U.S. Department
of Transportation
National Highway
Traffic Safety
Administration

NHTSA

DOT HS 812 922

June 2020

Functional Safety Research Considerations For Heavy Vehicles

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names are mentioned, it is only because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

Kellom, B., Monfalcone, M., & Pape, D. (2020, June). *Functional safety research considerations for heavy vehicles* (Report No. DOT HS 812 922). National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No. DOT HS 812 922	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Functional Safety Research Considerations for Heavy Vehicles		**5. Report Date** June 2020 **6. Performing Organization Code**
7. Authors Brandy Kellom, Marc Monfalcone, Doug Pape		**8. Performing Organization Report No.** 100068302-6
9. Performing Organization Name and Address Battelle Memorial Institute 505 King Avenue Columbus, Ohio 43201		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTNH2214D00327L/0001
12. Sponsoring Agency Name and Address National Highway Traffic Safety Administration 1200 New Jersey Avenue SE Washington, DC 20590		**13. Type of Report and Period Covered** Final Report September 2015 to August 2016 **14. Sponsoring Agency Code**

15. Supplementary Notes
The Volvo Group was a subcontractor for this project.

16. Abstract
Industry standard ISO 26262 Road Vehicles - Functional Safety currently applies to vehicles with gross vehicle mass up to 3,500 kg (7,716 lb). The published standard's scope excludes trucks and buses. This study documents the factors that might necessitate functional safety approaches to have different considerations between different weight classes of vehicles and to explore how the heavy-vehicle industry is currently applying functional safety to its electrical and electronic systems. Heavy vehicles differ from light vehicles in the systems they comprise, the ways they are developed, and how they are used. The heavy-vehicle industry is currently applying the principles of functional safety, for example, through established systems engineering practices or the general industry standard IEC 61508. A revision of ISO 26262 that will expand the scope to include trucks and buses was in the committee draft stage at the time this study was conducted. The revision is expected to clarify the demarcation between a truck and attached vocational equipment and to account for the wider variance in heavy vehicles, but not to fundamentally change the process deriving the requirements for functional safety.

17. Key Words functional safety, heavy-duty vehicle, passenger vehicle, ISO 26262, electrical, electrical/electronic control systems, programmable safety-related systems, safety-critical systems, IEC 61508	**18. Distribution Statement** Document is available to the public from the National Technical Information Service, www.ntis.gov.

19. Security Classif. (of this report)	**20. Security Classif. (of this page)**	**21. No. of Pages**	**22. Price**
Unclassified	Unclassified	33	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

LIST OF FIGURES

Executive Summary

Organizations developing electrical and electronic systems for motor vehicles must take steps to ensure that they operate safely and that they continue to function in a safe manner, even when inevitable failures occur. Functional safety spans the vehicle and electronic system lifecycle through concept, design, development, integration, testing, validation, manufacturing, deployment, operations, servicing, and decommissioning. The voluntary industry standard ISO 26262 Road vehicles—Functional Safety (2011) defines functional safety as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical and electronic (E/E) systems." It requires documentation of specific safety steps at each stage of the lifecycle. The standard limits its scope to "series production passenger cars with a gross vehicle mass up to 3,500 kg." This study investigates how practices for functional safety might be different for heavier vehicles, particularly trucks and buses.

This report addresses two questions: what are the differences between passenger cars and heavier weight class vehicles that may necessitate a specialized approach to functional safety; and what types of functional safety practices are used today by these segments of the vehicle industry? To answer these questions, the research team conducted a literature search and interviewed industry professionals on the practices, applications, and technologies currently in use by the vehicle segments heavier than passenger car classification

The research team found that there are many differences between passenger cars and heavier weight class vehicles. The most significant differences, especially between the opposite ends of the weight class spectrum are the working relationships between the supplier, OEM, body builder, and customer. Passenger car and heavy vehicle industries have contrasting supply chain relationships, which determine who in the supply chain process is responsible for specific functional safety elements. Another significant area of difference is the increasing variation of uses of vehicles. Between the manufacturing and use on the road, heavy vehicles undergo a range of modification and customization, which affect the degree and type of functional safety approach required.

Methods to achieve functional safety have been commonplace for many years in the heavy vehicle industry, despite its current exclusion from ISO 26262. Standards such as IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (2010), applicable sections of ISO 26262, and longstanding internally developed processes (hazard analysis, FMEA, SPICE, etc.) are used by the industry to ensure safe vehicles are delivered to customers.

Work is ongoing to adapt ISO 26262 to heavier vehicles. The next version of ISO 26262 is expected to be released in 2018. While it is scoped to include guidance for heavy vehicles, it is unlikely to introduce any major conceptual changes. Updates are likely to include improved safety analysis software, more detailed requirements for security, and improvements for the assessment and auditing process. In the meantime, the heavy vehicle industry performs vehicle safety engineering without a universal standard, instead using proprietary safety processes based on experience, influence from passenger safety standards (including the current ISO 26262), and governmental regulation.

Chapter 1. Introduction

As electrical and electronic systems become more complicated, safety becomes increasingly important. Organizations developing hardware and software must take steps to ensure that power and control systems operate safely and that they continue to function in a safe manner even when inevitable failures occur. This level of safety is not achieved as an afterthought; it must be explicitly incorporated throughout the product lifecycle.

To provide a methodical manner for addressing safety in devices with electronic systems, a number of industries came together to develop a voluntary standard, published by the International Electrotechnical Commission as IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (2010). IEC 61508 is intended to be a basic functional safety standard applicable to all kinds of industry and defines functional safety as "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the electrical/electronic/programmable electronic safety-related systems, other technology safety-related systems and external risk reduction facilities."

Consistent with the overall societal trend, electronics is finding its way into more vehicle systems, and controls in motor vehicles are assuming greater responsibility. Examples include familiar functions such as cruise control, otherwise impossible safety features such as stability control, mundane chores such as valve timing and air-fuel ratio, and operations transparent to the driver such as the connection between the accelerator pedal and throttle. In the foreseeable future, motor vehicles will achieve levels of automation that relieve the human of basic maneuvering tasks or more.

International standard ISO 26262, Road vehicles—Functional safety (2011), an adaptation of IEC 61508 for automotive electric/electronic systems, has been widely adopted by the passenger car industry. Currently, the scope of the ISO 26262 standard applies to road vehicles with gross vehicle mass up to 3,500 kg (7,716 lb). While a standard for heavy vehicles does not currently exist, work is underway to extend the ISO 26262 to include road vehicles of any mass. Being the agency responsible for the safety of motor vehicles, the National Highway Traffic Safety Administration desires that proper safety practices be followed in the design and manufacture of all vehicles, including heavy-duty vehicles.

FUNCTIONAL SAFETY DEFINED

ISO 26262 (2011) defines functional safety as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems." An E/E system in the standard is a "system that consists of electrical and/or electronic elements, including programmable electronic elements." Modern motor vehicles have many E/E systems and other features to improve crash avoidance or deliver customer experience or permit simpler operation. Those systems improve safety in the general sense, but functional safety addresses hazards caused by malfunctioning behavior of any E/E system.

PROJECT GOALS

The purpose of this "Functional Safety Research Considerations for Heavy Vehicles" project is to identify the similarities and differences between passenger vehicles and heavy vehicles from a functional safety standpoint, as well as understand and compare the functional safety practices currently in use in the heavy vehicle industry.

The project's goal is to help provide the foundation for safe, reliable, and secure vehicle systems, while identifying the unique attributes, advantages, or challenges that may be attributable to the various vehicle segments.

This project focuses on two areas: factors that affect functional safety and current industry practices. The report explores factors that affect functional safety as a way of identifying differences between vehicle segments, attributes that necessitate a specialized approach to functional safety, and the effect these unique attributes may have on system engineering, electronics hardware, software development, and other components of functional safety. These factors include truck versus bus platforms, vocational operations, and communication protocols.

The report also explores current industry practices, with the goal of identifying commonly used industry principles to better understand what is (and what is not) dictating functional safety. Research in this area investigates the heavy vehicle system integration process, the relationship between the supplier and OEM, lifecycle management process, challenges related to vehicle modification for recommission and how upcoming shifts, challenges, and technologies may affect functional safety practices in the future.

VEHICLE CLASSIFICATION AND GROSS VEHICLE WEIGHT RATINGS

The research for this project focuses on commercial vehicles—trucks and buses. The weight classes determined by the Federal Highway Administration (FHWA) are displayed in Figure 1. The vehicle weight classes set by FHWA are applied by NHTSA and used consistently by the industry. These classes are based on gross vehicle weight rating (GVWR), the maximum allowable weight of the vehicle plus the weight of the load it can safely carry, as specified by the manufacturer.

In this project, vehicles were categorized as Light Duty (Class 2-3), Medium Duty (Class 4-6), and Heavy Duty (Class 7-8). For simplicity, the term "heavy vehicle" in this report will be used to refer to any vehicle heavier than is currently in the scope of ISO 26262, i.e., any vehicle above 3,500 kg GVWR or 7,716 lb.

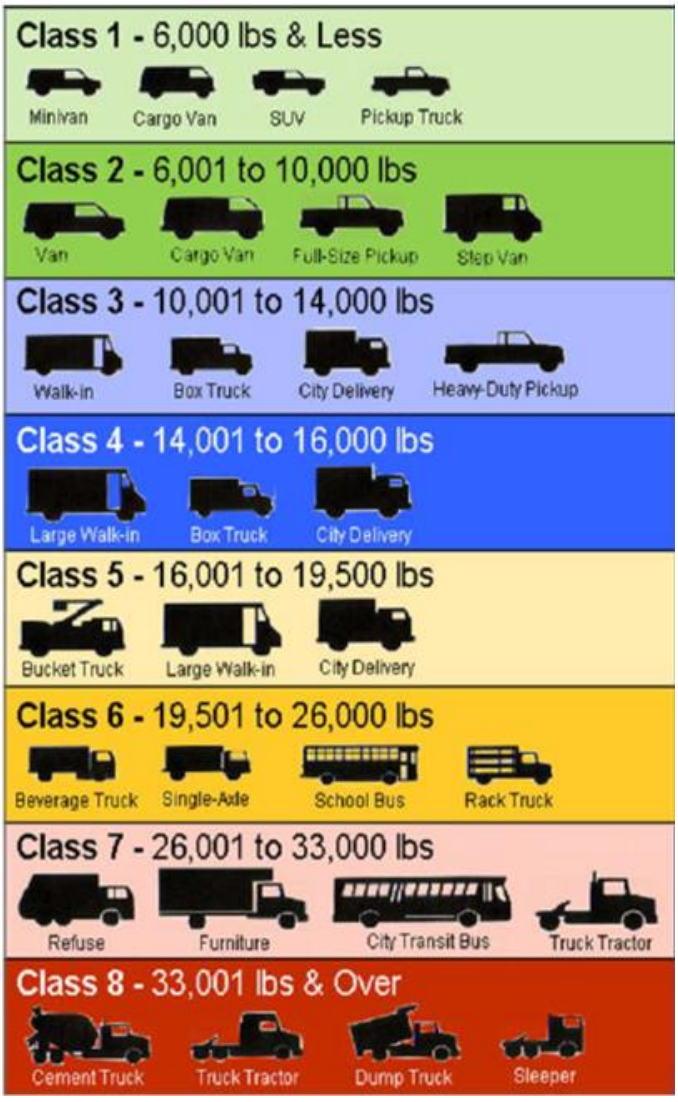

Figure 1. U.S. DOT Truck Classification and Gross Vehicle Weight Ratings

APPROACH

The research to support the Functional Safety Research Considerations for Heavy Vehicles project took on a two-prong approach and included a literature search and industry interviews.

To initiate the project, a Comparison Framework was developed to clearly determine the scope of research and identify key attributes based on vehicle duty class that were relevant to the functional safety of electronics. The attributes were listed in tabular form and included not only the systems onboard the vehicle, but safety factors during all stages of the manufacturing process, deployment, service

usage, and recommissioning. For reference, the Comparison Framework table, which concisely represents the attributes present by vehicle category and their effect on functional safety, is included in **Appendix A**.

Following the development of the Comparison Framework, a literature search was conducted using publicly available online information sources and indexes. The literature search focused on practices, applications, and technologies currently in use by the heavy vehicle segment. Several public and professional databases were searched using the terms "functional safety for medium and heavy vehicles," "electrical/electronic control systems for commercial vehicles," "programmable safety-related systems for heavy vehicles," "software and hardware functions heavy vehicles," "IVS for heavy trucks," and "ISO 26262 applications for heavy vehicles."

Other databases were searched with Boolean combinations of the terms below. Search strategies generally had the form: [functional safety] AND [truck].

- ISO 26262
- Functional safety
- Electronic safety
- Heavy vehicles
- Medium-duty vehicles
- Commercial vehicles
- Industrial vehicles
- E/E
- Formal methods
- Semi-formal methods
- Motor coaches
- Transit buses
- J1939
- Trucks
- Electric/electronic control systems
- ECU
- Safety-critical software
- Safety-critical hardware
- Programmable safety-related systems
- Active safety systems
- IVS heavy trucks
- Safety case or argument
- Connected vehicles
- Systematic failures
- ASIL (automotive safety integrity levels)
- Hazard analysis
- Safety process
- System verification

Approximately 25 abstracts were identified from 2006 to 2016, and after careful review, a portion were selected based on relevancy to functional safety and the heavy truck industry.

Following the literature search, the Battelle team interviewed 10 organizations that spanned the entire heavy-vehicle spectrum. The interview group included manufacturers, suppliers, bodybuilders, end users, and industry and labor associations. They described in detail the integral differences between passenger cars and heavy vehicles and how these differences affect the application of functional safety. Each interview was conducted by telephone and spanned approximately 45 minutes. The Battelle team contacted organizations with diverse perspectives in the heavy vehicle industry, as follows.

- Three manufacturers of medium- and heavy-duty vehicles
- Three suppliers, spanning the passenger car to class 8 markets
- A vehicle body builder
- Three organizations representing users.

Each interviewee was asked to describe the differences between passenger cars and heavy vehicles that might affect functional safety. The interview questions posed focused on the differences in use, functional safety methods, supply chain relationships, electronic and telematics systems, and maintenance practices between passenger cars and heavy vehicles.

The subsequent sections of this report go into greater detail and document the findings and insights of the literature search and industry interviews.

Chapter 2. Factors That Can Affect Functional Safety

The first key goal of this project was to identify the attributes in passenger cars and heavy vehicles that affect the practice of functional safety.

Trucks serve a vastly different purpose than cars. Passenger cars are typically used for personal transportation. Trucks are tools that undergo a range of modification and customization to suit the business' given tasks and needs. The vehicle components, electronic systems, application, and function vary between passenger cars and heavy vehicles. While these differences affect which elements are evaluated, based on the research gathered from published articles and interviews with industry professionals, the fundamentals and methods of functional safety appear to be similar across all vehicle segments.

This section of the report explores the basic differences in functional safety components and approaches for passenger cars and heavy vehicles, and describes why these attributes affect functional safety. It will highlight the differences in systems, development, and use. Some of the statistics in this section are for the United States; much of the discussion applies worldwide.

VEHICLE SYSTEMS

The systems onboard a vehicle include the engine, electrical components, transmission, brakes, wheels, suspension, tires, clutch, steering, lights, and climate and communication controls. The research compiled for this report is limited to onboard electronics. In general, this includes electronics that affect propulsion, steering, and braking. However, heavy vehicles have distinct features not found on passenger vehicles, such as air brakes or mechanical working elements found on vocational vehicles such as dump trucks. While the areas highlighted in the section below are not an exhaustive list of differences between light and heavy vehicles, it is intended to address, at a high level, many of the basic variations between the vehicle industry types.

Propulsion

Passenger cars in the United States are predominantly powered by gasoline engines. In 2014, over 16.4 million passenger cars and light trucks were sold in the United States, and diesel-powered cars accounted for 3 percent of the total sales (BEA, 2015). Alternative powered vehicles, including conventional and plug-in hybrid, battery-electric, flexible fuel, fuel cell, natural gas, and propane occupy market-share in the U.S., at 4.7 percent (NACS, 2013).

Trucks, on the other hand, are almost exclusively powered by conventional fuels, diesel and gasoline. Trucks in classes 3 to 6 are frequently manufactured with a range of propulsion options, including diesel, gasoline, hybridized diesel, and natural gas. The type of propulsion system selected, may vary based on business requirements, acquisition and maintenance costs, anticipated vehicle miles travel, lifecycle, and a host of other factors.

Diesel is the primary propulsion system for heavier trucks, classes 7 and 8, and has been a long-established engine of choice because of its fuel efficiency, durability, and reliability. According to estimates from the U.S. Energy Information Administration, heavy trucks are one of the largest consumers of fuel and consume more than 1.6 million barrels of oil per day, mostly in the form of diesel fuel. Figure 2 illustrates that diesel-powered vehicles represent a small percentage in the United States, and most diesel-powered vehicles are medium and heavy trucks.

To date, there has been significant progress in the development of hybrid options and alternative fuels for heavy vehicles in the marketplace. Hybrid and alternative fuel options tend to be a poor match for heavy vehicle truck duty cycles, but can be effective in several vocations such as drayage, refuse hauling, and bus applications.

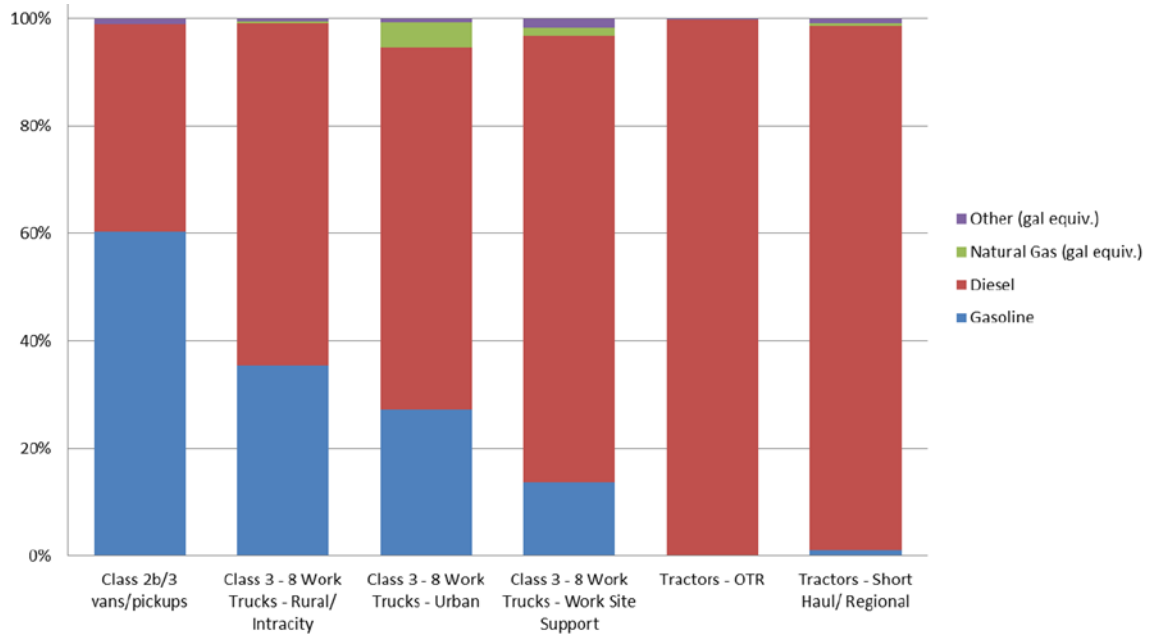

Figure 2. Fuel used by Truck Type and Category (Source: Air Resources Board, 2014)

Controller Area Network Standards

Passenger car manufacturers use proprietary protocols to communicate on the vehicle bus. While passenger car manufacturers use proprietary communications protocols and the message-layer (i.e. lower level of the protocol) contents vary considerably from one original equipment manufacturer (OEM) to the next, the Onboard Diagnostics II (OBD-II) system uses a standard industry protocol.

OBD-II is a computer-based system built into all 1996 and later passenger cars and light-duty vehicles, as required by the Clean Air Act Amendments of 1990.The system is designed to monitor the performance of a passenger car's major engine components, including those responsible for controlling emissions. The OBD-II system is the second generation of the OBD specification and allows for multiple electrical interfaces, which can complicate the hardware used to interface with the vehicle. The controller area network (CAN) is the newest protocol added to the OBD-II specification, and is mandated for all passenger cars with model years 2008 and newer. The CAN standard is a multi-master broadcast serial bus standard that allows electronic control units (ECUs, e.g., brake, engine, electronic fuel injection, automatic gear box, anti-lock braking system) to communicate with each other in a vehicle without a central computer.

In contrast, the communication standard for heavy vehicles is the SAE International's J1939, a an open standard protocol that provides direction for the physical layer, diagnostic connector, and several layers of messaging architecture.

The foreword of the J1939 protocol describes it as a "high speed ISO 11898-1 CAN-based communications network that supports real-time closed loop control functions, simple information exchanges, and diagnostic data exchanges between Electronic Control Units (ECUs), physically distributed throughout the vehicle. The SAE J1939 common communication architecture strives to offer an open interconnect system that allows ECUs associated with different component manufacturers to communicate with each other." Used as an

application layer, J1939 provides communication between the engine control, transmission control, vehicle body control, and other applicable sub-control systems. It also defines message timeouts, how large messages are fragmented and reassembled, the network speed, the physical layer, and how applications acquire network addresses. Because the J1939 protocol is connected under one central network, it enhances vehicle monitoring, management and system serviceability (SAE International, 2011).

While the J1939 standard is open, major modifications to the elements that affect functional safety must be approved by the consensus of the entire heavy vehicle industry. Additionally, proprietary protocols are also being used for heavy vehicles, but to a lesser degree.

Electronic and Telematics Systems

Telematics technology is becoming more and more important to the passenger car and heavy vehicle industry. Part of what is driving the increase in onboard telematics systems is the need to improve maintenance and repairs, fuel efficiency, security, road safety, communication, and navigation.

In passenger cars, telematics and connected vehicle systems can range from roadside assistance, vehicle tracking, vehicle diagnostics, as well as a host of embedded convenience applications such as remote door lock/unlock functions, vehicle remote-start, Wi-Fi hot spots and features for insurance company analytics, fleet management and electronic toll collection. In a report on the automotive OEM telematics market, researchers estimate that nearly 15 percent of all new passenger cars sold worldwide in 2014 were equipped with an OEM embedded telematics system. North America is the most advanced market with telematics systems installed in 34 percent of new vehicles, followed by other developed markets such as Europe, Japan and South Korea with rates of 14 to 15 percent (Malm & Fagerberg, 2014). Because passenger cars all have engines, transmissions, braking systems and suspension systems that operate in similar ways, the telematics that support them are often comparable.

Compared to passenger cars, heavy vehicles have many more electronic and telematics systems available for possible installation. These systems range from applications that help improve fleet management, fuel performance, and maintenance, to weigh-in-motion systems, vehicle location systems, parasitic load and battery power systems, camera event recorders, and collision avoidance systems. While there are more electronic and telematics systems available for trucks than passenger cars, not every system will be installed or available from every heavy vehicle OEM. Compared to passenger cars, the electronics on heavy vehicles have much longer lifecycles. Additionally, trucks have truck-specific functional controllers for chassis, body and in-cab controls, which are not found on passenger cars and influence the type of telematics systems installed.

Braking and Steering

Brake systems on light vehicles are universally hydraulically controlled, except in vehicles with at least partial electric propulsion, which may have a regenerative component to the braking. Brakes on heavy vehicles may be actuated hydraulically or pneumatically or by a combination. Electrically controlled brakes are more common in Europe, where they provide proportioning in combination vehicles. Electronic stability control, now required for both heavy and light vehicles in the United States, selectively applies the brakes on individual axle ends to help the vehicle follow the driver's steering input when the road friction capability is exceeded. Implementation certainly differs with vehicle weight, inertia, and braking mechanism, but the fundamental approach is identical.

Similarly, steering is by a mechanical linkage on most vehicles in all classes. Electric power steering is found in many high-volume for light vehicles, primarily to avoid the energy losses inherent in hydraulic power steering. Electronic controls are in limited use for heavy vehicles, where they reduce hysteresis and driver fatigue.

VEHICLE PRODUCT DEVELOPMENT

For any product, the process used to guide development is critical to success in the marketplace. For passenger cars and heavy vehicles, the development process is multi-layered and involves many different stakeholders to complete a product that is both comprehensive and practically integrated. This section of the report will focus on the business models and supply chain processes in place for passenger cars and heavy vehicles, highlighting their differences and similarities with respect to functional safety approaches.

Organizational Structure and Business Relationships

Passenger car OEMs are vertically integrated organizations, which are a single entity engaged in many parts of production process or owning several steps in the supply chain process to increase market share. As an example, most passenger car OEMs control every aspect of the vehicle's design and manufacture process and are heavily integrated with their suppliers.

In contrast, heavy vehicle OEMs are typically characterized as horizontally integrated organizations. Horizontally integrated companies increase their market share by acquiring similar companies, though the use of mergers and buyouts. As opposed to owning many facets of the supply chain process, heavy vehicle OEMs often assemble components from various suppliers specified by their customers. Specifically, in North America, truck OEMs tend to be more "semi-vertical" in their organization. While they still demand that components (such as engines, transmissions, braking systems, add-on safety systems, etc.) meet their specifications, many times these components are supplied by third parties. These systems are readily available, easy to integrate into a vehicle and satisfy the customer's demands. While the components meet the performance, reliability and safety specifications from the vehicle OEM, the vehicle OEM is not in control of the design specifications, process, or manufacturing.

Another area that differentiates functional safety approaches in heavy vehicles is the business models and working relationships. The passenger car industry has vastly different working relationships between the OEM and supplier. For example, in the passenger car and light-duty vehicle industry, the OEM is very much in control. The OEM provides the supplier with a detailed list of requirements (e.g., what types of ECU system to include in the vehicle) and initiates the hazard analysis process before engaging the supplier. The supplier may not be provided with details from the full hazard analysis or even know the full purpose of the components it is supplying. Using a Development Interface Agreement (DIA), the supplier assumes responsibility for its respective interface levels, however the OEM carries the sole responsibility for a system's functional safety at the vehicle level.

In the heavy vehicle industry, the supplier often assumes control for innovations. The supplier designs a product based on an industry need. The supplier then sells the product to an OEM. The product is developed using the System Element out of Context (SEooC) methodology. A SEooC is a safety-related element developed in isolation and without the context of a specific item. Therefore, the element developer makes assumptions on the context of an SEooC, in the form of requirements that are likely to be allocated to its environment. The difference between a regular element (part of an item) and a SEooC is that a SEooC makes assumptions on a general environment, while an element is to be integrated in a specific environment. The concept of SEooC addresses the need of third-party suppliers—an important aspect in the automotive industry since many OEMs rely on sub-systems developed external to the company (Westman et al., 2013). As per ISO 26262 part 10, vehicle components are permitted to be developed independently from their usage context, if assumptions are documented. The vehicle OEM is required to map the safety requirements provided by the SEooC component supplier to safety requirements derived for the vehicle element to ensure adequacy. Essentially, the SEooC process allows component suppliers to develop safe practices without regard to how their components will be used.

Product Specification

Passenger vehicles can be purchased “off the lot” from dealers or from specialty manufacturers. While customers can select options, many of these features are pre-selected by the manufacturer and offer limited customization. Additionally, passenger car OEMs have little or no direct relationship with their customers. It is the passenger car dealer that has the direct relationship with the customer. By contrast, heavy vehicle OEMs generally have close working relationships with their customers. Because heavy vehicles are tools that generate revenue for the customer, the customer has specific needs for these tools and works closely with the heavy vehicle OEM to get the best tool for the business. As a result, the number of options, modifications and variants in heavy vehicles is much greater than in passenger cars.

Heavy vehicles have a much greater number of options in size, number of axles, and safety features. The engine (manufacturer, horsepower rating, fuel type, etc.), transmission (manufacturer, manual, automated manual, fully automatic, etc.), driveline, differential, axle (manufacturer, axle ratio, weight ratings, etc.), braking and safety systems (manufacturer, automatic brake system, advanced automatic brake system, stability control, autonomous cruise control, etc.) and other features are selected by the customer. The specification for a truck tractor can run five pages, covering everything from axle rating to the mattress in the bunk. Fleets, particularly, are savvy and detailed in their specifications. This great variety of possibilities requires great attention to the integration of components and their proper functioning as a system.

Testing

Passenger cars and heavy vehicle OEMs run rigorous tests and inspections based on strict safety standards and regulations before entering the marketplace. For both passenger cars and heavy vehicles, the Federal Motor Vehicle Safety Standards (FMVSS) guide performance and safety testing in the United States. FMVSSs, first issued in 1967, are defined as the minimum requirements for motor vehicles and equipment to protect the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a vehicle. Motor vehicle manufacturers and equipment suppliers must conform and certify their compliance. NHTSA has a legislative mandate to issue FMVSSs, and manufacturers and suppliers of motor vehicles must certify compliance. Passenger car and heavy truck OEM also employ advanced testing to assess handling, suspension, braking, crash avoidance, durability, quality, and other critical vehicle components and systems.

While passenger car manufacturers may run crash tests frequently to verify compliance with regulatory standards, the greater unit cost of heavy vehicles precludes frequent crash testing. Changes to heavy vehicle structural components, steering, braking, and safety systems happen much less frequently than passenger car changes, and manufacturers adjust the crash testing schedule accordingly. Both passenger cars and heavy vehicles undergo extensive performance and safety testing; however, the high volume of production for passenger cars allows for the allocation of additional resources to conduct multiple tests to demonstrate compliance.

VEHICLE USE

For passenger cars, the weight and size of a vehicle drive the functional safety approachs used. Depending on the materials used during production, the engine size, and vehicle class, there can be significant variation in passenger car weights. Because passenger vehicle safety standards are based on the weight and size of a vehicle, it is directly tied to the approaches used to assess functional safety risks and exposure.

In contrast, for heavy vehicles, the base vehicle type is the main driver of functional safety approaches. Heavy vehicles and buses are categorized by base vehicle type, which include long haul, distribution, trailers, and coaches. Quantifying the independent effects of base vehicle type, body type (i.e., if it will be used for vocational applications), and use (i.e. cargo loading, with or without a trailer) is far more important for heavier vehicles in the assessment of risk and functional safety than is weight, as applied to passenger cars.

Figure 3. Photos of Truck and Bus Base Vehicle Types

Demographics and Market Size

In 2014 the most recent data available, there were approximately 16.44 million passenger vehicles sold to customers in the United States and over 88.6 million passenger vehicles sold around the world. According to the Energy Information Administration (2015), the 2015 global passenger vehicle fleet is approximately 830 million and the U.S. fleet is about 230 million. More passenger vehicles than heavy vehicles are produced in the United States and around the world.

The market size for medium and heavy trucks is a relatively small segment in the motor vehicle industry. In 2014, medium and heavy-duty truck sales amounted to 415,000 units in the United States. While there are far fewer medium and heavy trucks on the road, the bulk of industrial and consumer goods are transported by this vehicle segment. As a result, they consume over 20 percent of the fuel used for transportation in the United States, due to heavier gross weights and high mileage.

Based on an industry survey taken of over 200 fleet managers in 2012 (Figure 4), most of truck carriers have class 6 to 8 trucks, and most fleets include truck tractors. The survey allowed for multiple responses and asked, “What type of trucks does your fleet currently utilize?” and “Which of the following classes of vehicles do you currently have in use in your entire fleet?” (Kar, 2012).

U.S. Type of Fleet Trucks, 2012	
Type	Percentage of respondents with the vehicle in their fleet
Tractor	94%
Straight	59%
Other	4%

U.S. Class of Trucks, 2012	
Class	Percentage of respondents with vehicles of the class in their fleet
Class 1 to 3	41%
Class 4 to 5	36%
Class 6 to 8	99%

Figure 4. 2012 U.S. Truck Demographics—Type and Class (Source: (Kar, 2012)

Product Lifecycle

Passenger vehicles are purchased for individual, family, business, and rental use. In nearly every case, these vehicles are used for personal commuting (to or from work or events), shopping, and light transport. Most of the vehicle's life is in the "Park Mode." While car enthusiast clubs exist and custom modifications are made for street-legal vehicles, the percentage of affected vehicles is small.

The typical lifecycle for a **passenger car** vehicle is as follows.

- Concept and design
- Manufacture and deliver to dealer
- Purchase
- Drive
    - Short trips (<5 miles)
    - Medium trips (5 to 50 miles)
    - Long trips (>50 miles)
- Maintenance
    - Oil changes
    - Windshield Wipers
    - Lamps
    - Accessory Belts
    - Other routine maintenance
- Decommissioning: sell or trade in
- Repeat until an average of 8 years or 150,000 miles – the upper end of the curve is 12 years and 300,000 miles

A truck, on the other hand, is a tool. This tool is overwhelmingly owned by businesses. A truck fleet can range from a single vehicle to thousands. These (and the vehicle operators) are the prime tools used by these businesses to make money. The goal is for the vehicle to spend most of its time on road, hauling freight or performing its specialized tasks. The life of a medium or heavy truck begins with the selection of vehicle type, function, manufacture, and post-manufacture modifications and then follows a similar product lifecycle as light vehicles.

The typical lifecycle for a **heavy vehicle** is as follows.

- Concept and design
- Selection of vehicle type
    - Road vehicles
    - Vocational vehicle
- Selection of vehicle function (Air Resources Board, 2014)
    - Work site support
        - Utility, construction, etc.
        - Considerable idle time and PTO use
    - Rural or intracity
        - Cargo, freight, delivery collection
        - Higher vehicle miles traveled (VMT); higher average speed; combined urban or highway

- Urban
    - Cargo, freight, delivery collection
    - Lower (VMT); lower average speed; lots of stop and start
- Short haul or regional
    - Between cities, drayage, day cabs
    - Includes second-use trucks; trucks with smaller engines
- Over the road (long haul)
    - Younger trucks; high annual VMT
    - Mostly higher average speed, highway driving

- Manufacture
    - Class 4-7: May be built in a single stage. In many cases, a chassis manufacturer builds the cab and chassis and then a body builder builds the remainder of the vehicle.
    - Class 8: broken into manufacturers that build the tractor, engine, powertrain (including transmission) and an industry that manufacturers the trailer
    - Heavy-duty trucks are diverse and serve a variety of vocational applications from Agriculture, Construction to traditional long-haul trucking
- Post-manufacture modifications
    - Additional decorative lights added
    - Additional work lights added
    - Modifications to the frame, chassis, or body. Examples:
        - School bus
        - Transit bus
        - Tour bus
        - Snow plow or dump truck
        - Refuse truck
        - Tow truck
        - Concrete mixer
        - Concrete pumper
        - Automatic mulch spreader
        - Oilfield pumper
        - Mobile crane
        - Ambulance or rescue
        - Fire truck
        - Law enforcement

- Purchase
- Drive
    - Average of 100,000-200,000 miles per year
    - Trucks can travel more than a million miles over their lifetime
- Routine maintenance

- Decommissioning: repurpose or sell
    - Trucks often have multiple lives. For example, a Class 8 over-the-road vehicle is often sold and repurposed to perform the function of regional haul vehicle. A Refuse Truck may become a Pickup and Delivery truck – having its former modifications exchanged for a simple transit box.
- Disposal
    - Medium and heavy trucks have relatively long-life spans, upwards of 14 to 20 years depending on their duty cycle, level of maintenance, and abuse.

Maintenance

Passenger car maintenance practices are largely the responsibility of the end user, and include conducting basic preventive maintenance routines in a timely manner to identify vehicle problems and keep the vehicle systems in good repair. Maintenance services can be performed at a dealership or with a private mechanic. A passenger car fleet manager will typically develop and adopt a maintenance plan based on best practices to provide safe, comfortable, and reliable transportation to users. A single end user will likely reference the manufacturer's recommended maintenance schedule to conduct routine repairs and inspections.

Because heavy vehicles are business tools that generate income, the level of service and maintenance is considerably higher than that of a typical passenger car. Like dealers that sell and service passenger cars, heavy vehicle distributors both sell and service vehicles. Typically, large carriers have sophisticated maintenance staff and processes to keep vehicles up to specification. Owner-operators generally have their trucks serviced and repaired at the dealer, distributor, or a maintenance facility.

SUMMARY

The information used to review and assess the key factors affecting functional safety were largely formulated from interviews with industry experts. Based on the interviews, the key factors affecting functional safety can be summarized as follows:

Heavy vehicles are used for **different purposes** than passenger cars. Passenger cars are typically used for personal transportation. Heavy vehicles are tools for the needs of a business. Trucks and buses may undergo a range of modification and customization to suit those needs.

- The passenger car and heavy vehicle industries have **different business models**. Responsibilities need to be clearly allocated in the supply chain (manufacturer, supplier, body builder).
- The **volume** of passenger car production is orders of magnitude above that of heavy vehicles. As a result, the heavy vehicle industry cannot allocate the same level of resources to product development, including functional safety.
- Some, but not all, of the differences between passenger cars and heavy vehicles affect the way that functional safety is practiced. Only some of those differences will require significant changes to ISO 26262.

Chapter 3. History of Functional Safety

The second goal of this project is to document current industry practices in applying functional safety. This section of the report reviews industry standards that have influenced and shaped functional safety for all vehicle segments and in more depth, explores the functional safety practices and adaptations for heavy vehicles in use today.

The safety of electronics has always been a concern; as electronics have become more complex, the analysis has had to become more formal. With the release of ISO 26262 in 2011 the light vehicle industry had a common voluntary standard. The heavy vehicle industry continues its existing practices, with some organizations moving toward ISO 26262 more deliberately and more fully than others.

THE INCREASING COMPLEXITY AND IMPORTANCE OF ELECTRONICS

With the advent of solid state electronics, and following the continuing trend towards miniaturization and increased complexity of microprocessor-based control systems, many industries use microelectronics to implement control systems with embedded hardware and software systems. Microelectronic and microprocessor-based control systems find applications in consumer and industrial systems, including nuclear power, space flight, commercial transportation, and automotive applications. Historically in the United States, governmental and commercial system safety assurance processes have adhered to one or more Department of Defense standards, such as MIL-STD-882, which covers a variety of safety assurance analyses and processes. Subsequent industry-specific standards will often refer to these DoD standards as a baseline. Internationally, standards developed in the European Union, starting with CENELEC and moving to IEC standards, typically govern safety assurance processes, and these international standards use similar tools and methods as domestically applied standards.

As microelectronic and embedded hardware and software systems have become more prevalent, each industry developed standards for system safety assurance or adapted more generally standards for the specific needs of that industry. For example, the nuclear power industry requires that control systems maintain fail-safe operations always, but due to the significant costs of shutting down a nuclear reactor, high availability is critical to maintain efficient system operations. To support this, the nuclear industry developed a fault tree analysis (FTA) methodology, documented in the *Fault Tree Handbook* published by the Nuclear Regulatory Commission (Vesely, 1981).

As another example, NASA also uses FTA as part of its safety assurance process, but adapts the analysis to a considerably different operating environment. While nuclear applications require high availability, but can fail safely to a shutdown state, such an outcome would not be acceptable during spaceflight. In this case, the analysis performed by NASA for safety assurance must demonstrate that a space flight system (particularly where human spaceflight is concerned) must “fail operational,” or continue to operate at full or partial function, such that the mission can be completed. A further differentiating factor for spaceflight is that the mission time for a spaceflight is of relatively short duration, days or weeks, versus the continuous decades-long lifetime of a nuclear reactor. The takeaway from this is that the safety assurance methodology applied must be appropriate to the potential severity of an accident and the operational profile for the system, including environment and operating duration.

For passenger vehicles in the United States and internationally, ISO 26262 is applied in general for functional safety of electronic systems. This standard, in turn, is an industry-specific instance of the general IEC 61508 functional safety standard, tailored to the automotive industry. Similar to the CENELEC 50126/50128/50129 standards for the rail industry, the ISO 26262 advocates the “V-Model” approach to system safety assurance, with design documentation becoming increasingly finer in granularity as the design matures, and each successive iteration into the depth of the design is verified and validated with analysis and

testing at a similar level of detail, ensuring that the implementation of subsystems is a true representation of the requirements developed at the higher, system level.

The ISO 26262 standard now covers some heavy vehicles, but until it covers all the heavy vehicle manufacturing industry must still assure vehicle safety, without the benefit of a codified standard.

IEC 61508

Typical practice for safety assurance follows a process wholly or in part derived from MIL-STD-882. In more recent years, standards from Europe have gained acceptance in industry with the intent of streamlining the safety assurance process by using a common standard both in the US and internationally. IEC 61508 is a basic functional safety standard, intended to be adapted to any given industry. IEC 61508 provides a body of analytical tools and methods for demonstration of system safety in a Safety Case, and integrates the principles that:

- Zero (safety) risk can never be reached;
- Safety must be considered from the beginning of the system design process;
- Any safety risk that cannot be tolerated must be eliminated or mitigated to as low as reasonably practicable (ALARP principle);
- Safety Integrity Levels (SILs) are used to characterize subsets of system function based on how critical that function is to system safety, and thereby the level of safety evidence that must be provided to ensure that that subsystem will meet its safety target (such as an unsafe failure rate of less than 10^{-9} failures per hour)

IEC 61508 was adapted as ISO 26262 for the automotive industry, as discussed below.

CURRENT PRACTICES IN THE HEAVY VEHICLE INDUSTRY

When ISO 26262 was published in 2011, the practice of functional safety was not new in the automotive industry. The standard codified practices that were already in place. Similarly, corporations in the heavy vehicle industry had and still have existing practices and policies for developing new products.

While the scope of the current ISO 26262 standard excludes some heavy vehicles, discussions with manufacturers, suppliers, bodybuilders, end users, and industry associations, affirm that the methods to achieve functional safety have been commonplace for many years in the heavy vehicle industry. Interviewees spoke to the differences between passenger cars and heavy vehicles, but few cited differences in how functional safety is approached. Because many U.S. suppliers have a presence in both the passenger car and heavy vehicle markets, they already apply ISO 26262 to some extent. They note that ISO 26262 can be applied to heavy vehicles with little modification. Two of the suppliers of components for heavy vehicles reported that they continue to follow IEC 61508.

Many of the heavy vehicle manufacturers and suppliers referenced their own internally developed systems engineering or functional safety process. They use hazard analysis at the beginning to identify which components require the most attention. A risk assessment might lead to a new test or an improved process control. Several said they use failure mode and effects analysis (FMEA). Also mentioned were Automotive Software Process Improvement and Capability Determination (SPICE), Capability Maturity Model Integration (CMMI), regression testing, modeling, and electromagnetic compatibility testing. These tools are all consistent with ISO 26262.

PUBLISHED EXAMPLES OF ISO 26262 ADAPTED TO HEAVY VEHICLES

The literature search documented industry processes, methods, and applications of functional safety in heavy vehicles. The industry is known to apply practices such as FMEA, fault tree analysis (FTA), and event tree analysis (ETA) to address functional safety. However, several published materials spoke to advanced software tools, model-based approaches for fault and failure detection, and connected vehicle applications to achieve or enhance functional safety. Additionally, some organizations have adopted standards and processes like ISO 26262 to provide a measure of functional safety. While the literature search was conducted using several broad databases, many of the projects related to subcontractor Volvo in one way or another, a prolific publisher in this field. Projects by other organizations were found as well. Below is a summary of these documented functional safety approaches.

The VeriSpec Project: Formal Verification Tools

To address the challenges associated with functional safety and ISO 26262 adoption, Scania, a major Swedish commercial vehicle manufacturer, has partnered with Volvo Group Trucks Technology and Mälardalen University College to launch a joint research project on formal verification tools. The project is funded by VINNOVA, a Swedish research and development agency that seeks to develop new as well as adapt existing modeling and verification techniques for the analysis of requirements and architectural models of automotive systems. These methods and processes could be seamlessly integrated in the industrial methodology of system development. The project aims to develop a language by which requirements can be formalized, methods for automatic verification of architectural models can be referenced against requirements, and a compatible framework can be developed and applied in an industrial setting. The Verispec project will align itself with several other research projects relevant to heavy trucks, including MAENAD and SafeCer (Rodriguez-Navas et al., 2014).

SafeCer: Certification Guidelines

Safety Certification of Software-Intensive Systems with Reusable Components (SafeCer) was an international research collaboration that sought to increase efficiency and reduce the time and costs associated with the qualification, certification, and verification of safety systems. According to the research, qualification, certification, and verification of systems can account for more than 75 percent of all development costs. The goal of SafeCer (2013) was to develop a framework for compositional development and certification of safety systems, as well as certification guidelines for motor vehicles and other industry domains, including construction equipment, avionics, and rail.

The SafeCer initiative was led by several companies across Europe and includes OEMs, tool providers, and certification and standardization experts. The automotive-specific features of the SafeCer certification and verification methodologies have received guidance from the Volvo Group. In addition, Delphi, a global supplier of technologies for the automotive and commercial vehicle market, has been identified as the developer for the heavy vehicle embedded software. The SafeCer project and the process and methodologies developed from it will provide support for system safety arguments, and support for safety-related software reuse. By supporting the efficient reuse of systems and subsystems, stronger links will be created between certification and development, ultimately increasing quality, reliability and competitiveness.

The SafeCer Project was divided into two sub-projects, pSafeCer and nSafeCer. The pSafeCer project began in 2011 and consisted of planning and concept development. The nSafeCer project began in 2013 and took the concepts developed in pSafeCer and advanced them into tangible industrial implementations of project-ready solutions, using a demonstration and proof-of-concept. The project and solutions generated from the SafeCer project received funding through 2015.

Product Lifecycle Management for Heavy Trucks

In 2003 Volvo 3P initiated a process to develop a common embedded real-time E/E architecture for its next generation of Mack, Renault, and Volvo Trucks (as of 2012, Volvo 3P became Volvo Group Trucks Technology). The goal of the system was to manage all three E/E systems under one comprehensive information management system, offering a single source for development and implementation. After a year-long evaluation of over 20 different solutions, Volvo chose the SystemWeaver (Systemite AB, n.d.) platform, based on its clear product lifecycle management approach, performance, scalability and total system cost. The information used to model Volvo's process was highly inspired by EAST-ADL and AUTOSAR (ATeSST, 2010), two methods of describing and formalizing automotive software architectures. Named SE-Tool, it allows for different levels of abstraction to improve the possibility of reuse, supports concurrent engineering without the risk of endangering the integrity of the system, and formalizes Volvo 3Ps requirements and specification development process using a model-based approach.

Connected Vehicle Data Applications for Remote Diagnostics in Heavy Trucks

In 2015 the Volvo Group set out to demonstrate how connected vehicle data could be applied in the development of commercial vehicle diagnostic methodology. In recent years, the increase and integration of electronic control systems and components has resulted in more diagnostic codes that indicate below average vehicle performance or complete system failure. Operationally, the failures that are flagged by these codes have resulted in unplanned stops, truck breakdowns, and commercial goods arriving late or not at all.

The new remote diagnostic method was developed using traditional troubleshooting charts for inspections, with case-based reasoning knowledge (the process of solving new problems based on the solutions of similar past problems), and input from connected vehicle data. The new model captured relationships between diagnostic trouble codes and vehicle operation data. The proof of concept was tested on 1,500 trucks, with vehicles being split into control and test groups. Integrating the remote diagnostic trouble code model algorithm with the connected vehicle service architecture into the test group yielded results that were 61 percent better than the control group, measured by the overall improvement in efficiency, total labor repair time, and reduction in service costs. Based on these results, future developments in the remote diagnostic method have been recommended, as well as a return on investment study to evaluate the method's full market and cost reduction potential (Silva, 2015).

Industrial Applications of a Model-Based Approach for Software Lifecycle

CNH Industrial and Iveco are two Fiat Group companies that design and manufacture a range of light, medium, and heavy commercial vehicles. They documented and compared their former process with their new model-based approach for electronic control unit software development. To streamline their process, CNH Industrial and Iveco began by developing coding cooperation agreements with internal and external engine ECU suppliers, pursued a model-based approach for requirements and specifications, built a central repository of vehicle and engine functions, and streamlined their software development process under one common system. After reinventing their former engine electronic control systems process, CNH Industrial and Iveco

- Observed a reduction in the amount of time required to fulfill the design requirements of the lifecycle process;
- Were better able to anticipate risk earlier in the design phases;
- Increased the effectiveness, and timeliness of the system verification lifecycle; and
- Could satisfy elements of functional safety standards, such as ISO 12207 (Systems and software engineering), ISO 26262, Road vehicles, ISO 25119, Control systems for agriculture and forestry tractors, and ISO 13849,, Safety of machinery (Cortese, 2014).

Application of ISO 26262 Safety Case Requirement to a Heavy Truck E/E Subsystem

In 2012 Scania, a global manufacturer of heavy trucks, set out to apply the ISO 26262 safety case logic to its Fuel Level Estimation and Display System (FLEDS). Scania considers the FLEDS to be safety critical because an unexpected loss of fuel would lead to engine failure and loss of power assisted steering. The article documents the process used to support both process- and product-based safety case arguments. Based on the manufacturer's existing internal quality management and safety processes, researchers could collect information such as requirements definitions, item definition, hazard analysis using FMEA, and system design specifications. The rigorous documentation required to build a safety case consistent with ISO 26262 had not previously been part of the organization's process, and the article lists many lessons learned in this first application of the standard. Among the lessons learned were the finding that discussing the standard with employees developed interest, the company's traceability of documents needed to be improved, and a modular approach that follows patterns tends to ease the development of a well-structured safety case (Dardar Et al., 2012).

E/E Heavy Vehicle Hardware Application of the ISO 26262 Standard

In a student thesis (Johansson & Karlsson, 2015), an analysis was conducted to see how equipped the Volvo Group Truck business line would be if the standard were to be adopted for the engine brake control system. The case study focused on hardware elements of the engine brake control system and explored various methods to improve the existing system. Although ISO 26262 does not apply to the system, the report found that the system could be brought in compliance without deploying a significant amount of resources or introducing a large amount of new hardware. The report recommended the inclusion of a high-side switch, to complement the existing low-side switch, allowing the control system's actuator to disable in the event of system failure or fault. The lack of standardized methods for assessing safety mechanisms was a challenge in applying ISO 26262. The author recommended that these mechanisms be developed in in collaboration with industry partners to reduce the time and cost of implementation.

EAST-ADL2 and AUTOSAR Modeling Languages

EAST-ADL is an Architecture Description Language (ADL) developed in 2000. Since then, several internationally funded projects have refined the language. EAST-ADL provides a comprehensive approach for describing automotive electronic systems in a standardized form. It is closely aligned with the AUTOSAR standard and complements it with respect to functional structure, vehicle features, requirements, analysis functions, software and hardware components and communication safety properties. Both EAST-ADL and AUTOSAR address the model-based development process of embedded automotive systems. Together, EAST-ADL covers the function and system architecture elements and AUTOSAR covers the system configuration and software architecture elements.

SUMMARY

The above information is a scan of published reports and documents on functional safety applications for heavy vehicles. The literature search did, however, reveal some common themes, which included functional safety challenges for heavy vehicles, functional safety adaptations, and future developments in functional safety for heavy vehicles. A summary of these findings is below.

Challenges

- The functional safety challenges related to heavy vehicles fell into two categories: technical and organizational.
    - The technical challenges stem from a lack of technological advances in the design process and minimal use of formal verification methods. These issues are not unique to the heavy vehicle industry, but were mentioned or implied in many of the publications.
    - Many of the functional safety challenges faced by the heavy vehicle industry lie in the organizational process. These issues include the late stage in which functional safety falls in the development process, the lack of a clear decision model (cost, quality, or time-to-market) for choosing a functional safety architecture, development activities being traditionally human-intensive, and the lack of document automation and traceability, to name a few.

Functional Safety Adaptations for Heavy Vehicles

- A small number of projects published their application of functional safety principles to systems on heavy vehicles.
- These applications include the adoption of advanced software tools to increase automation and traceability, model-based approaches to better detect failure, integration with other advanced technologies such as connected vehicle applications, and emergent guidelines and standards to achieve functional safety goals.

Chapter 4. Anticipated Changes in ISO 26262, Version 2

The current version of ISO 26262, published in 2011, provides functional safety guidance to road vehicles under 3,500 kg or 7,716 lb., excluding heavy trucks and buses. This chapter discusses changes to accommodate trucks and buses. At the time this report was written, the update was in the committee draft stage, with balloting to begin. By the time this report is published, it is expected a revised version will have been released as a draft international standard for public comment. Therefore, this report describes anticipated changes only at a high level.

Figure 5 is an outline of ISO 26262, showing the parts of the standard where modifications are being planned for trucks and buses. "T&B" on the graphic signifies trucks and buses.

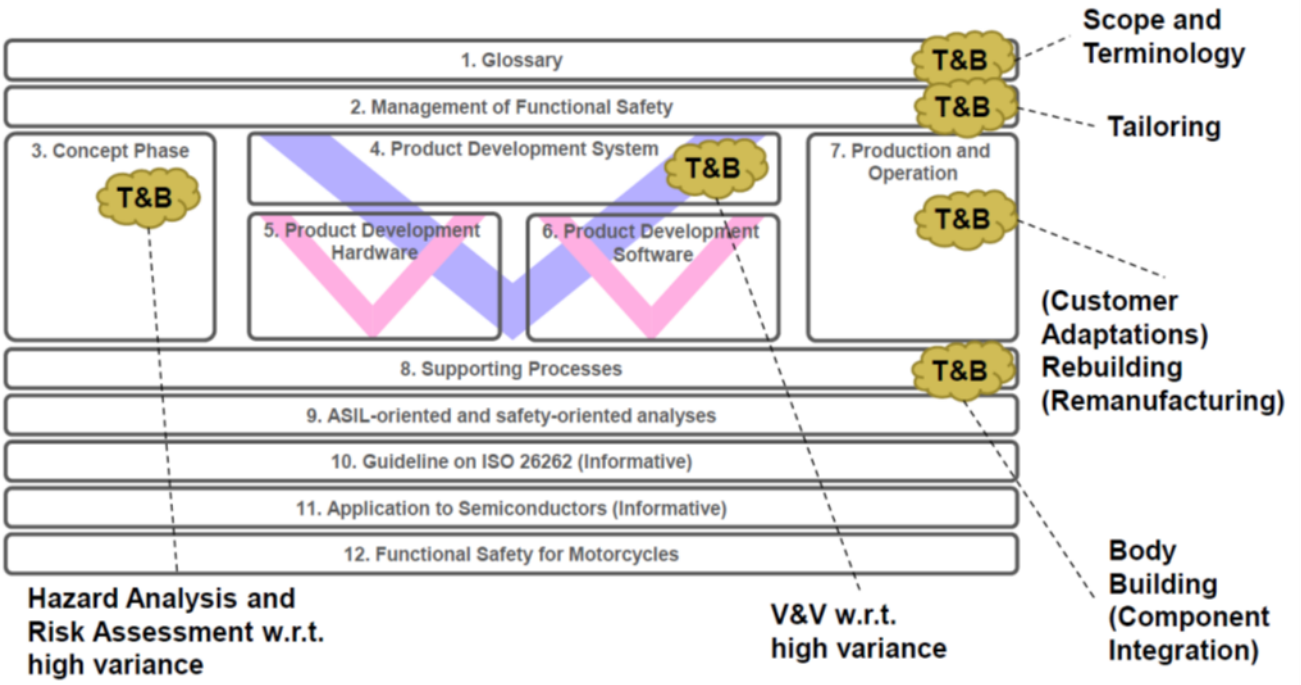

Figure 5. ISO 26262 Second Edition With Truck and Buses (Johannessen, 2015)

The revised ISO 26262 will have clear definitions and examples of truck and bus types and configurations, with specific requirements for hazard analysis and risk assessment for these vehicles. Vocational equipment will be outside the scope of the standard.

Risks are assessed by three factors: exposure, controllability, and severity. These factors jointly produce the Automotive Safety Integrity Level (ASIL). This same structure will be retained in the updated standard, with new informative examples to aid in assigning ratings for trucks and buses.

One of the factors that makes trucks and buses significantly different from passenger cars is the high variance and degree of customization. For example, a tractor may be sold with engines of different horsepower and from different suppliers. The new standard is expected to provide steps to assess the risks of the many variants and to perform verification and validation testing.

Chapter 5. Conclusions

The goals of this report were (1) to identify the major differences between light and heavy vehicles that necessitate a specialized approach to functional safety and (2) to explore how functional safety is applied and adapted in the heavy vehicle industry, outside the scope of ISO 26262. The information gathered for this report was largely formulated from published literature and interviews with industry professionals with a working knowledge of how and why functional safety approaches differ between light and heavy vehicles. Based on information compiled from these sources, the research team concluded that the factors that require a distinct functional safety approach between passenger cars and heavy vehicles are the supply chain relationships among the OEM, supplier, and customer; and the variation of vehicle use.

The difference in product life cycle approach and supply chain relationships between passenger cars and heavy vehicles directly affect who, in the chain, is responsible for functional safety assurance. Passenger cars are typically used for personal transportation. Heavy vehicles are used for business purposes and undergo a range of modifications to suit the needs of a business. The degree of modification and how the vehicle will be used by the end customer directly affect the type and degree of functional safety approach employed. Despite the differences that exist in vehicle components, electronic systems, application, and function between passenger cars and heavy vehicles, the fundamentals and methods of functional safety are similar across all vehicle segments. To facilitate the standardization and sharing of best practices regarding functional safety, the second edition of ISO 26262 will include heavy vehicles. The updated standard is expected to include guidance on specific requirements for hazard analysis and risk assessment and process support for managing variance and differing base vehicle types.

Appendix A.
Heavy Vehicle Framework for Functional Safety of Electronics

Heavy Vehicle Framework for Functional Safety of Electronics

Framework Element \ Vehicle Class	Passenger (for reference)	Light Duty (Class 1-3)	Medium Duty (Class 4-6)	Heavy Duty (Class 7-8)
Subsystems – Engine	• Starter • Alternators • Compressors • Pumps • Fuel injection • Sensors (i.e. oxygen) • Ignition	• Starter • Alternators • Compressors • Pumps • Fuel injection • Sensors (i.e. oxygen) • Ignition	• Starter • Alternators • Compressors • Pumps • Fuel injection • Sensors (i.e. oxygen) • Ignition	• Starter • Alternators • Compressors • Pumps • Fuel injection • Sensors (i.e. oxygen) • Ignition
Subsystems – Transmission	• All wheel drive • Front wheel drive • Rear wheel drive • Synchronous transmission	• All wheel drive • Front wheel drive • Rear wheel drive • Synchronous transmission	• Multiple drive wheels • Non-synchronous transmission	• Multiple drive wheels • Non-synchronous transmission
Subsystems – Braking	• Anti-lock brakes • Electronic parking brakes • Tend more toward disc brakes	• Anti-lock brakes • Electronic parking brakes • Tend more toward disc brakes	• Anti-lock brakes • Trailer hand brakes • Tend more toward drum brakes	• Air brakes (trailers) • Multi-trailer brakes • Anti-lock brakes • Trailer hand brakes • Tend more toward drum brakes
Subsystems – Steering	• Power steering • Input to ESC	• Power steering • Input to ESC	• Mechanical linkages • Input to ESC	• Mechanical linkages • Input to ESC
Subsystems – Suspension	• Shocks, struts • Interface with Electronic Stability Control (ESC)	• Shocks, struts • Interface ESC	• Shocks, struts • Interface ESC	• Shocks, struts • Interface ESC
Subsystems – Auxiliary	• N/A	• Trailer interface	• Towing rig • Bucket truck • Power take off (PTO) • Trailer interface	• Dump truck controls • Power take off (PTO) • Trailer interface

Vehicle Class / Framework Element	Passenger (for reference)	Light Duty (Class 1-3)	Medium Duty (Class 4-6)	Heavy Duty (Class 7-8)
Subsystems – Electrical	• Electronic Control Unit (ECU) • Exterior lighting • Interior lighting, instrument panel • Intelligent Vehicle Systems (ESC, traction control, collision-imminent braking, adaptive cruise control, lane keeping assistance, vehicle-to-vehicle systems)	• ECU • Exterior lighting • Interior lighting, instrument panel • Intelligent Vehicle Systems (ESC, traction control, collision-imminent braking, adaptive cruise control, lane keeping assistance, vehicle-to-vehicle systems)	• Ruggedized ECU • Additional ECUs for engine, transmission control, auxiliary equipment control • Exterior lighting • Power-line communication • Interior lighting, instrument panel • Intelligent Vehicle Systems (ESC, traction control, collision-imminent braking, adaptive cruise control, lane keeping assistance, vehicle-to-vehicle systems)	• Ruggedized ECU • Additional ECUs for engine, transmission control, auxiliary equipment control • Exterior lighting • Power-line communication • Interior lighting, instrument panel • Intelligent Vehicle Systems (ESC, traction control, collision-imminent braking, adaptive cruise control, lane keeping assistance, vehicle-to-vehicle systems)
Telematics	• Entertainment systems • Backup cameras	• Entertainment systems • Backup cameras • Electronic Logging Devices	• Entertainment systems • Fleet management (GPS, speed monitoring, hard brake) • Backup cameras • Electronic Logging Devices	• Entertainment systems • Fleet management (GPS, speed monitoring, hard brake) • Backup cameras • Electronic Logging Devices
Mechanical Components	• N/A	• N/A	• Working elements (e.g., tow rig, bucket)	• Working elements (dump truck)
Pneumatic Systems	• Tire pressure monitoring	• Tire pressure monitoring	• Tire pressure monitoring • Automatic tire inflation	• Tire pressure monitoring • Automatic tire inflation

Vehicle Class / Framework Element	Passenger (for reference)	Light Duty (Class 1-3)	Medium Duty (Class 4-6)	Heavy Duty (Class 7-8)
Development and Manufacturing	• Single-factory assembly	• Mostly single-factory assembly • Some applications involve body-builders after the frame is manufactured. • Coordination of interfaces between OEMs, bodybuilders, suppliers.	• Involvement of body-builders after the frame is manufactured. • Coordination of interfaces between OEMs, bodybuilders, suppliers. • Software development across multiple manufacturers	• Involvement of body-builders after the frame is manufactured. • Coordination of interfaces between OEMs, bodybuilders, suppliers. • Software development across multiple manufacturers
Use-related – Electrical	• Standard ECU	• Standard ECU	• Ruggedized ECU	• Ruggedized ECU
Use-related – Size	• Typical passenger usage profiles (commuting, occasional longer trips)	• Tend toward local movements • Vehicles towing trailers tend toward longer movements	• Tend toward local movements • Vehicles towing trailers tend toward longer movements	• Sleeper cab changes recommissioning options • Tend towards longer runs
Use-related – Maintenance	• Maintenance performed by dealership or owner • Maintenance not necessarily perfectly performed (fleet of one)	• Maintenance performed by dealership or owner • Maintenance not necessarily perfectly performed (fleet of one)	• Typically, smaller fleet sizes than heavy-duty vehicles • More outsourcing of maintenance, possibly lower quality maintenance	• Fleet size affects organizational maintenance practices • More focus on regular preventative maintenance
Use-related – “Second Life” and Recommissioning	• Typically discarded at end of life or continuing of operations with new owner.	• Typically discarded at end of life or continuing of operations with new owner.	• Vehicle may be rebuilt for new purpose (replacement of working element)	• Purchase by operator, usage basically unchanged • Reduced usage (long haul to short haul in second life)

Appendix B. References

IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. [2010, April; version 1 and version 2 parts of the standard range from 1998 to April 2010]

ISO 26262 – Road vehicles – Functional safety. (2011).

Bureau of Economic Analysis. (2015, August). Motor Vehicle Unit Retail Sales.

Advancing Traffic Efficiency and Safety Through Technology. (2010, June). EAST-ADL Overview. PowerPoint presentation at ATeSST workshop, Frankfurt, Germany.

Air Resources Board. (2014, September 2). Truck Sector Overview: Technology Assessment. (PowerPoint presentation). California Environmental Protection Agency. www.arb.ca.gov/msprog/tech/presentation/trucksector.pdf

Cortese, D. (2014). *New model-based paradigm: Developing embedded software to the functional safety standards, as ISO 26262, ISO 25119 and ISO 13849 through an efficient automation of Sw development life-cycle* (SAE Technical Paper No. 2014-01-2394). SAE International.

Dardar, R., Gallina, B., Johnsen, A., Lundqvist, K., & Nyberg, M. (2012, November 27-30). *Industrial experiences of building a safety case in compliance with ISO 26262*. 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, Dallas, TX.

Johansson, D., & Karlsson, P. (2015). *Safety mechanisms for random ECU hardware failures in compliance with ISO 26262* (Master's thesis). Chalmers University of Technology.

Johannessen, P. (2015, November 10-11). *ISO 26262 Trucks - Overview and roll-out in Volvo*. Presentation at safetronic.2015, Stuttgart, Germany.

Kar, S. (2012, February). U.S. Fleet Manager's Desirability and Willingness to Pay for Advanced Heavy-Duty Truck Technology. (PowerPoint presentation: Frost & Sullivan). www.slideshare.net/sandeepkar/2012-us-heavy-duty-truck-fleet-managers-desirability-and-willingness-to-pay-for-advanced-truck-technologies

Malm, A., & Fagerberg, J. (2014, September). *The Global automotive OEM telematics market*. Berg Insight AB.

NACS. (2013, November 19). Alternative Fuel Vehicles to Gain Traction. [Web page news release.] Author [formerly National Association of Convenience Stores]. www.nacsonline.com/Media/Daily/Pages/ND1119131.aspx

Rodriguez-Navas, G., Seceleanu, C., Hansson, H., Nyberg, M., Ljungkrantz, O., & Lönn, H. (2014, June 1-5). *Automated specification and verification of functional safety in heavy-vehicles: The VeriSpec approach*. Proceedings of the 51st Annual Design Automation Conference, San Francisco, CA. doi:10.1145/2593069.2602972

SAE International. (2011, September 11). *The SAE J1939 communications network, An overview of the J1939 family of standards and how they are used* (White Paper). Author.

SafeCer. Project D2.1.4: Standards-oriented, domain specific aspects in reusing software in SafeCer domains, 2013. [SafeCer is the acronym for Safety Certification of Software-Intensive Systems with Reusable Components.] www.safecer.eu/images/pdf/pSafeCer_Deliverable_D4_1_2.pdf

Silva, E. (2015). *Connected vehicle data applied to remote diagnostics methods for heavy duty trucks*. (SAE Technical Paper No. 2015-01-2879). SAE International.

Systemite AB. (n.d.) Systemite AB signs agreement with AB Volvo. http://systemite.se/news-events/0501/systemite-ab-signs-agreement-ab-volvo-systemweaver

U.S. Energy Information Administration. (2015, April). Annual energy outlook 2015 with projections to 2040 (Report No. DOE/EIA-038[2015]) www.eia.gov/forecasts/aeo/pdf/0383(2015).pdf

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault tree handbook* (Report No. NUREG-0492). Nuclear Regulatory Commission.

Westman, J., Nyberg, M., & Torngren, M. (2013). Structuring safety requirements in ISO 26262 using contract theory. *Computer Safety, Reliability, and Security Lecture Notes in Computer Science,* vol. 8153, pp. 166-177.

DOT HS 812 922
June 2020

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

14604-062520-v5