

Levels of Driving Automation – Of importance is the portion of the document that defines what NHTSA considers to comprise HAV technology, now officially recognizing the levels of automated driving as defined by the Society of Automotive Engineers (SAE). The NHTSA policy document identifies HAVs as levels 3-5 in accord with the following definitions:

- At SAE **Level 0**, the human driver does everything;
- At SAE **Level 1**, an automated system on the vehicle can *sometimes assist* the human driver conduct *some parts of* the driving task;
- At SAE **Level 2**, an automated system on the vehicle can *actually conduct* some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task;

[2] http://www.nhtsa.gov/nhtsa/av/

- At SAE **Level 3**, an automated system can both actually conduct some parts of the driving task and monitor the driving environment *in some instances*, but the human driver must be ready to take back control when the automated system requests;
- At SAE **Level 4**, an automated system can conduct the driving task and monitor the driving environment, and the human need not take back control, but the automated system can operate only in certain environments and under certain conditions; and
- At SAE **Level 5**, the automated system can perform all driving tasks, under all conditions that a human driver could perform them.

Federal Motor Vehicle Safety Standards and Regulations – Since the 1970s the National Highway Traffic Safety Administration (NHTSA) has been establishing and maintaining safety standards known as the Federal Motor Vehicle Safety Standards and Regulations (FMVSS) for the automobile industry in the United States[3]. Other countries around the world have followed suit with their own very similar safety requirements. As summarized in the referenced article, the three series of automobile safety requirements that are best known are as follows:

1. Crash avoidance (100-series)
2. Crashworthiness (200-series)
3. Post-crash survivability (300-series)

These standards also address the requirements for some specific parts (such as brake hoses), as well as the better-known standards for crashworthiness and crash survivability. The standards are maintained and compliance is monitored by NHTSA. There are multiple additional standards for miscellaneous items such as fuels, manufacturer and vehicle identification, seat belts, dashboard instrument lighting, and so on.

NHTSA also has defined a battery of tests and test acceptance criteria to monitor compliance with the FMVSS. NHTSA performs tests and rates the demonstration of compliance of every vehicle model sold in the United States though a five-star rating system. These traditional safety requirements will likely be gradually expanded to include HAV technology safety tests.

Currently, a process is underway to assess the applicability of FMVSS standards to AV technology[4]. Through this ongoing review process, NHTSA is identifying which standards may need to be changed to properly address highly automated roadway vehicles, as well as identifying what new FMVSS standards will need to be added to test and confirm the adequate safe design of both light and heavy vehicle AV products and other automation conversions (such as aftermarket AV "kits") that will likely be brought to the US marketplace.

Safe Design of Highly Automated Vehicles (HAVs) – NHTSA has made the following statement in the September 2016 policy document (p. 11, ref. footnote 1. above) concerning the self-certification of safety by HAV developers/manufacturers. It should be noted that with

[3] James Martin, et al; University of North Carolina, Certification for Autonomous Vehicles https://www.cs.unc.edu/~anderson/teach/comp790a/certification.pdf

[4] http://ntl.bts.gov/lib/57000/57000/57076/Review_FMVSS_AV_Scan.pdf

respect to the safe design of AV technology for any type of public roadway testing and deployment, NHTSA retains the requirements for compliance with the FMVSS.

> *Under current law, manufacturers bear the responsibility to self-certify that all of the vehicles they manufacture for use on public roadways comply with all applicable Federal Motor Vehicle Safety Standards (FMVSS). Therefore, if a vehicle is compliant within the existing FMVSS regulatory framework and maintains a conventional vehicle design, there is currently no specific federal legal barrier to an HAV being offered for sale.*
>
> *However, manufacturers and other entities designing new automated vehicle systems are subject to NHTSA's defects, recall and enforcement authority. DOT anticipates that manufacturers and other entities planning to test and deploy HAVs will use this Guidance, industry standards and best practices to ensure that their systems will be reasonably safe under real-world conditions.*

In establishing a framework within which each vehicle developer/manufacturer is to design for safe HAV operations, the September 2016 policy document identifies these three realms of guidance for design performance (Figure **1**):

- **NHTSA Guidance** – Scope and process
- **Automation Functional Key Areas** – Specific to each HAV system
- **Cross-Cutting Areas** – Applicable across all automated equipment/subsystems

The *operational design domain* (ODD) defines a particularly relevant set of criteria which is discussed further in Chapter 5 with respect to considerations for HAV applications in public transit service. Also important is the definition NHTSA gives to the "*fall back minimum risk condition*":

> *The fall back minimal risk condition portion of the framework is also specific to each HAV system. Defining, testing, and validating a fall back minimal risk condition ensures that the vehicle can be put in a minimal risk condition in cases of HAV system failure or a failure in a human driver's response when transitioning from automated to manual control.*

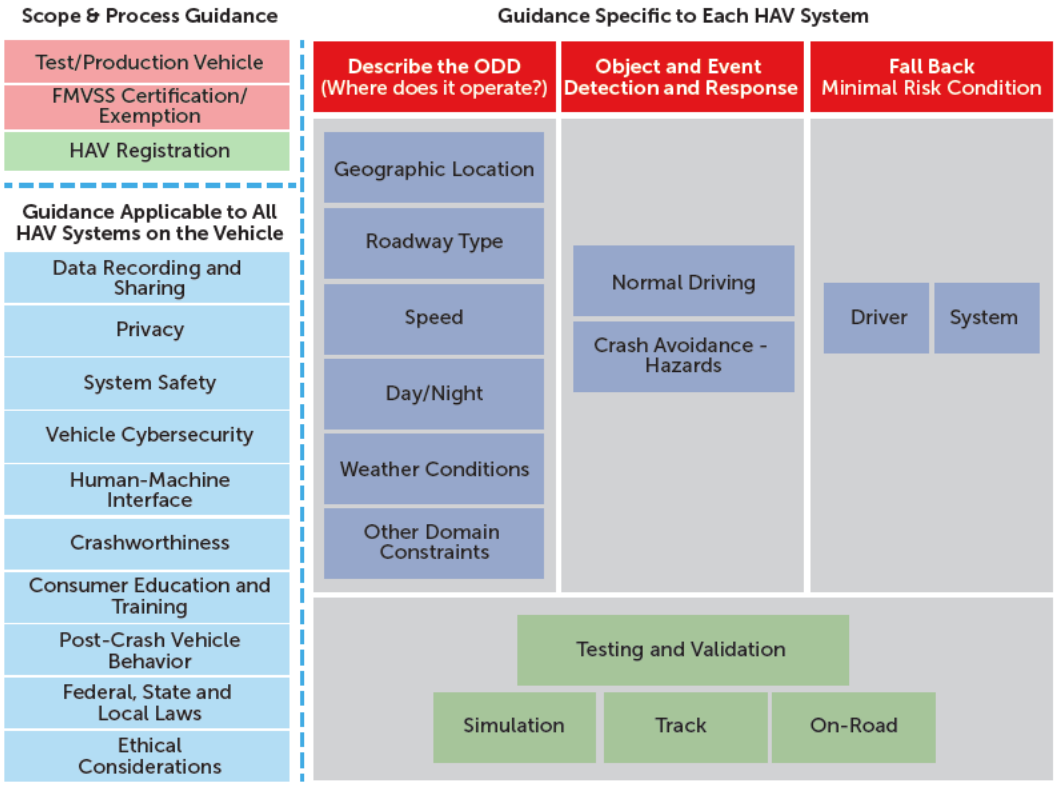

Figure 1. NHTSA Framework for Guidance of and Safe HAV Design Performance

Several important articles and reports have been referenced in the NHTSA policy document, including published articles by automobile manufacturers active in the CAMP Consortium[5]. Also, particularly noteworthy are several NHTSA reports that are specifically addressing **electronic control systems** for vehicle automation.

- USDOT/NHTSA Report to Congress: "Electronic Systems Performance in Passenger Motor Vehicles"
  http://www.nhtsa.gov/Laws-&-Regulations/NHTSA-Reports-Sent-To-Congress
- Assessment of Safety Standards for Automotive Electronic Control Systems
  http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2016/812285_ElectronicsReliabilityReport.pdf

These technical documents provide valuable information on safety methodologies and processes that provide a benchmark for continuing decisions by NHTSA as it moves toward rulemaking changes and additions to its safety regulations for HAV roadway vehicles. Further reference to these documents is given in Chapter 3.

[5] CAMP – Crash Avoidance Metrics Partnership (CAMP) Automated Vehicle Research (AVR) Consortium
http://www-esv.nhtsa.dot.gov/Proceedings/24/files/24ESV-000451.PDF

Model State Policy – Included in the NHTSA Federal Automated Vehicles Policy statement is a section that identifies "model" policy for individual state governments with respect to highway safety laws and roadway design requirements that accommodate HAV technology – either in *testing* or *deployment*. The definition of these terms is given in the Policy document's introduction to the Model State Policy, as follows (emphasis added by the authors of this report):

> *The following sections describe a model regulatory framework for States that wish to regulate procedures and conditions for testing, deployment, and operation of HAVs. For purposes of this section, "**testing**" refers to analyses and evaluations of HAV systems and vehicles conducted by a researcher, manufacturer, entity, or expert third party at the request of one of those entities. "**Deployment**" refers to use of HAV systems and vehicles by members of the public who are not employees or agents of researchers, manufacturers, or other entities. For purposes of State traffic laws that apply to drivers of vehicles (e.g., speed limits, traffic signs), States may wish to deem an HAV system that conducts the driving task and monitors the driving environment (generally SAE Levels 3-5) to be the "driver" of the vehicle. For vehicles and circumstances in which a human is primarily responsible for monitoring the driving environment (generally SAE Levels 1-2), NHTSA recommends the State consider that human to be the driver for purposes of traffic laws and enforcement.*

FTA National Public Transportation Safety Program

The USDOT Federal Transit Administration (FTA) has been preparing for a new Public Transportation Safety Program since 2013 when FTA introduced the transit industry to fundamental changes to the Federal transit safety program authorized by MAP–21. The final rulemaking was published as 49 CFR Part 670 in the August 11, 2016 Federal Register and established the new Safety Program – now in effect as of September12, 2016[6].

Overall, the new rules establish new requirements for Safety Plans and Safety Plan Documentation and Record Keeping, as well as providing more specific guidance for hazard analysis, management and the related risk assessments through a *Safety Management System*.

Safety Management System – One of the central elements of the FTA Safety Program is the new Safety Management System (SMS) framework[7], which has been introduced in 2016 through FTA outreach. SMS is now being publicized and explained by FTA on multiple fronts, beginning with the most safety-critical operations of rail/fixed guideway public transit systems. Applicability to bus operations is also being discussed by FTA with even smaller transit industry bus operators, as noted above. Eventually the SMS framework will be advocated to any size transit operator for application to their entire public transportation service.

[6] https://www.gpo.gov/fdsys/pkg/FR-2016-08-11/pdf/2016-18920.pdf

[7] https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/FTA_SMS_Framework.pdf

The attributes of SMS were described in the SMS Framework document released in 2015, as follows (pp. 1-2):

> *SMS is a formal, top-down, organization-wide approach to managing safety risks and assuring the effectiveness of safety risk mitigations. SMS helps a transit agency focus its safety management efforts by ensuring that:*
>
> 1. *Senior management has access to the information necessary to strategically allocate resources based on the unique safety priorities of the specific transit agency;*
> 2. *Lines of safety decision-making accountability are established throughout the organization to support the resolution of safety concerns and thus promote a proactive safety culture; and*
> 3. *Transit agencies address organizational factors that may lead to safety breakdowns, identify system-wide trends in safety, and manage hazards before they result in accidents or incidents.*
>
> *SMS can be adapted to the mode, size, and complexity of any transit agency in any environment: urban, suburban, or rural. The extent to which SMS processes, activities, and tools are implemented (and documented) will vary from agency to agency. For a small transit operation, SMS processes will likely be straightforward, and activities and tools less burdensome. For a larger transit agency with hundreds or thousands of employees and multiple modes, SMS processes will likely be complex, and activities and tools more resource-intensive.*

An overview of the SMS "components" and "subcomponents" is provided in FTA's SMS framework document (p.4) using the image shown in **Figure 2**. Three implementation phases for SMS within a transit organization are listed as:

- **Phase 1** – Planning, Organization, and Policy Development
- **Phase 2** – Safety Risk Management
- **Phase 3** – Safety Assurance

Of importance to issues regarding automation are the Phase 2 elements of Hazard Identification and Analysis, Safety Risk Evaluation and Mitigation, and related documentation and training of operations staff.

Safety Management Policy	Safety Assurance
1. Safety Management Policy Statement 2. Safety Accountabilities and Responsibilities 3. Integration with Public Safety and Emergency Management 4. SMS Documentation and Records	7. Safety Performance Monitoring and Measurement 8. Management of Change 9. Continuous Improvement
Safety Risk Management	**Safety Promotion**
5. Hazard Identification and Analysis 6. Safety Risk Evaluation	10. Safety Communication 11. Competencies and Training

Figure 2. FTA Safety Management System Components

State Safety and Security Oversight – One of the key tenets of FTA's safety regulations was established 25 years ago when the individual states were given responsibility for safety oversight of fixed guideway and rail systems. In the 1991 Intermodal Surface Transportation Efficiency Act (''ISTEA''), Congress determined that the States, *not FTA*, should be the principal oversight authorities for rail transit within their jurisdictions, given that public transportation is an inherently local activity which, with few exceptions, does not cross state boundaries.

Known as State Safety and Security Oversight (SSO) program, a new Rule 49 CFR Part 674 was finalized in March 2016 that provides the latest update to the requirements[8]. Under this regulation, each state is required to identify a State Safety Oversight Agency (SSOA), examples of which are the Public Utility Commission in California and the Department of Transportation in Florida.

Part 674 describes the minimum responsibilities of a state's SSO program as follows:

a) *Explicitly acknowledge the State's responsibility for overseeing the safety of the rail fixed guideway public transportation systems within the State;*
b) *Demonstrate the State's ability to adopt and enforce Federal and relevant State law for safety in rail fixed guideway public transportation systems;*
c) *Establish a State safety oversight agency, by State law, in accordance with the requirements of 49 U.S.C. 5329(e) and this part;*
d) *Demonstrate that the State has determined an appropriate staffing level for the State safety oversight agency commensurate with the number, size, and complexity of the rail*

[8] https://www.gpo.gov/fdsys/pkg/FR-2016-03-16/pdf/2016-05489.pdf
A history of the related federal regulations is covered first in the Federal Register record, followed by commentary on comments received to the proposed rulemaking. The actual new Part 674 begins on page 28 of the pdf document.

fixed guideway public transportation systems in the State, and that the State has consulted with the Administrator for that purpose;

e) *Demonstrate that the employees and other personnel of the State safety oversight agency who are responsible for the oversight of rail fixed guideway public transportation systems are qualified to perform their functions, based on appropriate training, including substantial progress toward or completion of the Public Transportation Safety Certification Training Program; and*

f) *Demonstrate that by law, the State prohibits any public transportation agency in the State from providing funds to the SSOA.*

It is important to note that these responsibilities of each state are separate and apart from the responsibilities laid out in the "Model State Policy" that NHTSA has described in its recent Federal Automated Vehicle Policy.

These USDOT policy, design and manufacturing guidance and safety regulations provide important background information for the discussion of the two safety analysis methodologies being espoused in the regulatory content between NHSTA and FTA – a vehicle-focused methodology and a system focused methodology.

3. Vehicle-Focused Safety Standards and Methodologies

NHTSA has been comparing and assessing the attributes of several safety standards, methodologies and guidelines as they progress toward becoming the regulator of the various levels of AV technology automation. Their specific focus has been on the electronic and computer systems that assume the decision-making process for driving the AV along its path. The three primary safety analysis process standards that have been analyzed in multiple NHTSA reports are described below:[9]

MIL-STD-882E: Department of Defense Standard Practice, System Safety – This system safety standard practice identifies the Department of Defense systems engineering approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. MIL-STD-882E is a required practice as part of military systems automation design.

DO-178C: Software Considerations in Airborne Systems and Equipment Certification – This is an industry-accepted guidance for software in airborne systems and equipment used in the Aviation industry. With the earlier advancement of flight control automation and the important lessons learned within avionics, this standard for automation control software is an important reference for NHTSA.

ISO 26262: Road Vehicles, Functional Safety – This *voluntary* industry standard is the first comprehensive and voluntary automotive safety standard that addresses the functional safety of electrical and/or electronic (E/E) and software-intensive features in road vehicles. ISO26262 has been developed from the original IEC 61508 machine automation safety standards and from other machine automation safety standards for different manufacturing industries. ISO26262 is a key element of SAE automotive safety standards.

See **Appendix A** for a summary of the NHTSA comparison between these primary safety standards[10], and two other software oriented standards: AUTOSAR – Automotive Open System Architecture, and MISRA C – Guidelines for the Use of the C Language in Critical Systems.

[9] Text combined from the descriptions found to NHTSA reports, with web links provided in Section 1 above – see page 2 in NHTSA Assessment of Safety Standards for Automotive Electronic Control Systems, and pp. 7-9 in NHTSA Report to Congress: "Electronic Systems Performance in Passenger Motor Vehicles".

[10] Appendix: Summary of Standards Comparison; NHTSA Assessment of Safety Standards for Automotive Electronic Control Systems; DOT HS 812 285, June 2016

Machine Automation Functional Safety Standards

In the *automated guideway* transit industry, there has been a growing interest in the application of a **functional approach** to defining and analyzing safety of the equipment and subsystems. IEC 61508 – Functional System Safety defines Functional Safety in terms of the requirements and analysis methodologies for electrical/electronic/ programmable electronic (E/E/PE) safety-related systems. This is a product design standard that has had major impact on the automotive industry, and by extension the future safety standards for AV Transit.

IEC 61508 Functional Safety of Electrical/Electronic/ Programmable Electronic Safety–Related Systems provides detailed guidance for every aspect of the safety design lifecycle:

- **Part-1** – General Requirements
- **Part-2** – Hardware Requirements for (E/E/PE) safety-related systems
- **Part-3** – Software requirements
- **Part-4** – Definitions and abbreviations
- **Part-5** – Examples of methods for the determination of safety integrity levels
- **Part-6** – Guidelines on the application of IEC 61508-2 and IEC 61508-3
- **Part-7** – Overview of techniques and measures

Safety Integrity Levels (SIL) – One of the most important contributions of the IEC 61508 functional safety standard was the concept of *safety integrity levels (SILs)*. This use of SIL criteria to define functional safety is specifically oriented toward manufactured products that have specific product design requirements that must be met. Within the 61508 framework, the assessment of safe design must be **certifiable** for specific components, assemblies/subsystems and entire electronic/programmable control systems. SIL ratings are used to specify the target level of safety integrity.

A benefit is that the approach using quantifiable SIL criteria makes failure rate probability calculations easier for third party verification and validation. Through commercial use of the IEC 61508 standards-based analysis methodology, off-the-shelf supply of pre-certified components can be established.

In general, the SIL criteria for safety analysis must consider the following factors:

1. **Failure rates** for elements of each automated control subsystem
2. Level of element **redundancy** with **identical or diverse** design
3. Failure of redundant elements due to a **common cause**
4. The control system's ability to **"detect" identified failures**

Safety integrity levels are defined as **order-of-magnitude levels of risk reduction** defined in terms of Average Probability of Dangerous Failures per hour. The IEC 61508 standard lists the following defining limits for the SIL values as a function of "PHF" criteria – Average frequency of a dangerous failure of the safety function [b^{-1}], i.e. dangerous failures per hour.

SIL 1 $\geq 10^{-6}$ to $< 10^{-5}$

SIL 2 $\geq 10^{-7}$ to $< 10^{-6}$

SIL 3 $\geq 10^{-8}$ to $< 10^{-7}$

SIL 4 $\geq 10^{-9}$ to $< 10^{-8}$

Other industry-sector standards provide automation safety guidance for a particular industry application as an extension of IEC 61508:

- IEC 61511 – Process Industry Sector: Petrochemical, pharmaceutical, power generation
- IEC 62061, ISO 13849 – Machinery Sector: Industrial machinery and robotic systems, automated guided vehicles
- IEC 61800-5-2 Adjustable Speed Electrical Drive Systems

ISO 26262 Road Vehicles – Functional Safety

The automotive industry has also applied the SIL methodology in a comprehensive manner using specific Automotive Safety Integrity Levels (ASIL) criteria in ISO 26262. Note again that ISO 26262 is one of the key safety standards that NHTSA has been evaluating as part of the Model Policy and regulatory role.

The ten parts of ISO 26262 include:

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level
6. Product development at the software level
7. Production and operation
8. Supporting processes
9. Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis
10. Guideline on ISO 26262

This automotive safety standard is specifically defined from the overall framework of functional safety methodologies defined in IEC 61508. Automotive Industry applications of ISO 26262 are being used internationally and adopted by the Society of Automotive Engineers (SAE). These vehicle-focused safety methodologies are highly relevant to connected and automated vehicle technology development and manufacturing, including the supply of public transit vehicles.

The attributes of the ISO 26262 functional safety standard for road vehicles will be addressed from this point on under through the continuing discussion of “The Society of Automotive Engineers standards”. For further details in the assessment of ISO 26262 by NHTSA refer to **Appendix A**.

Standards Program of the Society of Automotive Engineers

A series of new standards under the auspices of the Society of Automotive Engineers (SAE) have been in development for several years which are intended for application to AV technology. Some of these standards deal with communications links for inter-vehicle communications and for vehicle-to-roadway infrastructure and internet "cloud-based" functionality.

The areas of work in which specific standards are being formulated were identified in a presentation given at the 2016 TRB/AUVSI Automated Vehicle Symposium[11] in two topical groups of standards. The Part 1 topical group comprises 16 standards covering Terms & Definitions; Interoperability; and Vehicle & System Performance Requirements. Within this Part 1 group, standards are being developed on topics such as (selected examples):

- Automatic Emergency Braking Test Methods and Performance Assessment (SAE J3097)
- Automated Driving Reference Architecture (SAE J3131)
- Automated Vehicles Definitions: Key Terms Related to Human Interaction with Automated Driving Systems (SAE J3088)

Part 2 topical group deals specifically with safety, and has sub-groupings of Functional Safety; Safety & Reliability; Active Safety; Safety & Human Factors; and Other Safety. Selected examples from Part 2 are:

- Design FMEA (Potential Failure Mode & Effect Analysis) and Process FMEA (SAE J1739)
- Adaptive Cruise Control Operating Characteristics & User Interface (SAE J2399)
- DSRC Requirements for V2V Safety Awareness (SAE J2945/2)
- Recommended Practices for Signal Preemption Message Development (SAE J2945/10)

Product Orientation of Vehicle-Focused Safety Methodology

NHTSA has embraced the SAE standards program as a key element of the USDOT policy for highly automated vehicles. Therefore, it is anticipated that the vehicle manufacturers will be using these standards as the primary source of the vehicle-focused safety methodology from this point-in-time forward, within the functional safety framework based on ISO 26262.

By utilizing this set of standards for functional safety that allow a more precise and "transferable" calculation of the SIL level for components, assemblies and subsystems, manufacturers of AVs can supply products that are certifiable with respect to their safe design.

With this expectation of product certification, it is important to consider that the safety integrity levels and the associated methodologies are *product oriented*, and as such have "safety" criteria defined by design objectives and product failure norms. Per the NHTSA report

[11] https://higherlogicdownload.s3.amazonaws.com/AUVSI/14c12c18-fde1-4c1d-8548-035ad166c766/UploadedImages/documents/Weds/1100-1115%20Jack%20Pokrzywa.pdf

referenced above[12], the definitions of safety in ISO 26262 are the "absence of unreasonable risk." The definition of hazards are based on operating conditions for the manufactured components, assemblies and control systems – conditions in which failures are characterized by control system response that has "unintended behavior of an item with respect to its design intent." Although such criteria is appropriate for mass produced AV automotive products and other such automated machinery, it is different from the transit system-focused methodologies discussed in the next Chapter.

[12] Table 1 Definition of Safety and Hazard, p. 11; NHTSA Assessment of Safety Standards for Automotive Electronic Control Systems; DOT HS 812 285, June 2016

4. Transit System-Focused Safety Standards and Methodologies

The operation of roadway transit vehicles without a human operator or an attendant onboard is a complete paradigm shift from current roadway vehicle transit operations in the United States. Local transit operating agencies will need to bring wholly new levels of safety assessments into place as AV transit technology matures.

The new initiatives by FTA to emphasize Safety Management Systems are timely in that they begin to create a safety culture within each transit operating agency and authority. However, the details of the FTA requirements within the SMS framework are mostly in the form of guidelines which generally have intended application to fixed guideway/rail systems. The applicability of SMS methodologies to bus operating agencies is also highly relevant – especially with respect to safety risks of transit vehicle interactions with pedestrians and other traffic.

In addition, there are several existing and compatible standards for fully automated guideway transit systems which include safety analysis methodologies. These standards covering automated fixed guideway transit have been developed generally as consensus standards drawing from the experience of the automated fixed guideway transit industry over the last 50 years. Worldwide there are many automated people mover systems operating in major airports and major activity centers, as well as a growing number of regional metro systems that operate without any driver or attendant onboard. Most of these systems have been designed using the standards discussed in this section.

Some of these safety methodologies have been developed and applied for application through *progressive levels of automation*. This is particularly relevant to AV transit as the transition from pure human driver operation to completely self-driving invokes new levels of safety concerns to be addressed in the system/equipment design and operating plans.

To put the topic of system-level safety analysis in perspective, it is helpful to understand that the systems engineering practices and the related safety engineering methodologies generally referenced in the fixed guideway transit industry have been drawn from the standards guiding the automation of military and avionics systems over the past 50 years. Military and avionics/aerospace systems began to become increasingly sophisticated following World War II when the initial research began for the U.S. space program. The transit industry was simultaneously advancing the applications of automated systems when the first fully automated transit systems were deployed in the 1960s.

Safety engineering in these parallel fields began with a principle focus on the hazardous implications of failure modes which could result in “catastrophic” accidents. Safety was viewed in this context to assess and mitigate the risks of serious equipment damage, personal injury or fatalities resulting from such hazardous conditions.

MIL Standard 882

The approach to safety defined by MIL Std. 882 starts with a *Hazard Analysis* process that can begin in an early conceptual stage. Hazard Analysis combines the severity of the accident and

the probability of occurrence of the hazard to create the risk index for the system. The most recent versions of MIL Std. 882 add considerable information about the safety analyses of *software* from its importance in the control of the system – defined as a "software control category."

The FTA began to adapt the processes and methodologies of the military programs as the safety analysis of transit systems began to match the complexities of aerospace systems. During the 1980s and 1990s MIL Std. 882B and its successor 882C (i.e., version "C") became a specific document that transit agencies and system designers/suppliers called for in technical specifications and project requirements.

The "system-level" approach to a safety analysis from MIL Std. 882C System Safety Program Requirements proved very effective for guiding the increasingly more automated train control technologies that were being applied in the fixed guideway transit industry during the 1970s, 80s and 90s. However, the U.S. Military was not constrained to maintain a fixed version of the standard and superseding versions that followed 882C began to address military applications and equipment more explicitly in the text and tables/figures. Thus the "C" version of the standard became obsolete for military purposes and it was soon no longer being published or used – other than within the transit industry.

System-Focused Risk Assessment and Hazard Resolution Process – The Automated People Mover Standards Committee of the American Society of Civil Engineers (ASCE) determined in the review process for the 2005 update to ASCE 21 there was a need to codify the processes of MIL Std. 882C as it had been applied to transit systems in a manner that disconnected the text from the continually evolving Military Standards process. Because of this initiative, the essential content of MIL Std. 882C was adapted to a specific application for purposes of the APM Standard, and included in the ASCE-21 as Annex A: System Safety Program Requirements.

The System Safety Program (Annex A) of the APM Standards now covers the essential requirements for:

- System Safety Program Plan
- Preliminary Hazard Analysis
- Subsystem Hazard Analysis
- System Hazard Analysis
- Operating and Support Hazard Analysis

A distinguishing characteristic of the system-focused approach to the safety analysis is that the *whole operating system* is addressed, including vehicles, guideways, stations, surrounding right-of-way and all places and ways that people interact with the system. This means that all aspects of the specific site deployment for automated transit technologies must be addressed with each project, and the progressive application of different levels of automation bring different and important dimensions of hazards and risks to the analysis process.

A fundamental distinction of the MIL Std. 882 methodology is the classification of safety in terms of protection from human fatalities, protection from human injury, and protection from

damage to equipment and property. As such, the probability calculations that comprise the analysis process are based on the established list of hazards and the associates risk assessment in terms of the Severity of the consequences and the mean time between hazardous events (MTBHE).

Table 1 illustrates the risk assessment of hazard severity versus probability as used in the ASCE 21 Automated People Mover Standard. The definition of mean time between hazardous event (MTBHE) with respect to the Table **1** criteria is any occurrence of a hazardous event that has catastrophic or critical consequences.

Table 1. Risk Assessment of Hazardous Conditions (Source: ASCE-21 Table 3.1, referencing MIL Std. 882C)

Frequency of Occurrence	Hazard Severity			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A- Frequent	IA	IIA	IIIA	IVA
B- Probable	IB	IIB	IIIB	IVB
C- Occasional	IC	IIC	IIIC	IVC
D- Remote	ID	IID	IIID	IVD
E- Improbable	IE	IIE	IIIE	IVE

- IA, IIA, IIIA, IB, IIB & IC = ***Unacceptable***
- IIIB, IIC, & ID = ***Undesirable*** (allowable with agreement from Authority having jurisdiction)
- IVA, IVB, IIIC, IID, IIID, IE & IIE = ***Acceptable with notification*** to the Authority having jurisdiction
- IIIE, IVC, IVD & IVE = Acceptable

A – Frequent = MTBHE is less than 1000 operating hours.	I – Catastrophic = Death, system loss, or severe environmental damage.
B – Probable = MTBHE is equal to or greater than 1000 operating hours and less than 100,000 operating hours.	II – Critical = Severe Injury, severe occupational illness, major system or environmental damage.
C – Occasional = MTBHE is equal to or greater than 100,000 operating hours and less than 1,000,000 operating hours.	III – Marginal = Minor injury, minor occupational illness, or minor system or environmental damage.
D – Remote = MTBHE is equal to or greater than 1,000,000 operating hours and less than 100,000,000 operating hours.	IV -Negligible = Less than minor injury, occupational illness, or less than minor system or environmental damage.
E – Improbable = MTBHE is equal to or greater than 100,000,000 operating hours.	

Consequences resulting in either death, system loss, or severe environmental damage; or severe injury, severe occupational illness major system damage or major environmental damage. These calculations/assessments of probability are at the heart of the work within the RAMS field of the systems engineering discipline.

The following hierarchy of actions are defined to address hazards (ref. ASCE 21 Section 3.1.2 Hazard Resolution Process):

1. Design to eliminate hazards
2. Design to control hazards
3. Use safety devices
4. Use warning devices
5. Implement special procedures
6. Accept the hazard
7. Eliminate the system, subsystem or equipment

This process includes full documentation of the hazard resolution activities through a *Hazard Tracking System*. This Hazard Tracking System is used to manage and record identified hazards, associated mishaps, risk assessments, identified risk mitigation measures, selected mitigation measures, hazard status, verification of risk reductions, and risk acceptance. This is a document that is maintained from the early design phase of the system notionally updated throughout the lifecycle.

Inherent to the hazard resolution process is the quantification of the risk to determine whether a given system or subsystem needs further mitigation of the potential hazard. By its nature, the field of RAMS engineering requires experience with the realities of the operating world as a basis of the safety assessment when strict quantification of a hazard's probability is not possible. In those cases, there should be a *qualitative* assessment of the hazardous event's probability.

The ASCE-21 APM Standard deals with this reality of qualitative safety assessments in the following manner:

> "It is understood that the quantification of the probability or frequency of occurrence of elements within the safety verification process **may be required to be subjectively (i.e., qualitatively) determined**. All subjectively determined elements shall be identified, and the rationale and justification for the estimation shall be described."

There has been one additional change relevant to the comparisons of earlier and later versions of MIL Std 882 with respect to this table of hazards and risks, and its associated applicability to public transit vs. military systems. The MIL Std 882C criteria incorporated into ASCE-21 classifications of hazards and risks as shown in **Table 1** apply risk categories of Unacceptable, Undesirable, Acceptable with Notification of the Authority having Jurisdiction, and Acceptable. However, there has been a significant revision to the risk assessment and acceptance criteria in the newest version E of MIL Std. 882. For military purposes, the highest risk categories may now be judged to be acceptable, and the term "Unacceptable" has been removed from the table. But now, **Table 1** as given in ASCE-21 which uses the category of "Unacceptable" for

accidents potentially causing injury or fatality remains an important reference for applicability to risk assessment of hazardous conditions in public AV transit systems.

Safety Standards for Software-Controlled Functions – Highly relevant to modern automation technology is the use of computers to control many functions of machines, including some cases even where software performs vital, safety critical functions. In the case of the ASCE 21 APM Standard, several means of using software-based computer controls are identified and discussed in the Section 3.2.3 "Alternatives to Intrinsic Failsafe Design." The "means" identified in this ASCE standard were developed over 15 years ago for software-based microprocessor controls:

- Checked Redundancy
- N-Version Programming (two sets of software logic developed by independent sources)
- Diversity and Self Checking

More recently multiple new standards have been advanced to specifically address safety of software controlled systems, including the latest version of MIL Std. 882E which has a specific section addressing software control functions for military systems.

Also, the avionics industry has produced an important software standard – *DO-178C: Software Considerations in Airborne Systems and Equipment Certification.* Both software standards have been evaluated by NHTSA in the referenced NHTSA report from June 2016 (see the reference above in Chapter 2), and a useful comparison of the basic tenets of each of these standards for electronic and computer processor software controls has been made with ISO 62626 and other software safety standards. This NHTSA comparative summary (extracted from the referenced document) is included in **Appendix A**.

FTA Rules, Methods and Guidelines Drawn from MIL Std. 882

FTA Safety Program Requirements provide a general process that applies to all *rail* transit systems. Drawing from MIL Std. 882, FTA requires that an organized process be undertaken to perform a suitable safety analysis for any transit "system" project as a condition of receiving federal funding.

Rule 49 CFR Part 673 *Public Transportation Agency Safety Plan* establishes the requirements for Safety Plans, Safety Management Systems, and Safety Plan Documentation and Recordkeeping. As part of these updated program requirements, a further structuring of this process has been established under the new Safety Management System requirements (see Chapter 2) in which the conducting of a hazards analysis process is central to the requirements.

Although FTA does not specifically address automated train control or other signaling, communications, electronic subsystems, or software, there are typically other such standards that are identified, such as:

- AREMA Communications and Signals Manual of Recommended Practices
- IEEE 1483 for safety verification

- IEEE 1012 for software Verification & Validation

This process of referring to other standards for complex control system requirements establishes a potential model for the incorporation of AV technology to public transit applications under the FTA guidelines and program requirements.

Automated Guideway Transit System Safety Standards

Much can be gained from the methodologies of several international standards for fully automated guideway transit systems. In fact, there are three distinct sets of standards that have been developed – each of which has international participation in its development and application.

In the United States, a complete functional and operational standard that includes specific safety requirements has been developed under the auspices of the American Society of Civil Engineers (See **Figure 3**). The ASCE 21 Automated People Mover Standard (as discussed above) has had multiple updates of the past 20 years, and continues to be actively improved by representatives from APM technology system suppliers, owner/operator entities, and academia from around the world.

In 2009 the International Electrotechnical Commission (IEC) published a new safety standard for Automated Urban Guided Transport (AUGT) which is structured slightly differently from the ASCE standard (See **Figure 3**). IEC 62267 is specifically directed toward full regional unmanned metro systems.

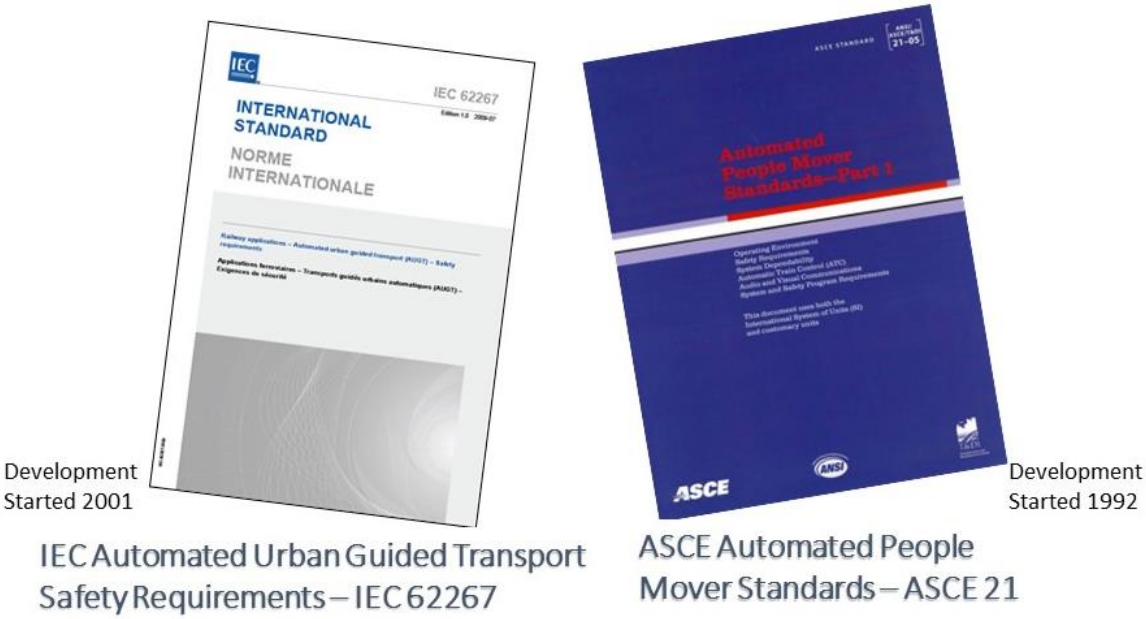

Figure 3. Two International Standards for Fully Automated Guideway Transit Systems

Added to these two international standards are the comprehensive railway system standards prepared and maintained under the European Union's Cenelec EN program. A noted set of related safety guidelines for EN standards are called MOD Safe – Modular Urban Transport Safety and Security Analysis. These guidelines are intended for hazard assessments and safety analyses throughout the life cycle of a transit system.

These consensus standards have been developed with the safety design requirements starting from a hazards analysis during the earliest stage of system design. Each is briefly described below.

ASCE 21 Automated People Mover Standard[13] – The committee that continues to enhance its content and make editorial improvements of the ASCE-21 APM Standard has worked continuously since the first version was published by ASCE in 1996. The work of the committee follows the ASCE standards committee criteria that ensures a balanced consensus process. The standard addresses minimum functional design requirements, safety requirements, acceptance testing requirements and operating requirements for fully automated guideway transit systems. The document has been developed to span as many guideway-based technologies as possible, while still maintaining acceptable requirements for both small and large fully automated systems. Although the committee participation over the last 20 years has had involvement of experts and system suppliers from around the world, the internally referenced standards and government regulations have to this point generally been those developed and applied in the United States.

ASCE 21 is structured around the basic functional subsystems comprising a fully automated fixed guideway transit system. The major chapter titles are as follows:

1. General
2. Operating Environment
3. Safety Requirements
4. System Dependability
5. Automatic Train Control (ATC)
6. Audio and Visual Communications
7. Vehicles
8. Propulsion and Braking
9. Electrical Equipment
10. Stations
11. Guideways
12. Security
13. Emergency Preparedness
14. System Verification and Demonstration

[13] http://ascelibrary.org/doi/book/10.1061/9780784412985

15. Operations, Maintenance, and Training
16. Operational Monitoring

See **Appendix B** for a complete listing of all sections and subsection titles describing the full scope and organization of ASCE 21 APM Standard.

Several aspects of the ASCE-21 standard concerning hazard resolution and safety analyses have been utilized in the discussion above to illustrate the MIL Std. 882 influence on system-focused safety assessments. One particularly noteworthy attribute that ASCE 21 requires that the APM system automatic train control (ATC) system must be designed, installed and operated to meet a specific mean time between hazardous event (MTBHE) requirement.

- Automatic Train Control System MTBHE = one failure in $1x10^8$ operating hours*
  ** This value equals an average of one catastrophic or critical hazardous event/failure every 11,400 years of operations*

There is another standard specifying MTBHE for automated train control system that is referenced in ASCE-21. IEEE Std 1474.1-2004, *IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements* is cited in Section 3.6 of ASCE-21 which identifies an even more stringent requirement for a limited portion of a large-scale CBTC system, as follows:

> *This section specifies a MTBHE of a least 10**9 operating hours for all wayside and train-borne CBTC equipment in a contiguous portion of a one-way route that can be traversed by a train traveling at the specified maximum authorized speed for one hour or less. In addition, the maximum number of trains should be in operation on the segment at their peak operating headway.*

This standard sets a very high bar for system safety within automated transit systems, but one which the automated guideway transit industry has been willing to apply as a basis of ATC design objectives. However, this value does not apply to the operating APM system as a whole.

Figure 4 illustrates this ASCE 21 maximum unsafe failure rate for the ATC system in comparison to the IEC 61508 SIL criteria for functional safety in machine automation – criteria also used in the ISO 26262 safety standard for automobiles. The threshold between SIL 3 and SIL 4 is shown to be the equivalent level of probability of dangerous failure condition that is deemed to be Unacceptable in the transit system-focused methodology prescribed in the ASCE-21 Automated People Mover Standard.

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

ASCE 21 Automatic Train Control MTBHE requirement of one failure in (1 x 10^8) hours, or one failure in 11,415 years

Figure 4. Safety Integrity Levels Defined in IEC 61508 with Comparison to the Mean Time Between Hazardous Events for Automated Train Control Systems in ASCE 21

Appendix C provides a brief comparison of the similarities and differences between ASCE 21, FTA and Cenelec EN standards (both addressed below) in terms of the safety analysis and assessment process requirements in each set of standards. This is useful reference material that has been prepared by the ASCE-21 safety working group for their internal assessments of safety requirements being applied around the world for highly automated transit systems.

IEC 62267 Automated Urban Guided Transport Safety Requirements – This standard was first published in 2009. As the name indicates, this standard for "automated urban guided transport" is intended to address safety requirements for large, urban metro systems and not small scale "people movers". This IEC standard is specifically targeted toward:

> *" … the safety requirements needed to compensate for the absence of a driver or attendant staff who would otherwise be responsible for some or all of train operation functions."*

This limitation of the intended "scope" of the IEC 62267 AUGT safety requirements to only those functions that are assumed by the automation in replacement of a "driver" makes it not directly comparable to standards that encompasses all aspects of an operating transit line – such as ASCE 21. Further, the organization of the IEC standard content is by driver/attendant functions which are assumed by the automated system. Refer the complete table of contents of IEC 62267 in **Appendix D**. The major section titles are as follows:

1.0 Scope
2.0 Normative references
3.0 Terms, definitions and abbreviations
4.0 Methodology
5.0 System description
  5.1 Station
  5.2 Train
  5.3 Guideway between stations
  5.4 System boundaries
6.0 Entities to be protected
  6.1 Persons
  6.2 Property

7.0 Identified hazardous situations and possible safeguards
- 7.1 Supervising guideway
- 7.2 Supervising passenger transfer
- 7.3 Operating a train
- 7.4 Ensuring detection and management of emergency situations

8.0 Safety requirements
- 8.1 General requirements
- 8.2 Monitoring the AUGT system
- 8.3 Operational rules
- 8.4 Safeguards on platforms
- 8.5 Safeguards in trains
- 8.6 Safeguards for passenger transfer area
- 8.7 Safeguards for guideway
- 8.8 Safeguards for transfer areas and depots

9.0 Information for use

10.0 Specific safety requirements for upgrading existing lines to DTO or UTO

11.0 Verification of safety
- 11.1 Documentation and responsibilities
- 11.2 Verification process

An important supplemental safety document to IEC 62267 was published as a separate technical report following the publishing of the standard. This work involved an international working group that developed a consensus statement of a "generic system-level hazard analysis". Published under the same IEC number, the special study document carry's the designation as a "Part 2" technical report – IEC 62267-2.

The following excerpts from the Introduction of the IEC 62267 Part 2 report are very instructive as to the importance of a system level hazard analysis as the first step of any new fully automated transit system project:

> *… this technical report is intended to support Transport Authorities and Safety Regulatory Authorities in hazard identification as well as selecting and combining safeguards as a basis for a specific risk analysis required for any application with regard to their local safety culture. …*
>
> *The hazard analysis and the safeguards derived from it, together with their safety requirements, are based on experiences gained from design and operation of existing AUGT systems in North America, Europe and Asia.*
>
> *The present generic hazard analysis and the derived safety requirements can be seen and used as part of the lifecycle of the system as defined in IEC 62278[14], required for*

[14] The IEC document that is referenced is IEC 62278 Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), and it is essentially identical to EN50126 which is referenced throughout this working paper. The RAMS analyses are dealt with specifically under the progression of a transit system's life-cycle, beginning with the concept, system definitions and conditions of application, risk analysis, and determination of system requirements, then followed by design and implementation, manufacturing, installation and test, operations, performance monitoring and modification/retrofit.

any railway application including AUGT systems. The present hazard analysis covers the required hazard identification as part of risk analysis (lifecycle phase 3) and determination of safety-related system requirements (lifecycle phase 4) on a generic level, which is indispensable for design/implementation of an AUGT system. …
The use of the present hazard analysis and derived methodology can additionally help harmonize the process of specific risk analysis in this field of application. Such a harmonized process has the intention to facilitate the necessary agreements between Transport Authorities and the resulting approval by Safety Regulatory Authorities.

European Standards for Railway Applications – European railway standards called **Cenelec EN standards** address RAMS in an integrated and cohesive manner, and have strong correspondence to many of the IEC standards. Relevant EN standards for fully automated fixed guideway transit systems include:

- CENELEC EN 50126 – Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- CENELEC EN 50128 – Railway Applications – Communications, signaling and processing systems – Software for railway control & protection systems; and
- CENELEC EN 50129 – Railway Applications – Communications, signaling and processing systems – Electronic systems for signaling.

European standards, as well as the IEC standard 62267, are designed specifically to assist operating agencies that have manually or semi-automated railways in the orderly process of migrating them to full automation of the transit line. **Table 2** shows the progressive levels of train automation that is used for railways in Europe (and internationally through the IEC 62267) in accord with the definitions given below.

Table 2. Progressive Levels of Train Automation

EN/IEC Designation of Levels of Train Automation

- TOS – On-Sight Train Operation
- NTO – Non-Automated Train Operation
- STO – Semi-Automated Train Operation
- DTO – Driverless Train Operation
- UTO – Unattended Train Operation

Basic Functions of Train Operation Which Can Be Automated

- Ensuring safe movement of trains
- Driving
- Supervising guideway
- Supervising passenger transfer
- Operating a train
- Ensuring detection and management of emergency situations

Another key difference of the EN safety program in the railway standards when compared to ASCE 21 is that *safety risk is assessed based on functions rather than components* – with similarity to the principles of Functional Safety. The safety criticality of a *function* determines the Tolerable Hazard Rate (THR) for that function, and the corresponding Safety Integrity Level

(SIL) that needs to be achieved. This determines the acceptable failure rates and development processes for the hardware and software that support each function. EN 50129 Annex A includes a Table that defines SILs by quantitative values, which are compatible with IEC 61508 Functional Safety criteria discussed above under machine automation methodologies.

Other differences lie in the hazard risk assessment criteria and residual risk acceptance policy. The hazard risk assessment criteria in EN has a few differences from ASCE 21, with the severity of a single fatality is rated less severe than multiple fatalities, and the risk classifications are grouped differently. When a risk lies between an unacceptable level and a broadly acceptable level, a specific approach is taken to determine whether the risk has been reduced to an acceptable level. This risk acceptance policy is usually specified by the approval authority and in some places is defined by Law within the given jurisdiction.

Safety documentation formats for specific reports are prescribed in EN standards. A Safety Assessment Report by an Independent Safety Assessor (ISA) is also needed to achieve approval of the safety certification. The ISA activities are extensive and are conducted throughout the project life cycle.

All identified hazards are tracked in a hazard log from initial definition with progressive updates through to resolution, and a summary of all safety activities and evidence is compiled into a document called the **Safety Case**.

There is also an EN compatible set of safety assessment and analysis guidelines developed under the auspices of the European Union known as **MOD Safe**, or Modular Urban Transport Safety and Security Analysis. The work evaluated where there were deficiencies of standardization for technical safety functions when applying the safety process over the complete project life cycle and multiple guideline documents have been prepared for progressive use. **Figure 5** shows how the process directed by the MOD Safe guidelines begins with a hazard analysis at the beginning of the project life cycle during the conceptual development stage, as can be seen in the upper-left of the figure.

Process Orientation of System-Focused Safety Methodology

MIL Std. 882 has shaped and influenced essentially all the system oriented safety analysis methodologies that now exist by establishing the **process** for defining the hazards that must be mitigated, and then organizing the continuing process of analyzing, evaluating and assessing the associated risks. Key to the methodology is the classification of risks based on the probability that a human fatality, human injury or significant equipment/system damage could occur.

NHTSA's assessment of electronic control system safety standards concludes that MIL Std. 882 is "not a safety *certification* standard." Rather MIL Std. 882 is a process of safety analysis and documentation that can support appropriate oversight through reviews and audits, while still allowing flexibility to the project program manager and contractors to determine the details

of the safety design[15]. It remains a system-focused safety analysis process that is structured to protect human life and property.

In addition, the NHTSA report from June 2016 that assessed multiple different safety analysis methodologies described the difference between MIL Std. 882 and other methodologies in the following way.

> *ISO 26262 and DO-178C both make safety engineering an integral part of the product development process. On the other hand, MIL-STD-882E specifies a system safety engineering process separate from but parallel to the product development process.*[16]

It is reasonable, therefore, to use a different characterization of the system-focused process of safety analyses and assessments for transit applications of automation technology, when compared with methodologies that focus on the functional safety of machines and manufactured products leading to "safety certification."

Working from the same foundation of MIL Std. 882 methodologies, the FAA defines **Safety Assurance** as a process that evaluates the continued effectiveness of implemented risk control strategies, supporting the identification of new hazards. Working from the same framework of a Safety Management System as the FAA, FTA also uses the term "safety assurance" as the steps taken to resolve hazards after the risks have been defined (refer to **Figure 5**). Therefore "safety assurance" is an appropriate characterization of the process oriented, system-focused methodology that has been described in this chapter. Safety Assurance will be the general term used to identify the system-focused methodology throughout the rest of this working paper, and throughout the remaining project documentation.

[15] P. 23, Section 3.11 Review, Audit, and Certification; NHTSA Assessment of Safety Standards for Automotive Electronic Control Systems; DOT HS 812 285, June 2016

[16] P. 9, Section 3.1.1 Process Prescription, Ibid

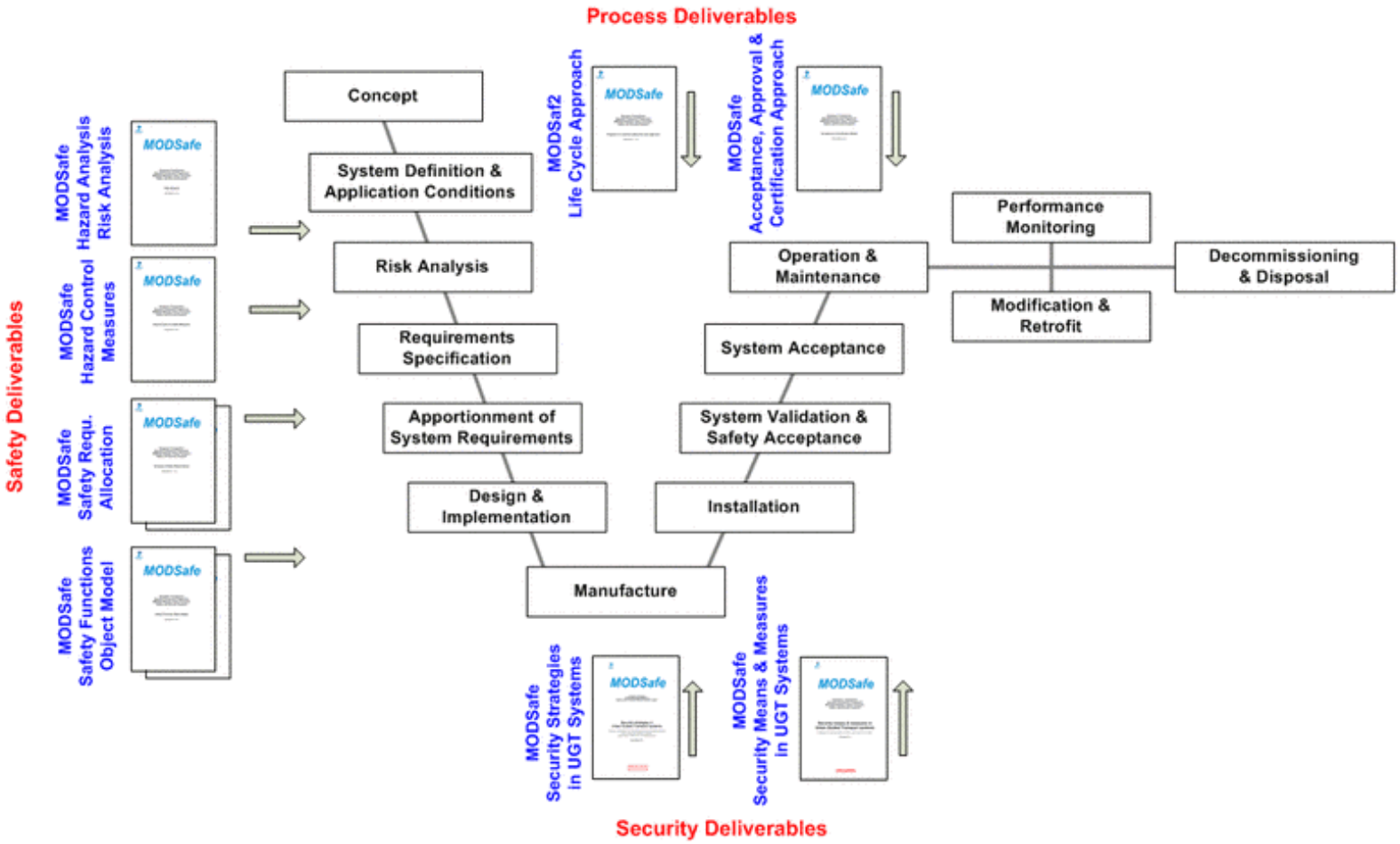

Figure 5. European Union's Life Cycle Approach to Safety Analysis for Automated Railway Systems Through MOD Safe – Modular Urban Transport Safety and Security Analysis

5. Considerations of AV Transit Safety Assurance

The chapters above provide a broad overview of various safety analysis methodologies developed and applied for different sectors of the transportation industry. For consideration of the safety analysis process suitable for AV roadway vehicle technology deployment in public transit service, the focus of the methodology should be placed on the whole operating system throughout the project life-cycle. However, this system focus does not obviate the need for operating vehicles that have been safely designed as products intended for use in public transit service. This process of comprehensive safety assurance methodology means that all aspects of the specific site deployment must be addressed with each project.

Further, there is an important complication to the safety assurance process for AV transit with the reality that there will be a progressive application of different levels of automation, particularly for bus operations. This will inherently create different and important new dimensions of hazards and risks that analysis processes will have to address.

The best approach appears to be a blending of automotive and transit system safety methodologies discussed in the previous chapters. The discussion that follows provides considerations of how these and other factors may play into a comprehensive safety assurance process for AV transit systems.

Detailed discussion of regulatory and safety oversight responsibilities by governmental entities are addressed in Working Paper #5.

Nature of Hazards and Risks in the AV Transit Operating Environment

Each project and local site application of automated roadway vehicles will necessitate specific attention to the operating environment and inherent hazards that could be faced for that specific transit service. Applying an appropriate system safety assurance process is essential, along with the overall planning and execution of the system safety program in accord with the FTA Safety Management System guidelines.

For purposes of this paper, the following discussion is based on the premise that NHTSA will develop an appropriate definition of the form and requirements for safe design of the AV transit vehicles in accord with the new NHTSA policy announcement. As described in Chapter 2, a definition by NHTSA of design criteria for “highly automated vehicles (HAV)” would include the Operational Design Domain (ODD – refer to **Figure 1** above) – operational conditions that also have corresponding vehicle-related failures and hazards for which the vehicle design must safely mitigate. From these requirements, the vehicle manufacturers will assess the probability of a hazardous event occurring from which unacceptable failures could occur that are outside the vehicle’s intended design.

This SAE compliant design will be done within an AV manufacturer’s self-certification process and the corresponding safety assessment letter submitted to NHTSA. The “cross-cutting” areas and automation functions that are to be addressed in the letter are summarized in **Table 3**, which is taken from p. 34 of the recently released USDOT/NHTSA policy document. The

complete discussion of these cross-cutting areas is found in pp. 17-34 of the policy document (refer to footnote 1. above).

Table 3. Applicability of Federal Automated Vehicle Policy Guidance Areas to SAE Level 2-5 Automated Vehicle Systems

Levels of Automation	SAE Levels 3, 4, 5 (HAVs)	SAE Level 2
Safety Assessment Letter to NHTSA	***Yes***	***Yes***
C. Cross-Cutting Areas	***Fully***	***Partially***
C.1.Data Recording and Sharing	Yes	Yes
C.2 Privacy	Yes	Yes
C.3 System Safety	Yes	Yes
C.4 Vehicle Cybersecurity	Yes	Yes
C.5 Human Machine Interface	Yes	Yes
C.6 Crashworthiness	Yes	Yes
C.7 Consumer Education and Training	Yes	Yes
C.8 Registration and Certification	Yes	Yes
C.9 Post-Crash System Behavior	Yes	Yes
C.10 Federal, State and Local Laws	Yes	Clarify to driver
C.11 Ethical Considerations	Yes	Yes
F. Automation Function	*Fully*	*Partially*
F.1 Operational Design Domain	Yes	No
F.2 Object and Event Detection and Response	Yes	No
F.3 Fall Back (Minimal Risk Condition)	Yes	No
F.4 Validation Methods	Yes	Yes
G. Guidance for Lower Levels of Automated Vehicle Systems	***No***	***Yes***

Based on this premise of vehicle-focused safety certification inherently addressed by the vehicle product design, the AV transit system operator and the authority having jurisdiction will conduct the overall safety assurance program that would include the vehicle's design safety certification along with other systems (such as transit signal priority or preemption, roadway lane markings, off-line stations, fences, etc.) to assess hazards and risks for the entire transit operation. This safety assurance program would begin with the initial planning of the system, and continue throughout the design, implementation and on-going operations of the AV transit system. In a sense, the safety assurance process of the operating agency wraps around the safety certification provided by the vehicle manufacturer.

One item to be considered in the application of the NHTSA vehicle self-certification process in public transit applications and the overall safety assurance process is that there is no prescription of analytical methodology for the hazard analysis and risk assessment in ISO 26262. Various methodologies such as a Hazard and Operability Analysis (HAZOP), Failure Modes and Effects Analysis (FMEA), and System Theoretic Process Analysis (STPA)[17] are allowed with regard to the vehicle's electronic control system at the discretion of the vehicle manufacturer. Various alternative analytical methodologies and their associated standards are addressed in a comparative discussion in Section 3. Comparative Analysis of Standards of the NHTSA Report assessing of safety standards[18]. Subsection 3.4 Hazard and Safety Analysis Methods (p. 12-15 of the referenced NHTSA Report) specifically discusses these analysis alternatives allowed by in ISO 26262, which by extension are allowed by current NHTSA policy.

Driving Tasks in Transit Vehicle Operation – In considering the criteria defining the ODD of public transit vehicles, it important to recognize that automated operation of transit vehicles within a fully automated system imposes more than automation of just the driving functions within the responsibilities of the "machine-operator." Compare the IEC automation "tasks" for train automation (**Figure 6**) with the AV driving "tasks" recently developed by CAMP as shown in **Figure 7**. Note that the automated transit operations tasks that should be included in the automation based on IEC automated train operations include the following items not addressed by the CAMP automated driving tasks:

- Supervising passenger transfer (i.e., the boarding and alighting process),
- Operating a train to and from storage locations or the maintenance depot, and
- Detection/management of emergency situations.

These are tasks that are complex and impose different kinds of hazardous situations from those tasks of driving the vehicle. New vehicle subsystems not typically provided with regular automotive applications of AV technology may be required, such as systems to monitor the doorways of the vehicle to ensure that passengers have passed safely through the doorways and have not been trapped in the doors when closed by the automated vehicle. Such requirements may dictate a different set of operational design domains for public transit applications of Level 4 automation when the vehicle is certified by the vehicle manufacturer to operate in an unmanned mode.

[17] https://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/SAE/2015/2015SAE-Hommes-SafetyAnalysisApproaches.pdf

[18] Assessment of Safety Standards for Automotive Electronic Control Systems, NHTSA DOT HS 812 285, June 2016; http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2016/812285_ElectronicsReliabilityReport.pdf

Basic functions of train operation		On-sight train operation TOS	Non-automated train operation NTO	Semi-automated train operation STO	Driverless train operation DTO	Unattended train operation UTO
		GOA0	GOA1	GOA2	GOA3	GOA4
Ensuring safe movement of trains	Ensure safe route	X (points command/ control in system)	S	S	S	S
	Ensure safe separation of trains	X	S	S	S	S
	Ensure safe speed	X	X (partly supervised by system)	S	S	S
Driving	Control acceleration and braking	X	X	S	S	S
Supervising guideway	Prevent collision with obstacles	X	X	X	S	S
	Prevent collision with persons	X	X	X	S	S
Supervising passenger transfer	Control passengers doors	X	X	X	X or S	S
	Prevent injuries to persons between cars or between platform and train	X	X	X	X or S	S
	Ensure safe starting conditions	X	X	X	X or S	S
Operating a train	Put in or take out of operation	X	X	X	X	S
	Supervise the status of the train	X	X	X	X	S
Ensuring detection and management of emergency situations	Perform train diagnostic, detect fire/smoke and detect derailment, handle emergency situations (call/evacuation, supervision)	X	X	X	X	S and/or staff in OCC

NOTE

X = responsibility of operations staff (may be realised by technical system).

S = realised by technical system.

Figure 6. Levels of Train Automation from European and IEC Standards

Complete Automation Indicated by the Blue Box and
Automated Functions Unique to Operating a Transit Vehicle Indicated by the Red Box

Source: IEC 62267

Automation Level Name	Dynamic Driving Sub-Tasks		Functional Capability	
	Sustained Execution of Lateral and/or Longitudinal Control	Object & Event Detection and Response (OEDR)	Fallback Performance of Dynamic Driving Task	Driving Mode Circumstance, Location Capabilities
0 No Automation	Driver	Driver	Driver	None of the DDT is automated
1 Driver Assistance	Driver and system	Driver	Driver	Some driving modes
2 Partial Automation	System	Driver	Driver	Some driving modes
3 Conditional Automation	System	System	Driver	Some driving modes
4 High Automation	System	System	System	Some driving modes
5 Full Automation	System	System	System	All driving modes

Figure 7. Distribution of Functions by SAE/BASt Driving Automation Level

Source: Key Considerations in the Development of Driving Automation Systems, Crash Avoidance Metrics Partnership (CAMP) Automated Vehicle Research (AVR) Consortium;

http://www-esv.nhtsa.dot.gov/Proceedings/24/files/24ESV-000451.PDF

Further, there could be a requirement for different sets of operational design domain criteria when vehicles are specified, competitively purchased (per FTA funding requirements) and deployed into operation within different operating environments, such as:

- Protected environments like campuses with very low speed operations (e.g., less than 15 mph),
- Semi-protected environments like BRT corridors with dedicated transitways and operations with higher speeds (e.g., less than 55 mph),
- Mixed traffic in un-protected environments like arterial streets with moderate speed operations (e.g., less than 45 mph),
- High Occupancy Vehicle (HOV) lanes and segregated managed lanes operating at higher speeds (e.g., 55+ mph), or
- Classical bus operations at all speeds in any mixed traffic environment.

Although multiple formal variations in the NHTSA ODD definitions given to the AV manufacturers for purposes of self-certification are not necessarily proposed, a range of operational design domains for public transit applications may be appropriate to define.

Complexities of AV Transit Hazards and Risk Assessments – The breadth of the AV transit vehicle and system safety assurance process must encompass failures and hazardous conditions overall that include:

- Roadway infrastructure design and maintenance
    - Lane markings, signage, lane geometry
    - Signal systems and TSP/Spat V2I
    - Communications system backbones
- Environmental conditions and variations
- Pedestrian, bicycle and non-automated vehicle interactions
- Vehicle Hardware system failures
- Vehicle Electronic control systems & detection/sensing system failures
    - Multi-signal sensor/detector interpretation & harmonization
- Vehicle Programmable software-based control & monitoring systems failures
    - Failures and programming anomalies, obsolescence
- Vehicle Human-Machine interfaces and interactions/response conditions
    - Alertness, understanding, knowledge, ability to act (SAE Level 2-4)
    - ADA passenger boarding/alighting provisions, visual and audio announcements, wheelchair restraint systems, etc.
- Malicious, capricious security breaches and manipulations

The premise of this discussion is that many of these elements that must be designed to mitigate hazardous operating conditions will in fact be addressed within the NHTSA vehicle safety certification requirements. However, the Operational Design Doman (ODD) that is required for non-transit vehicle use may be different from an ODD that should be defined for AV transit use. In fact, there could be different classes of AV technology that are given different

ODD criteria when intended for different types of transit applications – e.g., first-mile/last-mile circulators/shuttles, BRT lines in dedicated guideway corridor service, and Park and Ride HOV facilities within mixed-traffic freeway corridors.

It is also important to recognize that automated roadway vehicle systems in transit service is considerably more complex than any such train control systems applied to automation in fixed guideway transit. This is particularly true within the automated roadway vehicle's control system which employs multiple sensor systems, electronic and software driven control systems, and (perhaps) artificial intelligence. While ISO26262 provides a clear process for functional safety, automated driving sensors provide inputs that are now effectively infinite as the range of environments that a given AV can navigate is uncontrollable. Machine learning and pattern recognition systems that process the inputs can produce non-deterministic and un-provable responses to a given set of inputs, resulting in a system that can't reasonably be verified to do "action X" in response to "input set Y". These conditions are more complex than anything that has been attempted in the safety assurance processes developed in the automated fixed-guideway transit field.

We expect, however, that within a few decades we will start to see large scale automation for whole transit systems operating across large metropolitan regions as technology matures and as demonstrations and tests become more and more successful. The smallest public transit bus operator to the largest scale regional transit authority should therefore begin now to put in place safety assurance programs recommended by the FTA SMS guidelines across bus and rail systems to prepare for this future reality. The complexities of automation will necessitate this comprehensive safety assurance process.

Operating Authority's Involvement in Risk Assessment – The various standards and FTA SMS safety program approach generally follows the safety assurance process derived from the MIL Std. 882 methodology. As shown in **Table 1** above, the resolution of hazards and the resulting acceptance of operating risks by Owner/Operator (or another entity designated as the local Authority Having Jurisdiction) are an integral part of the safety assurance process. In accord with the MIL Std. 882 methodology, risks that are classified as **Undesirable** *are allowable only with agreement* from Authority Having Jurisdiction, and risks classified as **Acceptable** *must be addressed with notification* to the Authority Having Jurisdiction. This process of assessing risks through the system safety assurance process, with the Authority Having Jurisdiction directly involved, will reasonably include:

- Local safety-culture considerations
- Risk comparisons to human-operated transit
- Cost considerations of implementing the possible hazard mitigations
- Adjusting the ODD or system deployment approach to eliminate the hazard

Hazards of Operations Within Transitways – By its nature, the safety analysis for AV transit systems will need to assess both equipment failures and hazards due to "external causes" that are not strictly related to equipment or system operations, but which can possibly penetrate within the transit system operating environment.

A relatively simple example recently cited by Dr. Adriano Alessandrini – Project Manager for the European Union's CitiMobil2 Project – involved the mitigation of a hazard for one of the CitiMobil2 installations. The concern was a site specific hazardous situation where the transitway passed adjacent to a children's daycare facility. The hazard of a child running into the path of an AV transit vehicle was identified as a risk that was unacceptable to accept, and it was resolved by building a fence to prevent children from entering the transitway.

These situations of external causes and the human-factors aspects of people (or objects) entering the transitway operating environment to create hazards will be much more common with AV transit vehicle operating at-grade on roadways than has been the case with automated guideway transit systems operating on exclusive guideways.

Hazards During Failure-Mode Operations – One of the factors creating hazards found to be important in automated guideway transit operations is the tendency for human intervention when fail-safe protective features restrict or degrade a transit system's operation. Willful override of control system safety functions is a serious issue when automation acts in accord with fail-safe design principles. The "safest state" for a fail-safe system is to bring operations of the failed train, or even the entire transit system to a complete stop. Such action to stop a train (or vehicle) causes substantial human anxiety in the transit system operations context where moving the maximum quantity of people is often considered paramount.

These scenarios for system failure, and the potential for hazardous conditions becoming more probable due to human intervention to override safety functions, requires implementation of strong procedures and protocols that must first be defined and vetted through the hazards and risk assessment process while the system is in the conceptual design phase.

Another human-response condition involves how the operational plan allows for personnel to respond to a vehicle failure. For example, provisions in a Level 4 AV transit system conceptual design could address a safety requirement to take a failed vehicle out of service by diverting to a vehicle parking location along the transitway (e.g., the city street on which the FMLM vehicle are operating, or along the dedicated BRT line right-of-way). When placed with adequate frequency along the route, the failed vehicle parking locations would need to be assessed for attributes necessary to protect passengers onboard the failed vehicle – possibly providing a place for passengers to exit the vehicle that is well lit and reasonably secure if the emergency response plan allows for this when vehicle evacuation is necessary. Operational considerations of the length of time required for personnel to reach the failed vehicle should be factored into the safety assurance process, along with the implied staffing levels that will be required to achieve this failure response time.

AV transit operating plans and associated protocol for actions by on-board backup operators or roving operations "recovery" personnel therefore must be an integral part of the SMS hazard analysis and resolution process. The combination of vehicle response to a failure or hazardous condition that reverts to what NHTSA calls a "fall-back" action, as well as the operations personnel failure response rules and protocol, must be part or the safety assurance plan for the specific transit system deployment.

Hazards in Semi-Automated Operations – The hazards and risks during the period of semi-automation when operators could take the inherent driving capabilities of the automated machine too much for granted and inappropriately divert their attention has been one important points of emphasis by representatives of the aviation industry. As has been found in the application of automated flight controls, there will be times when a machine (automated vehicle) is "driving" and it reaches a point where it doesn't know what to do next in the context of its operating environment, or when it has a serious failure within the control system.

In the early stages of AV automation, the technology may not have been developed to a level where the vehicle always knows how to "fail safely."[19] During those times the operator onboard the vehicle must be able to very quickly understand the environment, the system failure and/or the circumstances surrounding the vehicle. Aviation Industry accidents have demonstrated that there can be seriously unsafe situations develop within a matter of seconds if the operator is not available and sufficiently alert to assume control, and accidents will then happen that threaten the vehicle occupants with injuries or fatalities.

The safety assurance process must delve deeply into when/how those hazardous situations could prevent a timely and effective transition to human operation. Under situations when unsafe operations could occur, the analysis must address the risk mitigation of an accident.

[19] "Fail Safely" Interpretation – Current industry discussions show an intent to require any AV technology which is self-certified by the vehicle manufacturer to operate in L4 automation must maintain a "fail safely" capability. The vehicle manufacturer will define where the L4 automation is certified – typically within certain geographic boundaries and when operating along specific roadways. NHTSA interprets the fail safely intent to mean that the AV automated control system must ensure when it determines a need to transition from L4 to L3 or L2, and which if after a predetermined time an on-board human operator does not assume proper L3 or L2 control when requested, then the vehicle will automatically "fail safely." This means that the vehicle will act to automatically degrade its operations to a known safe state. Whenever this "fail safely" process is initiated, the vehicle must continue automated operations sufficiently to reach a physical location suitable to automatically take itself out-of-service, and to do so without causing an unacceptable hazard for other vehicles operating in its proximity.

Comprehensive Approach to AV Transit Safety Assurance

A comprehensive approach to developing the US transit industry's approach to safety assurance can help speed this disruptive technology revolution. A cooperative effort between the USDOT/State government sector, the automotive/transit vehicle manufacturers and AV technology development sector, and the public transit industry sector will yield the best result. Taking a proactive approach in the consensus process will have substantial benefits over delaying until one or the other sectors takes the next step or simply reacting to the direction the technology is heading.

Functional Safety is provided through self-certification by the manufacturers/vehicle supplier using the approach in the SAE/ISO 62626 standards. The Safety Assurance Process building from the FTA SMS principles then would wrap around the vehicle technology and add other physical elements and subsystem equipment such as the right-of-way, roadway infrastructure wayside V2I Communications Equipment, supervisory dispatch control systems, and the fixed facilities and associated station equipment.

Benefits of Industry Consensus Standards for AV Transit – Taking a comprehensive approach to developing an industry norm for AV transit systems will not only involve the methodologies described, and not only the expansive system elements mentioned, but also creating a suitable consensus standard(s) that addresses the whole transit system's safety requirements.

The automated guideway transit industry has demonstrated the benefits of preparing an industry consensus standard, particularly considering the number of variations that could evolve in the safety assurance process if left to individual countries, states and transit operators to create through their own means and methods. Having at least a generic framework for definitions of hazards and risk mitigation measures, as well as a uniform analytical methodology to address the effects of the hazards would speed the development of AV technology application and shorten the delivery times for transit projects going forward.

Such an industry definition of methodology and a generic framework of hazard definitions will not remove the need for the safety assurance process to be applied to every new project to address unique hazards that are present in each site-specific location. If properly developed, the industry norms will facilitate each local authority's application of the methodologies for their local projects.

Examples cited of industry developed standards in the automotive industry are certainly important to NHTSA's highly automated vehicle policy, and these automotive standards must also be an integral part of a coordinated set of transit industry consensus standard for AV transit. Within an AV transit consensus standard, the industry could select the preferred detailed hazards analysis methodology that is otherwise left to the discretion of the vehicle manufacturer in the ISO 62626 standard process (see the related discussion above in the subsection titled Nature of AV Hazards and Risks in the Transit Operating Environment).

In developing a transit industry consensus standard, a key issue would be to addresses the system failure response that "falls back" to a "minimum acceptable risk condition". Safety

criteria suitable for the transit industry would have to be defined with respect to a product manufacturer's minimum design requirements, particularly with how exactly an AV responds to defined hazards to provide an "absence of unreasonable risk" in accord with a manufacturer's "design intent."

Although the suggestion of a consensus standard is possibly a disruptive idea in the current free market of AV development, such an endeavor would need the full involvement of SAE, both Federal and State government agencies, and the transit industry through entities like APTA in North America and possibly UITP in Europe.

The following briefly discusses the similar consensus standards that have been developed for automated guideway transit, and how they could be a model for an AV transit standard.

ASCE-21 APM Consensus Standard Model – ASCE-21 is a comprehensive standard that is formulated around the basic subsystems and their functional requirements. Prescriptive requirements are generally given only when safety is involved in the design aspects of the specific equipment (e.g., maximum closing force on vehicle doors).

The APM Standard provides a very good point of reference for safe design principles that can be utilized and referenced during the design of AV Transit systems. Although the comparisons of safety for AV transit will likely be made primarily to the accident and fatality rates for non-automated transit buses being driven by human operators, the "high bar" of automation safety that has been set by ASCE-21 will remain a valid point of reference.

The MTBHE requirement for the automated train control system of 1 failure with catastrophic or critical consequences every 1 x 10^8 operating hours may be unrealistic to model in transitways that are not exclusive and where transit vehicles must interact with pedestrians and non-automated vehicles. But the principle of establishing a minimum safety requirement in the form of a mean time between hazardous events is a very relevant characteristic to model in an AV consensus standard.

Features of ASCE 21 that are also relevant as a model standard are the inclusion of chapters on Security; Emergency Preparedness; System Verification and Demonstration; Operations; Maintenance, and Training; and Operational Monitoring. These topics are also highly relevant to the overall safety assurance process, and are elements of the life cycle of the project that must be part of the hazards analysis and risk assessment on an ongoing basis.

IEC 62267 AUGT Consensus Standard Model – IEC 62267 is an industry consensus safety standard developed in a form that addresses the functions of a fully automated, unattended transit systems which would normally have been performed by a human operator and/or train attendants (refer to UTO functions in **Table 1** above, the source for which was this IEC standard). The functions are not with respect to the subsystems and related equipment (as was the case for ASCE-21), but rather with respect to the whole vehicle or whole transit system functions. A comparison of the table of contents for ASCE-21 (**Appendix B**) and the table of contents of IEC 62267 (**Appendix D**) clearly shows these differences.

This difference in approach makes IEC 62267 another important reference document that could provide a model of an industry consensus standard for fully automated AV transit systems.

In addition, the technical report on system-level hazard analysis in Part 2 of IEC 62267 provides an excellent example of the type of generic, system-level hazards analysis that is needed for AV transit applications. In fact, at the time of this working paper's publishing, there is a current TRB research needs statement that proposes this type of generic hazard analysis for AV transit, sponsored by TRB AP 040:

https://rns.trb.org/dproject.asp?n=39074

EN 50126/CityMobil2 Safety Case Model – CityMobil2 recently completed its successful 4-year pilot program that deployed AV technology in a series of 6 month demonstrations at five different sites within the European Union[20]. The project had 45 partners drawn from system suppliers, city authorities (and local partners), the research community and networking organizations. Throughout the duration of the pilot demonstrations a total of 60,000 passengers were transported in automated shuttle vehicles operating in mixed pedestrian and some mixed traffic environments.

Figure 8 shows one of the demonstration projects which utilized a vehicle operating in a transit lane distinguished only by lane markings, with traffic able to cross the lane when necessary. The shuttles in this lane configuration that was not physically protected had a maximum speed of 10 kilometers per hour (6 mph) in mixed traffic operations. The AV shuttles operated at 20 kilometers per hour (12 mph) when only pedestrians were present.

The safety assessments for CitiMobil2 were performed in accord with EN standards for fixed guideway transit (refer to the discussion of Cenelec EN standards in Chapter 4), with adaptation to the purposes of the automated roadway vehicle application. The safety certification process started from the set of EN industry consensus standards for automated railway systems, with emphasis on CENELEC EN 50126 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). In the European Union, the completion of the safety analyses and certification under the review and approval of an oversight governmental agency is referred to as the "safety case."

Further details on the safety case and the related operational hazard analyses are expected to be released in 2017 as part of the documentation of the CitiMobil2 project work.

[20] A presentation overviewing the accomplishments of the CitiMobil2 project was given by Professor Adriano Alessandrini at the 2016 TRB/AUVS Automated Vehicle Symposium;
https://higherlogicdownload.s3.amazonaws.com/AUVSI/14c12c18-fde1-4c1d-8548-035ad166c766/UploadedImages/documents/Weds/1000-1015%20Alessandrini.pdf

Figure 8. CitiMobil2 AV Shuttle Vehicles Were Demonstrated to be Operable in Mixed Traffic at Low Speeds Determined to be Acceptable Through the Development of the Safety Case

Enhancement of System Safety Assurance Process Through EN50126 Safety Case Approach – The "safety case", as the term is used in Europe, is the complete set of documentation by which the hazards and risk assessment is managed and recorded. This safety case, by definition, is a life-cycle safety assessment process performed in accord with the CENELEC consensus standard EN 50126 Reliability, Availability, Maintainability and Safety (RAMS) as it is applied to railway signaling systems. The leader of the ASCE-21 System Safety Working Group (see the Acknowledgements page) presented a technical paper[21] on the use of the safety case as a "living document" to manage the life-cycle safety process. The comprehensive approach of the safety case also integrates the management of quality, as well as design of functional and technical safety. This is an approach consistent with our findings in this working paper for AV transit deployment under FTA's Safety Assurance program. The referenced APTA paper [21] begins with this summary:

> *Hazards may be introduced to a program in various ways; most people immediately associate hazards with hardware failures, software faults or human interactions. Hazards may also be introduced systematically through failures or omissions of the system safety program itself. When executing a system safety program, it is important to address the safety management, the quality management, and the functional and technical safety aspects in full measure. This broad perspective is encouraged in Europe as embodied in the CENELEC standards EN 50126 Railway Applications – Specification and*

[21] Sue Cox presented this approach to safety analysis and management at a 2012 APTA conference. http://www.apta.com/previousmc/rail/previous/2012/papers/Papers/Cox-S-The-Safety-Case-as-a-Living-Document.pdf

Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), and EN 50129 Railway Applications – Safety-Related Electronic Systems for Signaling, which documents the evidence for all three aspects into a safety case for safety acceptance and approval.

Experience has taught two important lessons; that the safety case does not have to be voluminous, nor should it be deferred until the end of a project. The safety case can be drafted at the beginning of a project and used as a living document to manage the system safety program. The living safety case records progress, deviations and issues in a concise format that facilitates the identification of project risks which supports project management and helps achieve schedule milestones and manage budget. Based on the author's CENELEC experience, this paper will discuss the application of a living safety case to manage a system safety program based on MIL-STD-882 System Safety to address hazards that may be introduced systematically, by random failure, by human interaction or through external influences.

This paper focuses on the safety case for a specific system element (e.g. the signalling system), however it can be extrapolated to the safety case for a full transit system including facilities and multiple systems elements.

Safety Assurance Process Roles and Responsibilities

There are a number of parties that typically would have a role to play in the deployment and operation of an AV public transit system, including the governmental bodies, local transit authority or bus operator, as well as the employee unions/ and insurance companies. But not all have a direct responsibility with respect to the implementation of a comprehensive safety assurance program. Roles and responsibilities with respect to safety assurance, contractual obligations/liability, system planning/design/implementation, as well as vehicle/system testing and acceptance will need to be defined for a number of players.

All of the following entities should have input to and/or responsibilities resulting from the system safety assurance program:

- Local Authority Having Jurisdiction for Safety Assurance – e.g., regional authority or municipality legally responsible for the transit operating company
- System Equipment/Facilities Manufacturers, Suppliers and Constructors
    - Automated Vehicle Manufacturer/Supplier
    - System Integration Contractor-- ITS systems, V2V/V2I communications systems, vehicle dispatch and operations command and control (supervisory control system), station systems and equipment, etc.
    - General Contractor(s) – Transit Stations, Maintenance/Operations and Ancillary Facilities, and Transitways/Roadways
    - Transit System Operating Agency (or contractor)
- Local and State Government Agency(ies) responsible for roadway design/maintenance and traffic signal system management
- Local Government(s) responsible for multimodal transportation infrastructure

    - Agency/management district responsible for ancillary transportation facilities (e.g., street parking, street lighting, street furniture, signage and lane marking, etc.)
    - Agencies/Department(s) responsible for building codes and land-use ordinances, roadway system right-of-way planning and complete street/pedestrian/bicycle facilities design provision, etc.
- State Safety Oversight Agency (e.g., State Department of Transportation)
- National Highway Traffic Safety Administration (NHTSA)
- Federal Transit Administration (FTA)
- Industry Groups Providing Consensus Standards
    - Society of Automotive Engineers (SAE)
    - American Public Transportation Association (APTA)
    - Others as they become involved

This comprehensive approach to AV transit system safety assurance starting at the project level through the involvement of the local and state parties, combined with a comprehensive approach to developing regulations and standards at the national and international levels, offers the best promise for a fast and effective deployment of AV technology.

6. Findings and Recommendations on AV Transit System Safety

Early deployments of AV technology are pushing outside the envelope of legally permitted manual operations of roadway vehicles on public streets, and the Federal Government is responding to establish new vehicle safety policy guidelines in advance of as-yet undetermined regulatory changes. The policy position announced by USDOT/NHTSA in September 2016 sets a useful and somewhat flexible framework for self-certification of AV vehicle manufacturers and new AV technology developers. These guidelines will allow continued research and development of Level 2, 3 and 4 driving automation, while beginning to set initial parameters and advancing research into eventual changes to the Federal Motor Vehicle Safety Standards.

NHTSA Policy – The Federal Automated Vehicles Policy established an initial process whereby automobile manufacturers and AV developers can submit a written assertion of their safe design, using SAE standards as their primary basis of certification – a standard regiment that is supported by the ISO 62626 Road Vehicle Functional Safety standard. Within that safety standard a process of certification documentation is established, although the precise calculation details in hazard analysis and risk assessment are allowed through several different methodologies (such as Failure Modes and Effects Analysis -- FMEA, or System Theoretic Process Analysis – STPS). The safety analyses are performed to a level that calculate the high probability that the vehicle design will meet the design intent of the product, with a manufacturer's own minimal risk criteria established as an acceptable condition of safety under what is called "fall back" conditions in the NHTSA policy document.

FTA Policy – Transit system safety has been addressed by the FTA through the timely establishment of a new Safety Management System rulemaking. The SMS is very similar to a process also adopted by FAA, and is well suited to serve as a foundation for future safety assurance processes that will be necessary for complex AV deployments in transit service.

Vehicle-Focused Methodologies – Safety methodologies that use an approached based on "functional safety" are derived from an original machine automation IEC 61508 standard which defined a process of assessing "functional safety", from which numerous industry-sector specific application standards have been prepared. In the automotive industry, the resulting functional safety standard is the ISO 62626 standard that has become the principal safety methodology written into the SAE standards for automated vehicles. The level of safety that is determined through a rigorous calculation of probability of failure or hazardous event is called an automotive safety integrity level (ASIL), and the calculations are reasonably repeatable and suitable for certification purposes from the subsystem level up to the whole vehicle level.

System Focused Methodologies – The military/aviation industry has been the primary source of the methodology for safety analysis and design safety program management for complex control systems. Originally applied as MIL Std. 882, the basic methodology of following a set program of safety methods, beginning with the performance of a hazards analysis and risk assessment. The methodology then continues with the conducting of a systematic program to identify, mitigate and manage the risk of any unacceptable accidents which could result in a hazardous event that is unacceptable – i.e. resulting in fatalities, injury and/or significant equipment damage.

A whole linage of safety standards has followed on this basic MIL Std. 882 methodology, and several have direct relevance to AV technology applications to public transit. The FTA safety methodologies and guidelines are themselves directly in line with this system-focused approach, and give the process the title of "safety assurance" in correspondence with FAA terminology. In addition, several safety standards written specifically for automated guideway transit systems also follow in this line of methodology, including ASCE 21 Automated People Mover Standard, IEC 62267 Safety Requirements for Automated Urban Guided Transport, and the set of Cenelec EN standards for railways applicable to fully automated railways.

AV Transit Safety Assurance Considerations – The operation of an automated transit system requires a comprehensive safety assurance approach, with assessment of safety impacts of hazards beginning in the conceptual design phase, and continuing throughout the life cycle of the project. Assessment of the system-level hazards are required in this process, with the vehicle-focused functional safety would be included as one element of the overall hazards analysis and risk assessment/management process.

Hazardous condition that are possible and which must be assessed for risk and then through design (or other means of risk mitigation/acceptance) the hazard must be reasonably mitigated. This process must extend from the AV technology to the transitway/roadway on which the vehicles would operate, the ITS/V2I communications equipment/system, the stations/facilities of the system and the whole range of possible operating conditions. The nature of hazards and risks under AV transit applications have a particular need for safety analyses which address the following aspects of automated transit operations from the earliest stages of system design:

- **Operating Tasks in AV Transit Vehicle Operation** – broader in scope than those of AV automotive standards definition of Dynamic Driving Tasks.
- **Complexities of AV Transit Hazards and Risk Assessments** – multiple subsystems with software-based controls, multi-sensor harmonization, vehicle/human interfaces and interactions.
- **Hazards During Failure-Mode Operations** – combinations of vehicle response to failure which bring the vehicle to a stop, and human reaction that may act over-ride safety functions.
- **Hazards in Semi-Automated Operations** – human expectations of automated functions can exceed the design provisions, and transitions from L4 full automation can become hazardous when a human operator does not take assume control in a proper manner.

Guidance of AV Transit Deployments – Several players have a role in the process of safely planning, designing and deploying the AV Public Transit system. Multiple federal government agencies, state government agencies, and local government agencies affect the preparation and execution of a safety assurance program by the local public transit operator/authority. Some are involved at the top regulatory level to which the safety process must comply, while other are involved in the design decisions to adjust the physical built environment to accommodate the AV system. These parties and their roles and responsibilities have a bearing on executing a comprehensive safety assurance program.

There are examples of consensus standards that have used a comprehensive approach to safety assurance for automated systems. ASCE 21 Automated People Mover Standard, IEC 62267 Safety Requirements for Automated Urban Guided Transport, and Cenelec EN standards (used in the CitiMobil2 project) all provide a possible model for developing an AV transit consensus standard.

Finally, the most important consideration that the Federal Government agencies, State Oversight Agencies and local Transit Operating Agencies must address is the fact that safety analyses which focus only on the driving automation systems and the other vehicle safety features/systems are addressing only part of the operating realm within which public transit systems must safely operate. Only a blended approach of the different vehicle-focused and system focused methodologies can comprehensively provide operational safety of automated transit systems. The role of a conventional transit vehicle's human operator goes well beyond just "driving the bus." The management of passengers and the situations that they can bring into the operating system cannot be addressed by vehicle automation technology alone. Human oversight and associated supervisory systems must also perform key functions in safety and security of public transit.

Recommended Research Projects on AV Transit Safety – There are significant matters to be addressed in the near to medium term regarding the safety analyses required for AV transit deployment in passenger service, especially when automation levels reach L4 full automation. The following key research projects are recommended for undertaking based on the discussions and findings of this working paper:

1. ***Definition of Complete Transit Functions to be Automated*** – Research is needed to assemble a comprehensive definition of tasks/functions typically performed by a human operator or attendant in a conventional transit vehicle/train. The study should also perform a detailed evaluation of automation prospects for those tasks/functions not included in the SAE J3016 defined dynamic driving task (DDT) and operational design domain (ODD).
2. ***Categories of Hazards and Risks*** – Assessment of categories for hazards and risks as defined by MIL Std. 882 and its derivatives (e.g., ASCE-21, per **Table 1** above) is recommended in a technical study, while considering the necessary criteria and operating environments to assess whether scenarios with any fatality or injury are always Unacceptable for any AV transit application. Further, the study should assess whether there are scenarios where one or more fatalities could be categorized as Undesirable or Acceptable for some AV transit applications or circumstances. Subsequently, the study should provide a definition of associated operating environment, level of automation, conditions of other vehicle access control, etc. for the scenarios as defined.
3. ***Generic Hazards Analysis*** – Preparation of a Generic Hazard Analysis for each type of operating environment and level of automation is a recommended study, beginning with IEC 62267, Part 2 as an initial template of methodology and types of hazards and then expanding the analysis to represent conditions of AV transit deployment.

4. ***New Consensus Standard for AV Transit Systems*** – Research is needed that would perform an adaptation of an existing automated guideway transit safety standard, or alternatively creation of a totally new standard, with full involvement of the transit industry (operating agencies and system equipment suppliers), governmental authorities and AV technology researchers/developers.
5. ***Transit Operational Design Domain*** – Development of the parameters, criteria and characteristics of the AV transit specific operational design domain is needed in a form compatible with the ODD defined by the Society of Automotive Engineers for non-transit applications.

Appendix A
NHTSA Assessment of Safety Standards for Automotive Electronic Control Systems (DOT HS 812 285)

Appendix: Summary of Standards Comparison

This study compared and assessed the following relevant safety standards:

- ISO 26262: Road Vehicles – Functional Safety
- MIL-STD-882E: Department of Defense Standard Practice – System Safety
- DO-178C: Software Considerations in Airborne Systems and Equipment Certification
- FMVSS: Federal Motor Vehicle Safety Standard
- AUTOSAR: Automotive Open System Architecture
- MISRA C: Guidelines for the Use of the C Language in Critical Systems

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Type of Standard	Process	Process	Process and method	Design (architecture)	Design (coding)
Definition of Safety	Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	No clear definition provided. Based on Failure Condition Category (Figure 37), the definition is similar to MIL-STD-882E.	Absence of unreasonable risk.	Same as ISO 26262.	No explicit definition.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Definition of Hazard	A real or potential condition that could lead to an unplanned event or series of events (i.e., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	No definition provided.	Potential source of harm caused by malfunctioning behavior of the item Malfunctioning Behavior: failure or unintended behavior of an item with respect to its design intent.	Same as ISO 26262.	No explicit definition.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Identification of Safety Requirements	Functional hazard analysis on predefined nominal system functions is used to identify safety hazards.	Assumes software requirements are flowed down from system-level activities, and provides no guidance on how to further decompose the requirements and identify additional safety-critical requirements at each level of the system decomposition hierarchy.	At high level of the system, use hazard analysis method. At lower levels of the system, use safety analysis methods.	Focused on architecture design requirements. Depend on ISO 26262 to identify safety requirements.	Focused on coding standard.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Hazard and Safety Analysis Methods	Functional hazard analysis on predefined nominal system functions is used to identify safety hazards.	Not discussed.	Hazard Analysis includes: brainstorming, checklists, quality history, Failure Models and Effects Analysis, and field studies. Safety Analysis include: Failure Modes and Effects Analysis, Fault Tree Analysis, Event Tree Analysis, and Hazard and Operability Analysis, Markov Model, Reliability Block Diagram, etc.	Not discussed.	Not discussed.
Management of Safety Requirements	Hazard Tracking System used separately from other requirements management system.	Safety requirements and regular system requirements are managed together.	Safety requirements and regular system requirements are managed together.	Not discussed.	Not discussed.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Risk Assessment	For general system: Severity and Probability of occurrence For software: Severity and Software Control Category (no probability) Uses the term of "acceptable risk," but mentions user involvement in decision. Accepts both qualitative and quantitative probability assessment.	Only considers severity, no probability assessment. Hazards are considered to be caused by software behavior inconsistent with specified requirements, assuming all safety requirements are identified already.	Uses three dimensions—Severity, Exposure, and Controllability to generate ASIL-Automotive Safety Integrity Level. Uses the term of "acceptable risk," without sufficiently precise definition. Accepts both qualitative and quantitative probability assessment. Suggests ASIL decomposition for all hardware and software.	Not applicable.	Not applicable.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Design for Safety Approach	Thoroughly discussed starting with prevention and elimination.	Not explicitly discussed.	No explicit discussion. Focus on *safety mechanism.*	Good architecture may prevent hazards.	Good coding practice will reduce errors in software.
Software Safety	Same as Hardware Development Process, following the systems engineering process.	Follows the systems engineering process. Uses the concept of *Software Anomaly*.	Follows the systems engineering process. Uses the concept of *Software Fault*.	Not applicable.	Coding standards.
System Lifecycle Consideration	Prompts considerations for various aspects after system is in operation, but does not mention safety considerations for the manufacturing process.	Focuses on software lifecycle considerations such as coding, configuration management, etc.	Considers lifecycle of the system, including manufacturing, but does not explicitly discuss the safety of human operators and maintainers, and the environmental hazard.	Focuses on reusability, modifiability.	Not applicable.

	MIL-STD-882E	DO-178C	ISO 26262	AUTOSAR	MISRA C
Human Factors Considerations	Emphasized throughout the standard.	Not discussed.	Not emphasized. Only controllability assessment in ASIL relates to human factors.	Not discussed.	Not discussed.

Appendix B
ASCE-21-13 Automated People Mover Standard – Table of Contents

5. Automatic Train Control (ATC)

5.1 Automatic Train Protection (ATP) Functions
5.1.1 Presence Detection
5.1.2 Separation Assurance
5.1.3 Unintentional Motion Detection
5.1.4 Overspeed Protection
5.1.5 Overtravel Protection
5.1.6 Parted Consist Protection
5.1.7 Lost Signal Protection
5.1.8 Zero Speed Detection
5.1.9 Unscheduled Door Opening Protection
5.1.10 Door Control Protection Interlocks
5.1.11 Departure Interlocks
5.1.12 Direction Reversal Interlocks
5.1.13 Propulsion and Braking Interlocks
5.1.14 Guideway Switch Interlocks
5.1.15 Off-line sections operation – special conditions
5.2 Automatic Train Operation (ATO) Functions
5.2.1 Motion Control
5.2.2 Programmed Station Stop
5.2.3 Door and Dwell Time Control
5.3 Automatic Train Supervision (ATS) Functions
5.3.1 Constraints on ATS
5.3.2 Status and Performance Monitoring
5.3.3 Performance Control and Override
5.4 Manual Operation Limitations

6. Audio and Visual Communications

6.1 Audio Communication
6.1.1 Station Public Address
6.1.2 Emergency Station and Wayside Communications
6.1.3 Train Voice Communications and Public Address
6.1.4 Operations and Maintenance (O&M) Personnel Communications
6.1.5 Recording of Audio Transmissions
6.1.6 Intelligibility of Audio Communications
6.2 Video Surveillance
6.2.1 Central Control Equipment
6.2.2 Passenger Station Equipment
6.2.3 Recording of Video Transmissions
6.3 Passenger Information Devices
6.3.1 Vehicle
6.3.2 Stations

7. Vehicles

7.1 VEHICLE CAPACITY AND LOAD
7.2 VEHICLE DYNAMIC ENVELOPE
7.3 CLEARANCE IN STATIONS
7.4 VEHICLE STRUCTURAL DESIGN
7.4.1 Structural Analysis
7.4.2 Previous Structural Analysis
7.4.3 Structural Design Life
7.4.4 Structural Design Criteria
7.5 COUPLING
7.5.1 Mechanical Design
7.5.2 Electrical/Control
7.5.3 Coupler Interfaces
7.6 SUSPENSION AND GUIDANCE
7.7 PASSENGER COMFORT
7.7.1 Heating and Air Conditioning
7.7.2 Ventilation
7.7.3 Ride Quality
7.7.4 Noise Levels
7.7.5 Vibration
7.7.6 Passenger Compartment Provisions
7.8 DOORS, ACCESS, AND EGRESS
7.9 WINDOWS
7.10 FIRE PROTECTION AND FLAMMABILITY
7.10.1 Material Selection
7.10.2 Thermal Protection
7.10.3 Fire Extinguishers
7.10.4 Smoke Detectors
7.11 LIGHTING
7.11.1 Interior Lighting
7.11.2 Emergency Lighting
7.11.3 Directional Identification and Headlights
7.12 ELECTRICAL SYSTEMS
7.12.1 Propulsion Subsystem
7.12.2 Auxiliary Subsystem
7.12.3 Wiring
7.12.4 Power Collectors
7.12.5 Grounding

8. Propulsion and Braking

8.1 PROPULSION AND BRAKING SYSTEM RATING
8.2 PROPULSION AND BRAKING METHODS
8.2.1 Adhesion Propulsion
8.2.2 Tension Member Propulsion
8.2.3 Air Flow Propulsion

10. Stations

10.1 DISABLED PERSONS ACCESS REQUIREMENTS
10.1.1 Vehicle–Platform Gap
10.1.2 Detectable Warning Strip
10.2 PLATFORM EDGE PROTECTION
10.2.1 Intrusion Prevention System
10.2.2 Intrusion Control System
10.2.3 Intrusion Detection System
10.3 EVACUATION OF MISALIGNED TRAINS
10.4 EMERGENCY LIGHTING AND VENTILATION
10.5 FIRE PROTECTION
10.5.1 Fire Detection
10.5.2 Fire Containment
10.5.3 Fire Suppression

11. Guideways

11.1 BLUE LIGHT STATIONS
11.2 INTRUSION PROTECTION AND DETECTION
11.3 EMERGENCY EVACUATION AND ACCESS
11.3.1 Tunnel Guideway
11.3.2 Surface Guideway
11.3.3 Elevated Guideway
11.4 FIRE PROTECTION
11.5 SIGNAGE
11.6 EMERGENCY LIGHTING AND VENTILATION
11.7 EMERGENCY POWER SUPPLY
11.8 GUIDEWAY ALIGNMENT
11.8.1 Clearances
11.8.2 Operating Equipment Interfaces
11.8.3 Drainage
11.9 STRUCTURAL CRITERIA
11.9.1 Loads and Forces
11.9.2 Load Combinations
11.9.3 Design and Analysis

12. Security

12.1 SYSTEM SECURITY PROGRAM
12.1.1 Management and Accountability
12.1.2 Security Problem Identification
12.1.3 Employee Selection
12.1.4 Training
12.1.5 Audits and Drills
12.1.6 Document Control
12.1.7 Access Control
12.2 SYSTEM SECURITY PROGRAM PLAN

13. Emergency Preparedness

13.1 EMERGENCY PREPAREDNESS PROGRAM PLAN
13.1.1 Objective of Plan
13.1.2 Contents of Plan
13.1.3 Guidance
13.2 TRAINING AND DRILLS
13.3 POST-EMERGENCY INCIDENT AND DRILL COORDINATION

14. System Verification and Demonstration

14.1 APPLICABILITY OF PRIOR VERIFICATION
14.2 METHODS OF VERIFICATION
14.3 SYSTEM VERIFICATION PLAN
14.3.1 Plan Requirements
14.3.2 Verification Sequence
14.3.3 Inspection and Test Procedure Documentation
14.4 MINIMUM VERIFICATION REQUIREMENTS
14.5 APPLICATION-SPECIFIC ACCEPTANCE REQUIREMENTS

15. Operations, Maintenance, and Training

15.1 SYSTEM OPERATIONS PLAN
15.1.1 System Operational Strategies
15.1.2 Manual of Operating Procedures
15.1.3 Staffing Plan
15.2 MANAGEMENT PLAN
15.3 PLANNED SYSTEM STARTUP AND SHUTDOWN
15.3.1 Planned System Startup
15.3.2 Planned System Shutdown
15.3.3 Unscheduled System Shutdown/Startup
15.4 SERVICE RESTORATION ANALYSIS
15.5 ALARMS AND MALFUNCTIONS REPORTING
15.6 RECORDKEEPING AND MANAGEMENT REPORTS
15.7 MAINTENANCE
15.7.1 System Maintainability
15.7.2 Maintenance Plan
15.7.3 Maintenance Manuals
15.8 TRAINING
15.8.1 Training Plan
15.8.2 Training Instructors
15.8.3 Training Materials
15.8.4 Ongoing Training
15.8.5 Training Manuals

Appendix C
A Brief Comparison of Safety Methodology in ASCE 21 Standard, FTA Rules, and EN 50126 Standard

Prepared by ASCE 21 Automated People Mover Standards Committee – Safety Working Group

Table 4 Comparison of ASCE 21 Standard and FTA Process

ASCE 21 Section	Similarities	Differences
3.1	• A System Safety Program is mandatory.	• ASCE 21 program is developed for fully automated systems • FTA program is developed for rail transit in general
3.1.1	• System Safety program plan is used and updated/maintained throughout the project.	• ASCE 21 requires a SSPP [and SSCR –proposed edit]. • FTA requires SSMP, SSCP, SSPP and SSCVR. • ASCE SSPP item for System Safety Interfaces is not included in the FTA SSPP. • Since the FTA SSPP is intended for O&M phase in addition to project design/build phase, the FTA safety program has several additional elements such as: policy statement; control changes to SSPP; modifications that do not require formal safety certification; emergency management program; configuration management control; ensure local state and federal requirements included; hazardous materials; drug and alcohol; and ensure safety included in procurement process.
3.1.2	• Hazard resolution processes are very similar.	• ASCE 21 specifies hazard risk assessment criteria. • FTA guidance for hazard risk assessment is identical, except for more conservative classification of a few risks: IID and IIIC as Undesirable instead of Acceptable with Review/Notification, and IIIE is Acceptable with Review instead of Acceptable.
3.1.2.1	• Hazard analyses are similar; PHA, SSHA, SHA, O&SHA.	• Operating and Support Hazard Analysis (O&SHA) is termed Operational Hazard Analysis (OHA), although scope is the same. • FTA requires a Software Safety Analysis (SSA).
3.2	• Safety Principals are very similar.	• ASCE 21 specifies Safety Principals in the standard. • FTA Hazard Analysis Guidelines provides Safety Principals (informative).
3.3		• ASCE 21 specifies Fail-Safe Design.
3.4	• Designated safety elements undergo rigorous verification and validation.	• ASCE 21 identifies safety elements by the hazard analysis process. • FTA identifies certifiable elements and certifiable items from design criteria, codes and standards, and staff experience.
3.5		• ASCE 21 sets an additional requirement for the Automated Train Control (ATC) subsystem or Communications Based Train Control (CBTC) subsystem based on MTBHE.
4		• ASCE 21 specifies system dependability. • FTA is beginning to address reliability in Transit Asset Management (TAM) Proposed Rule, dated Sept 2015.
15	• ASCE 21 O&M and training requirements are like the FTA requirements for Operational Readiness.	

Table 5 Comparison of ASCE 21 Standard and EN Process

ASCE 21 Section	Similarities	Differences
3.1	• A System Safety Program is mandatory.	• ASCE 21 program is developed for fully automated systems • EN program is developed for rail transit RAMS in general, and for Communications, signaling and processing systems.
3.1.1	• System Safety Program Plan is used and updated/maintained throughout the project.	• ASCE 21 requires a SSPP [and SSCR –proposed edit]. • EN requires SSP, RAM Program Plan, Safety Case and Safety Assessment Report. • EN requires organizational independence and independent safety assessment. • EN incrementally develops certification and supports cross-acceptance of products.
3.1.2	• Hazard resolution processes are very similar.	• ASCE 21 specifies hazard risk assessment criteria. • EN 50126 Section 4.6 provides sample hazard risk assessment criteria. • EN Frequency definitions differ. EN "Occasional" is "Likely to occur several times". Then the following EN frequencies are one category off from ASCE. For example, EN "Remote" is the same as ASCE "Occasional". EN "Improbable" is the same as ASCE "Remote". EN has an additional Frequency classification of "Incredible", which is the same as ASCE "Improbable". • EN does not provide the MTBHE hours as part of the Frequency definition. • EN Severity definitions differ. For example, Catastrophic includes "fatalities and/or multiple severe injuries …"; and Critical includes "single fatality and/or severe injury …". Category IV is called "Insignificant" instead of "Negligible". • EN risk assessment levels are called Intolerable, Undesirable, Tolerable, and Negligible.
3.1.2.1	• Hazard analyses are similar; PHA, SSHA, SHA, O&SHA.	• EN 50128 prescribes a very thorough software development program.
3.2	• Safety Principals are very similar.	
3.3	• Fail-Safe Design techniques are very similar.	
3.4	• Safety elements are designated by the hazard analysis process, and undergo rigorous verification and validation.	
3.5	• Both standards are intended to support Automated Train Control (ATC) or Communications Based Train Control (CBTC)	
4	• Dependability (RAM) is integrated with safety program.	

Table 5 continued

ASCE 21 Section	Similarities	Differences
15		• ASCE 21 lists specific important O&M and training documents/requirements. • EN 50126/50129 does not have a similar list of O&M related required documents. However, EN addresses O&M issues as part of the detailed process. For example, see EN 50129 Section 1, 5.3.12, and 5.5.3, Annex B.2, B.4, B.5, and E.10. B.2.3 requires the Technical Safety Report demonstrate operational functional requirements, which are specified in the System Requirements are fulfilled by the design. B.4 requires demonstration of operation with external influences. B.5 defines all the rules, conditions and constraints that are necessary for safety, which include maintenance and operational procedures. E.10 is a table that identifies the application and O&M required by SIL level.

Abbreviations and Acronyms

AREMA	American Railway Engineering and Maintenance-of-way Association
CEL	Certifiable Elements List
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIL	Certifiable Items List
EN	European Standards
ETSI	European Telecommunications Standards Institute
FMECA	Failure Modes, Effects, and Criticality Analysis
FTA	Federal Transit Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
MTBHE	Mean Time Between Hazardous Events
PHA	Preliminary Hazard Analysis
OHA	Operational Hazard Analysis
O&SHA	Operational and Support Hazard Analysis
O&M	Operations and Maintenance
RAMS	Reliability, Availability, Maintainability and Safety
SHA	System Hazard Analysis
SILSafety	Integrity Level
SSA	Software Safety Analysis
SSCP	System Safety Certification Plan
SSCR	System Safety Certification Report
SSCVR	Safety and Security Certification Verification Report
SSHA	Subsystem Hazard Analysis
SSMP	System Safety Management Plan
SSO	State Safety Oversight
SSPP	System Safety Program Plan
TAM	Transit Asset Management
THR	Tolerable Hazard Rate

Appendix D
IEC 62267 Automated Urban Guided Transport Safety Requirements – Table of Contents

8 Safety requirements

- 8.1 General requirements
  - 8.1.1 Public works regulations to protect the guideway
  - 8.1.2 Fire protection
  - 8.1.3 Systems and equipment
  - 8.1.4 Rules for passenger behaviour
- 8.2 Monitoring the AUGT system
  - 8.2.1 Monitoring by the OCC staff
  - 8.2.2 Action of operational staff
  - 8.2.3 Communication systems
- 8.3 Operational rules
  - 8.3.1 Rules for rescue of passengers
  - 8.3.2 Rules for fire emergency
  - 8.3.3 Rules for foreseeable vandalism
  - 8.3.4 Rules for checking guideway clearance
  - 8.3.5 Rules for start-up and shut down of operations
  - 8.3.6 Rules for train operations in the depot
  - 8.3.7 Rules for trains to be put in or taken out of operation
  - 8.3.8 Rules for stranded train removal
- 8.4 Safeguards on platforms
  - 8.4.1 Common safeguards for enclosed and open platforms
  - 8.4.2 Enclosed platforms
  - 8.4.3 Open platforms with detection systems
- 8.5 Safeguards in trains
  - 8.5.1 Door closed supervision
  - 8.5.2 Door release for passenger transfer
  - 8.5.3 Door release for emergency opening
  - 8.5.4 Emergency exits
  - 8.5.5 On board obstacle detection device
  - 8.5.6 Derailment detection device
  - 8.5.7 On board video surveillance
  - 8.5.8 Public address system (train)
  - 8.5.9 On board announcement for taking a train out of operation
  - 8.5.10 Emergency stop demand on board
  - 8.5.11 Emergency call device on board
  - 8.5.12 Fire and smoke detection (train)
  - 8.5.13 Train status supervision and testing
  - 8.5.14 Manual operation
  - 8.5.15 Safe speed during automatic coupling
  - 8.5.16 Reaction to unexpected train movement
  - 8.5.17 Warning means in the train for evacuation
- 8.6 Safeguards for passenger transfer area
  - 8.6.1 Train immobilisation during passenger transfer
  - 8.6.2 Safeguards related to the opening of the doors
  - 8.6.3 Safeguards related to the closing of the doors
  - 8.6.4 Marking of train door areas on the platform
  - 8.6.5 Surveillance by operational staff
  - 8.6.6 Safeguards related to gap between train and platform

Appendix E
Content of IEC/TR 62267-2 Technical Report – Automated Urban Guided Transport (AUGT) Safety Requirements; Part 2 – Hazard Analysis at Top System Level