Juraj Pancik - Peter Drgona - Marek Paskala

FUNCTIONAL SAFETY FOR DEVELOPING OF MECHATRONIC SYSTEMS - ELECTRIC PARKING BRAKE CASE STUDY

The electric parking brake (EPB) system as the complex mechatronic system consists of the actuators that generate the clamping force necessary to hold the vehicle safe, the conventional calipers that convert clamp force into brake torque, electronic hardware with the Electronic Control Unit (ECU), cable harness and switches and especially the control software providing the functions that the driver will experience. Like most of the modern automotive components, the EPB is equipped with embedded electronic systems that include ECU, electronic sensors, signals, bus systems, and coding. Due to the complex application in electrical, electronics and programmable electronics, the need to carry out detailed safety analyses that are focused on the potential risk of malfunction is crucial for automotive systems. This paper describes a possible division of the EPB sub-functions between the supplier the wheel brakes and the supplier which supplying the ECU. Functional safety must be a guarantee with concerning the overall vehicle system. Functional safety is according to the requirements of the ISO 26262 standard and in the context of this paper relates solely to the E/E components (electrical and/or electronic) of the EPB. This paper covers the hazard analysis and risk assessment relevant to the EPB control software, and the derived allocation of ASIL risk levels to the EPB software elements of the functional architecture of the EPB.

Keywords: *functional safety management, ISO26262, ASIL, electric parking brake*

1 Electric parking brake (EPB) systems

The automotive market globally demands Electric Parking Brake Systems (EPB) in the goal to improve the overall safety, performance, and comfort of passenger cars on the path to autonomous driving and braking. Therefore, the market share for EPB systems is continuously growing from year to year. Figure 1 shows how the fitment rate of the EPB develops compared to conventional options. The production of the 60 millionth EPB caliper in 2015 was a remarkable milestone and the market share will most likely reach 30% within the next years. Meanwhile, the EPB is available in all major vehicle platforms and produced globally while the share of conventional park brake systems is getting smaller. Even in the segments of small cars and light trucks the demand for EPB systems increases. The forecast shows that the fitment rate could nearly reach half of the market within a decade. While the overall volume demand for EPB Systems is growing additional EPB suppliers entered the market in recent years. This is associated with more diversity regarding system layout and design. Vehicle manufacturers developed individual requirements to specify their needs and system suppliers reacted with individual specifications for test and release.

The efforts required to test and release a safe EPB system significantly contribute to the overall engineering costs. Hence, there is a growing need to establish globally harmonized standards and rules for collaboration between OEM and OES and avoid distortion of competition.

1.1 The EPB functionality

The release process for EPB systems represents its main functionality. Since the EPB was first launched in 2001, several of EPB functions continue to rise significantly. The EPB offers by far more than the basic application and release of a conventional parking brake. It interacts with several other driver assistance systems. Figure 2 gives some examples of typical functions of actual EPB systems.

The EPB offers the driver a comfortable hold and launch on gradients not only on a hill but also in daily car park situations. It can safely hold the vehicle in all situations, for example, when the engine start-stop automatic is active even if the driver leaves the car on a gradient. This is a common situation for delivery service drivers who frequently leave their cars. The EPB satisfies legal requirements regarding the holding ability of a vehicle on inclined surfaces and guarantees safe parking even when all other assistance systems are in sleeping mode and the main power supply is off. If the hydraulic system fails, the EPB allows an emergency stop by applying the EPB switch (following standard ECE-R13H [2-3]).

Juraj Pancik*, Peter Drgona, Marek Paskala
Department of Mechatronics and Electronics, Faculty of Electrical Engineering and Information Technology, University of Zilina, Slovak Republic
*E-mail of corresponding author: juraj.pancik@fel.uniza.sk

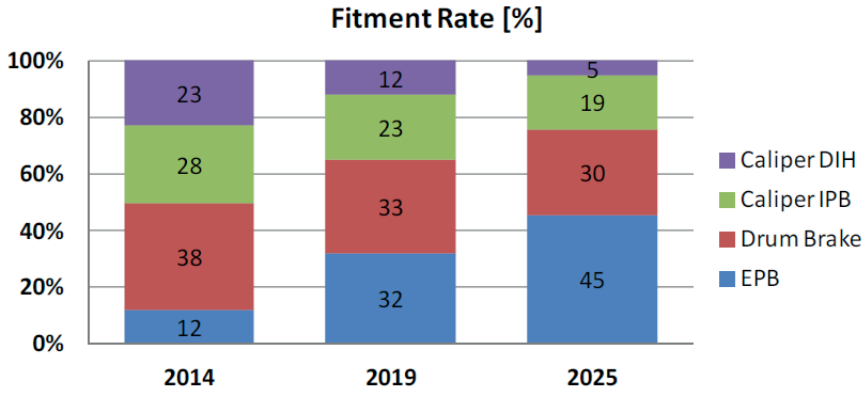

Figure 1 *EPB fitment rate [%], actual and forecasted [1]*

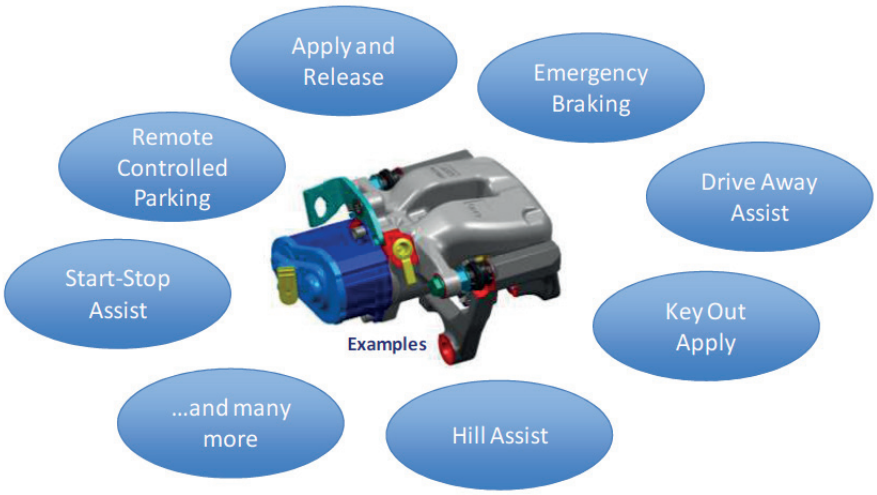

Figure 2 *Functionalities of the Electric Parking Brake*

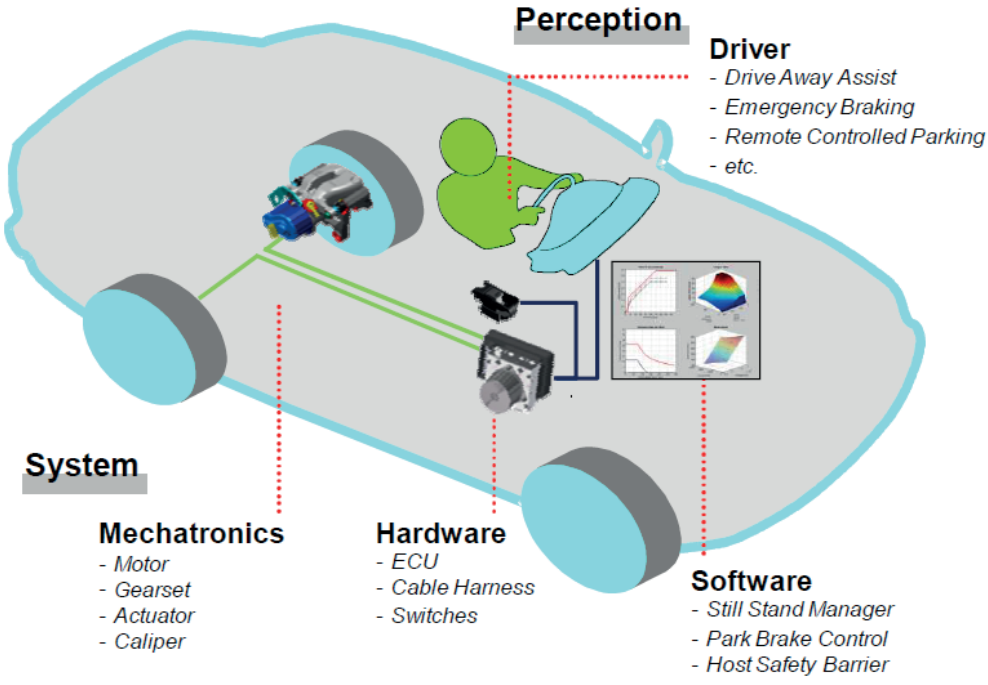

Figure 3 *Electric Parking Brake System (EPB)*

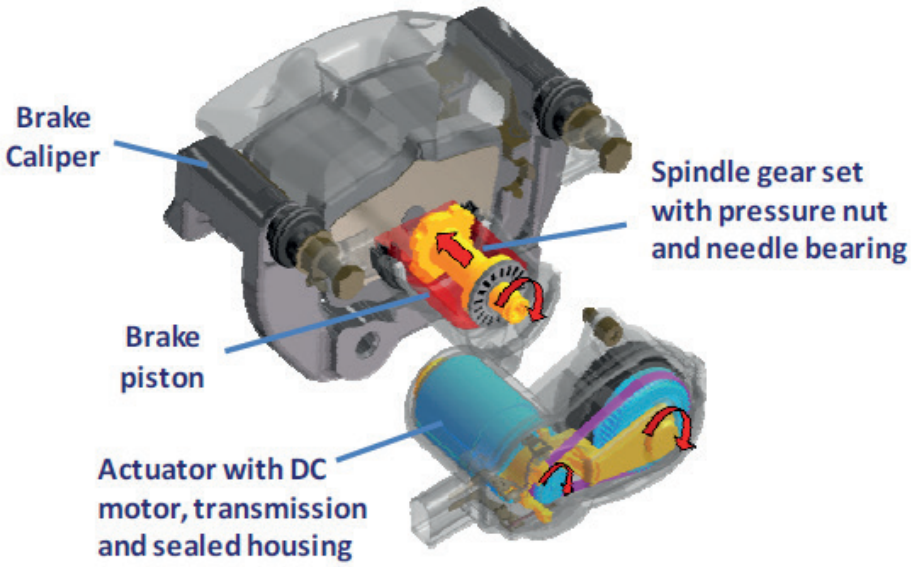

Figure 4 *Mechatronic EPB actuator and caliper assembly [1]*

1.2 The EPB system

Figure 3 gives an overview of the EPB system with the functionality perceived by the driver on the one hand and the components with their technical characteristics on the other hand.

The EPB system consists of the actuators that generate the clamping force necessary to hold the vehicle safely, the conventional calipers that convert clamp force into brake torque, electronic hardware with the Electronic Control Unit (ECU), cable harness and switches and especially the control software providing the functions that the driver will experience.

Figure 4 shows a typical EPB actuator and caliper assembly. The actuator is screwed on the brake caliper. The spindle gear set converts rotational torque coming from the motor, belt drive and planetary gear set into translational clamp force that is applied to the conventional piston. Brake fluid is present in the piston chamber and separated from the sealed actuator. This is just an example as there are also other designs on the market.

1.3 EPB crosswise integration projects

Let introduce the definitions OES and OEM abbreviations. An original equipment manufacturer (OEM) is a company that produces parts and equipment that may be marketed by another manufacturer. The OES (Original Equipment Supplier part) is made by the manufacturer who made the original factory part for the vehicle model. On the other hand, an Original Equipment Manufacturer may not have made that specific part (e.g. EPB) for vehicle originally, but has an official contract history with the automaker [4]. The integrated EPB system can be divided into two parts:

OES-EPB supplier: One part of the EPB system contains the parking brake actuator, the parking brake caliper and the actuation logic (Park Brake Control PBC) which can be represented in our case by PBC software library

OES-ESC supplier: The second part of the EPB system, also called the host, contains the EPB power electronics and necessary peripherals and controls the functions

In addition to the independent EPB control unit, it is possible to integrate the EPB control unit into the ECU with the name Electronic Stability Control (ESC) system. The state of the art is to integrate the EPB control unit into the electronic stability control (ESC) system. On the market, there are OES - specific solutions as well as OES - independent combinations from different ESC and EPB suppliers. The latter case OES - independent is commonly called crosswise integration. In crosswise integration projects, the OES-EPB supplier is responsible for the first part and the OES-ESC supplier is responsible for the second part. The aims of this division are:

- encapsulation of knowledge about particular components
- clearly defined areas of responsibility
- independent testing and approval of components from the different suppliers
- enabling manufacturer-specific levels of functionality of the individual components.

The development and release of such integrated systems need clear requirements for the interfaces and rules for collaboration between the development partners.

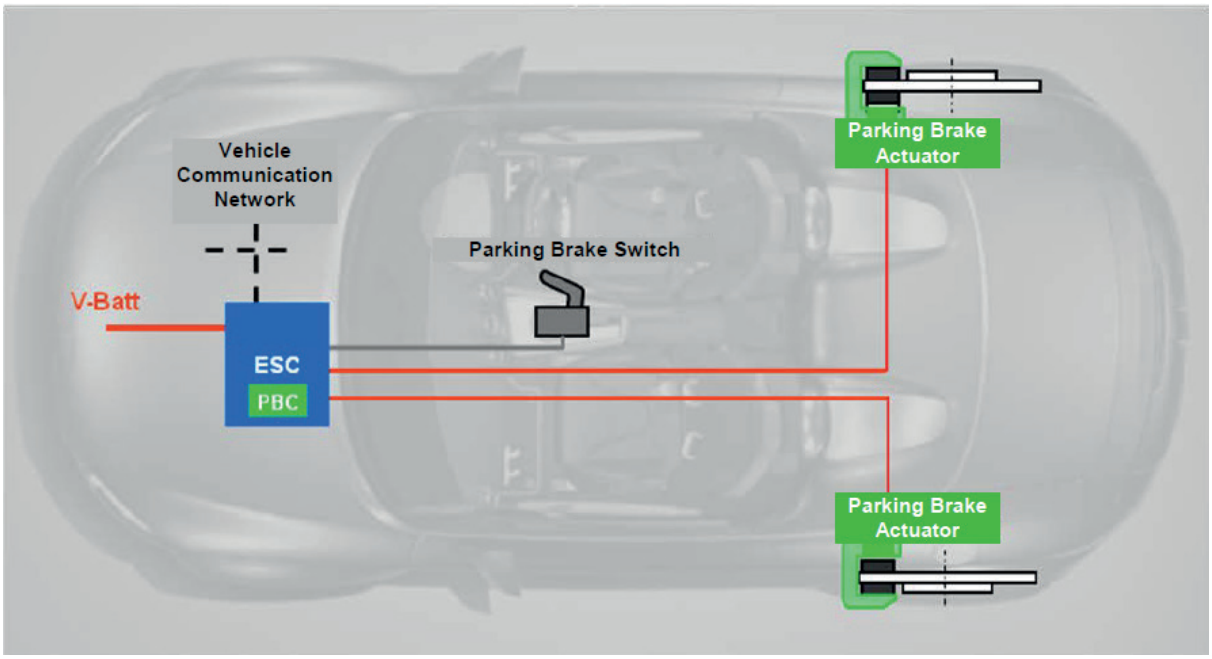

Figure 5 *Schematic diagram of the integrated electric parking brake when it is produced by two suppliers (EPB system green and ESC system as blue) [6]*

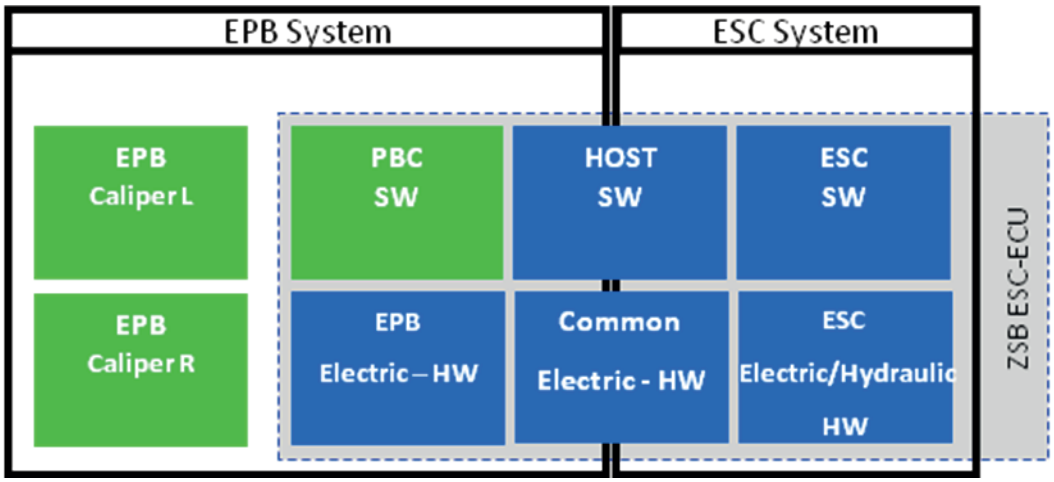

Figure 6 *System network of the integrated electrical parking brake when it consists of two suppliers (EPB system green and ESC system as blue) [6]*

1.4 EPB integration into host ECU according to the VDA recommendation 305-100

Within the VDA [5] working groups were formed who elaborate relevant recommendations to harmonize requirements and procedures between the development partners for braking systems in case of EPB crosswise integration projects. VDA recommendation 305-100 [6] defines the integration of the EPB control unit into an ESC type control unit from different manufacturers. For such a crosswise integration the work products of functional safety of each part need to be distributed on both OES to realize a systematic verification and validation. The content of this recommendation has been selected such that the constraints permit combining EPB and ESC but without restricting further product - specific development by these different OES.

The VDA Recommendation 305-100 describes and defines the integration of the control of caliper-integrated parking brake actuators into an ESC control unit from a different manufacturer. The Brake Assembly supplier (brake or OES-EPB supplier) is responsible for the parking brake actuator, the parking brake caliper and the actuation logic (parking brake controller, PBC) (see Figure 5; green). The ESC supplier (host or OES-ESC supplier) is responsible for the EPB power electronics and necessary peripherals and the functions that the driver can experience (see Figure 5; blue).

The PBC is a software component designed specifically for the parking brake actuator and is integrated into the host. The integration of the EPB as described in this VDA recommendation 305-100 is distinguished by the use of a single ESC control unit. The logical representation of the

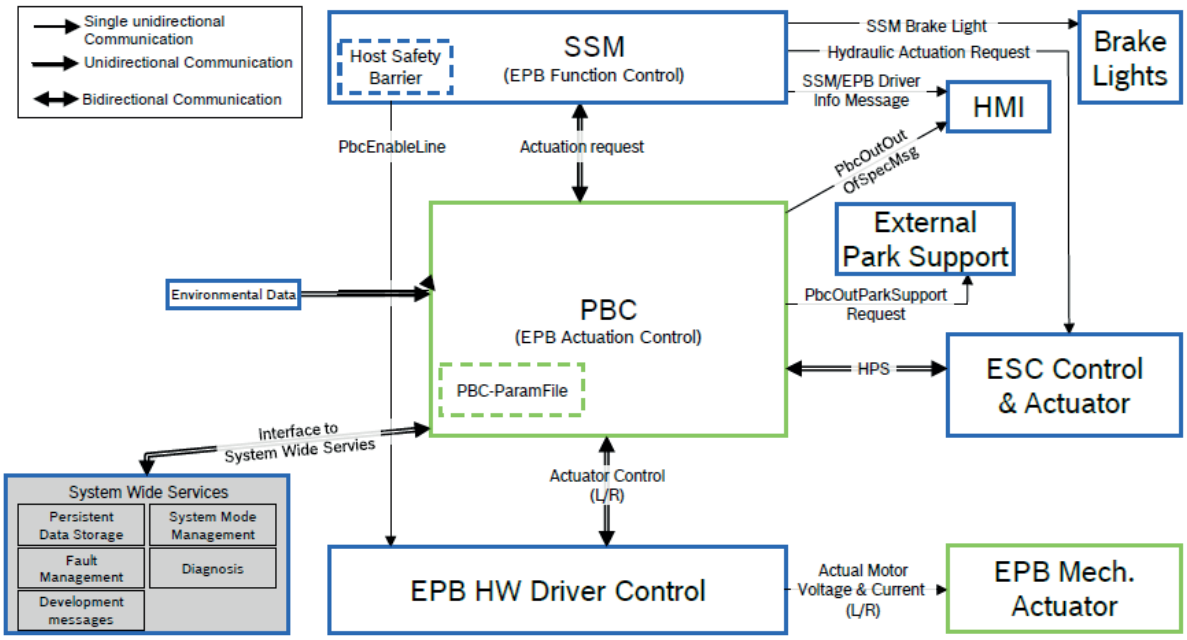

Figure 7 *Overview of the functional architecture of the integrated EPB system including interfaces [6]*

Table 1 *List of the functional architecture blocks of the integrated EPB*

Function block	Task
PBC	Proper control of the EPB Mech. Actuator for safe parking of the vehicle and releasing of the parking brake, arbitration between actuation requests from diagnosis and SSM, control of the dynamic deceleration actuation via the parking brake actuators. The PBC parameter file (PBC-ParamFile) contains specific parameters of the PBC.
EPB HW Driver Control	Activation unit for the parking brake actuators (acc. requested direction) and providing electric measurements to the PBC.
EPB Mech. Actuator	Providing and archiving the electromechanical clamping force; reducing the electromechanical clamping force.
System Wide Services	Providing services for data storage, diagnosis and monitoring of the system modes; fault management; communication of development messages.
HOST Safety Barrier	Safety mechanism to enable the EPB hardware drivers to avoid PBC safety-critical activations of the parking brake actuators.
HMI	Control logic and actuation of driver information (e.g. warning lamps, status lamps and text messages).
Brake Lights	Control logic and request for brake lights
ESC Control & Actuator	Control logic and hardware of the hydraulic actuator.
Environmental Data	Collecting, preparing and providing environmental data to the PBC.
External Park Support	Control logic for requesting external parking support (depending on available parking support actuators).

components used and their allocation to the EPB and ESC systems are shown in Figure 6.

1.5 Functional architecture of EPB

The functional architecture of EPB with the marked system boundaries is shown in Figure 7

Figure . Green boundaries specify the subject of interest in this work. Table 1 describes functional architecture blocks of the integrated EPB and Table 2 describes interfaces between the function blocks.

2 Functional safety for PBC - EPB software part of the electric parking brake

Functional safety management (FSM) in general represents planning, coordinating, and documenting activities related to functional safety. The FSM implements of the management plan for all phases of the safety lifecycle, including:

- Overall safety management
- Project dependent safety management
- Safety management for production, operation, service and decommissioning

Table 2 *List of interfaces between the function blocks [6]*

Interface	Task
SSM ←→ "Actuation Request"	SSM →PBC: actuation request PBC →SSM: status information from the Brake Assy
PBC ←→EPB HW Driver Control "Actuator Control L/R"	PBC →EPB HW Driver Control: actuation command from the PBC. EPB hardware driver control →PBC: status information, current and voltage of the hardware driver for the parking brake actuators.
EPB HW Driver Control →EPB Mech. Actuator "Actuator Voltage & Current" Supply"	EPB HW Driver Control →EPB Mech. Actuator: activation of the parking brake actuators in the direction requested, separate for L/R, by supplying current and voltage.
PBC ←→System Wide Service "Interface to System Wide Services"	PBC →System Wide Service: providing internal PBC data for the ECU Diagnostic Interface, fault manager (FM) interface, providing data to be stored System Wide Service →PBC: providing stored data, transferring diagnostic requests, FM interface
PBC →HMI "PbcOutOutOfSpecMsg"	Display indication of Brake Assy operation outside the specification range.
PBC ←→ ESC Control & Actuator "HPS"	PBC →ESC Control & Actuator: hydraulic support request from the PBC to ensure Park brake hold capability. ESC Control & Actuator →PBC: status information
Environmental Status Information →PBC	Providing environmental data to the PBC
SSM →HMI "SSM/EPB Driver Info Message"	Request driver information relevant to EPB (e.g. EPB status information, EPB fault information, function-based text messages)
SSM →Brake Lights "SSM Brake Light"	Request brake lights during an emergency brake request via the parking brake control unit
SSM →ESC Control & Actuator "Hydraulic Actuation Request"	Requests for holding (e.g. Auto Hold) and hydraulic dynamic deceleration via the hydraulic actuator.
HOST Safety Barrier →EPB HW Driver Control "PbcEnableLine"	Enabling the "EPB HW Driver Control" for each direction separately (apply/release), for driving the parking brake actuators.
PBC →External Park Support "PbcOutParkSupportRequest"	Requests for external parking supp

2.1 Standard ISO 26262 - functional safety for road vehicles

The only widely/internationally recognized standard for functional safety management (FSM) in the automotive industry is the ISO 26262 [7]. This standard must be followed for all development, production and service activities of safety - related electrical and electronic components and systems (E/E-components/-systems) in the automotive industry. Though currently there does not seem to be any direct legal requirement it is nevertheless mandatory to develop E/E - systems according to the ISO 26262 standard because this is considered to be "state-of-the-art" in product development at present and this legal standard is a requirement of legislation in general. Additionally, increasingly many customers in automotive explicitly demand ISO 26262-compliant development and corresponding contracts and agreements are undoubtedly legally binding.

2.1.1 Automotive Safety Integrity Level (ASIL)

The standard ISO 26262 defines functional safety as "the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical or electronic systems." ASILs establish safety requirements - based on the probability and acceptability of harm - for automotive components to be compliant with ISO 26262. There are four ASILs identified by ISO 26262 - A, B, C, and D. ASIL A represents the lowest degree and ASIL D represents the highest degree of automotive hazard. Systems like airbags, anti-lock brakes, and power steering require an ASIL - D grade-the highest rigor applied to safety assurance-because the risks associated with their failure are the highest. On the other end of the safety spectrum, components like rear lights require only an ASIL - A grade. Headlights and brake lights generally would be ASIL - B while cruise control would generally be ASIL - C. ASILs are established by performing hazard analysis and risk assessment. For each electronic component in a vehicle, engineers measure three specific variables:

- Severity (the type of injuries to the driver and passengers)
- Exposure (how often the vehicle is exposed to the hazard)
- Controllability (how much the driver can do to prevent the injury)

Each of these variables is broken down into sub-classes. Severity has four classes ranging from "no injuries"

Table 3 *Safety goals of the EPB system according to VDA recommendation 305-100 Chapter 4*

Case (operational situations and operating modes)	Hazard	Risk assessments
Too high or unintended braking torque while the vehicle is in motion (max. ASIL D)	1a) Incorrect actuation of EPB in the locking direction when v > vcrit.	ASIL D
	1b) Execution of the function 'Dynamic deceleration' intended by the driver leads to vehicle instability when v > vcrit.	ASIL B
	1c) Execution of the function 'Dynamic deceleration via the parking brake actuators intended by the driver' leads to vehicle instability when v > vcrit.	ASIL A
	1d) Incomplete release of the EPB with residual braking torque.	ASIL B
Unintended braking torque while the vehicle is stationary (max. QM)	2a) EPB cannot be released.	QM
Too low braking torque while the vehicle is stationary (max. ASIL C)	3a) Incorrect EPB actuation in the releasing direction (driver absent, vehicle parked, ignition off).	ASIL C
	3b) Too low build-up of EPB holding force (driver absent, road slope ≤ 8%).	ASIL B
	3c) Incorrect release of the EPB (driver absent, vehicle held, ignition on).	ASIL B
	3d) Required EPB function 'proactive re-clamping' is either not executed, or is executed insufficiently (driver absent, vehicle parked).	ASIL A
	3e) Required EPB function 'hydraulic support' is either not executed, or is executed insufficiently (driver absent, vehicle held).	ASIL A
	3b) Too low build-up of EPB holding force (driver absent, road slope > 8%).	ASIL A
Incorrect driver information (max. ASIL A)	4a) EPB specific driver information on the EPB function status incorrectly signals EPB status 'locked' (EPB opened).	ASIL A

(S0) to "life-threatening/fatal injuries" (S3). Exposure has five classes covering the "incredibly unlikely" (E0) to the "highly probable" (E4). Controllability has four classes ranging from "controllable in general" (C0) to "uncontrollable" (C3). All variables and sub-classifications are analyzed and combined to determine the required ASIL. For example, a combination of the highest hazards (S3 + E4 + C3) would result in an ASIL D classification. Given the guesswork involved in determining ASILS, the Society of Automotive Engineers (SAE) drafted J2980, "Considerations for ISO 26262 ASIL Hazard Classification" in 2015 [8]. These guidelines provide more explicit guidance for assessing Exposure, Severity, and Controllability for a given hazard.

2.1.2 Benefits of ASILs

ISO 26262 is a goal-based standard that's all about "preventing harm." Despite their challenges, ASIL classifications are intended to "prevent harm" and help us achieve the highest safety rating possible for myriad automotive components across a long and often disjointed supply chain. Key benefits of ASIL include:

- Establishing safety requirements to mitigate risks to acceptable levels
- Managing and tracking safety requirements
- Ensuring that standardized safety procedures have been followed in the final product

2.2 Functional safety solution for PBC software

2.2.1 Management of functional safety of PBC software

A central functional safety department inside of an organization manages the functional safety process area in the EPB system development. The safety - lifecycle requirements for automotive products are defined in the specific FSM guidelines, which assign the safety activities required by ISO 26262. The functional safety management within the project is carried out by a project-specific team, which is supported by the central functional safety department of developing an organization. The team must prepare prescribed documents (work products) that are related to developing. The PBC software development process has to follow the requirements of the Automotive SPICE Process Reference Model Process Assessment Model Version 3.1 [9] and should be tailored in the system development manual prepared by the organization. Implementation ASPICE in the software development of

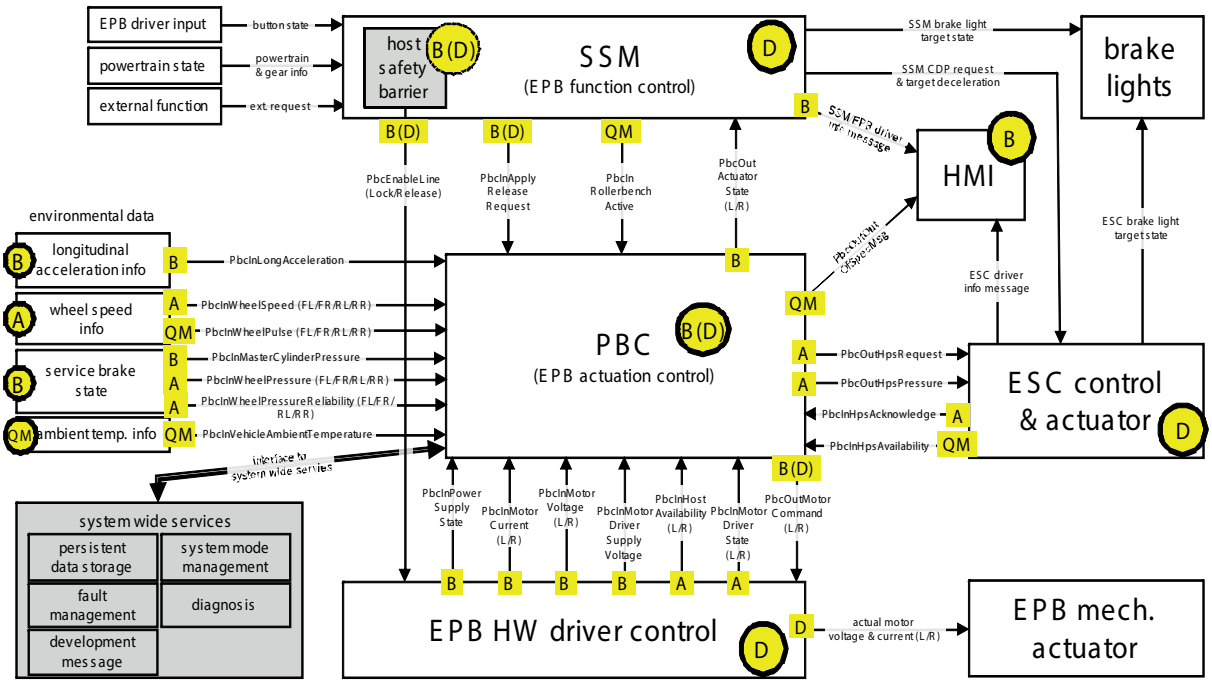

Figure 8 *Overview of EPB functional architecture with relevant ASIL levels (maximum overall hazards, hazard 1a) according to ASIL B(D) and ASIL B(D) decomposed) signals*

Table 4 *ISO 26262 recommended rules that govern ASIL decomposition [11-12]*

ASIL before decomposition	ASIL after decomposition
ASIL D	ASIL D(D) + ASIL quality management (QM) (D)
	or
	ASIL C(D) + ASIL A(D)
	or
	ASIL B(D) + ASIL B(D)
ASIL C	ASIL C(C) + ASIL QM(C)
	or
	ASIL B(C) + ASIL A(C)
ASIL B	ASIL B(B) + ASIL QM(B)
	or
	ASIL A(B) + ASIL A(B)
ASIL A	ASIL A(A) + ASIL QM(A)

automotive parts with embedded software is recommended by standard IATF 16949:2016 [10].

2.2.2 Hazard Analysis and Risk Assessment (HARA) for the parking brake assembly

Even if the brake assembly is only a part of the parking brake system, a hazard analysis as specified work product has been carried out by the team for the overall parking brake system on vehicle level. All possible hazards have been analyzed by taking account of the operational situations and operating modes according to ISO 26262-3. The resulting hazardous events have been classified and the corresponding safety goals have been defined. Table 3 shows the safety goals for the electric parking brake with the resulting ASIL classification according to VDA recommendation 305-100, Chapter 4 [6] and standard J2980 [8].

2.2.3 Functional safety concept

Based on the safety goals, the functional safety concept has been specified by deriving the functional safety requirements in the document PBC SRS2 Safety and allocating them to the item architecture elements in the PBC system architecture. The specification of the functional safety requirements considers the parking brake realization concept, which unifies the host part and the brake assembly part. The functional safety requirements allocation in the SRS2 Safety document and the ASIL allocation to the host

part and the assembly brake part comply with the contents of chapter 4 of the VDA recommendation 305-100.

2.2.4 Technical safety concept

The technical safety concept work product has been derived from the functional safety concept, considering the interchangeability concept described in the VDA recommendation 305-100. In this document, ASIL decompositions at the interface between the host and the brake assembly are determined for the fulfillment of the safety goals and the technical safety requirements concerning the interfaces between the host and the brake assembly are specified and addressed to the responsible part(s). Furthermore, the interface signals between the host and the brake assembly are defined and specified in the VDA recommendation 305-100. The corresponding ASIL classifications are also assigned to the interface signals where are described in the EPB functional architecture (Figure 8). The maximum overall hazard is hazard 1a with ASIL D (Table 3). In other words, the parking EPB brake assembly is an item with ASIL D risk.

2.2.5 PBC software safety requirements

Software safety requirements are derived from the technical safety concept and the system architectural design specification (inherit the ASIL). The EPB safety requirements implemented in the PBC software module must not be greater than ASIL B. To ensure this, the method of ASIL decomposition is applied for all hazards classified as ASIL C or ASIL D. The confirmation measures for park brake assembly system were estimated in the HARA work product (chapter 3.2.2) with ASIL D and used accordingly (ISO 26262-2, chapter 6.4.7). The used process for decomposition can be found in ISO 26262-9, chapter 4. In general, an ASIL D functional safety requirement can be decomposed into ASIL B (in support of D) + ASIL B (in support of D) - see Table 4. The PBC software is part of the ASIL decomposition with the Host safety barrier (ASIL D => ASIL B (D) + ASIL B (D)) and fulfills, therefore, ASIL B (D).

3 Conclusion

The electric parking brake (EPB) system is a complex mechatronic system. In our work possible hazards for the EPB system have been analyzed with taking account of the operational situations and operating modes according to ISO 26262. We presented an overview of the EPB functional architecture with relevant ASIL levels (maximum overall hazards for EPB system is ASIL D). Software safety requirements for the PBC software module are following the ASIL B(D). The PBC software safety requirements can be applied to software development, integration, testing and used tools for EPB software development and they were not a subject of our research.

References

[1] REITZ, A., LOEHR. B., KOHRT, J.-P. Harmonisation of the release process for electric parking brake systems. In: Euro Brake 2016 : proceedings. 2016.

[2] ISHIHARA, K. Introduction of R13H: brake regulations for passenger vehicles. In: 3rd Asia Expert Meeting on Braking Systems for Passenger Vehicles : proceedings. 2005.

[3] ECE Regulation No. 13-H. Uniform provisions concerning the approval of passenger [online] [accessed 2019-09-18]. Available from: http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/R13hr2e.pdf

[4] FYNES, C. What's the difference among OES, OEM, and Aftermarket Car Parts? - Your Mechanic [online] [accessed 2019-09-18]. Available from: https://www.yourmechanic.com/article/-what-s-the-difference-among-oes-oem-and-aftermarket-car-parts-by-conor-fynes

[5] Verband der Automobilindustrie / Association of the Automotive Industry [online] [accessed 2019-09-18]. Available from: https://www.vda.de/en

[6] VDA 305-100 Recommendation for integration of electric parking brakes control into ESC control units - Verband der Automobilindustrie / Association of the Automotive Industry [online] [accessed 2019-09-18]. Available from: https://www.vda.de/en/services/Publications/integration-actuators-of-electric-parking-brakes-esc.html

[7] KAFKA, P. The automotive standard ISO 26262, the innovative driver for enhanced safety assessment and technology for motor cars. *Procedia Engineering* [online]. 2012, **45**, p. 2-10. ISSN 1877-7058. Available from: https://doi.org/10.1016/j.proeng.2012.08.112

[8] SAE International. Examples and GUIDANCE for brake and park brake functions HARA. In: J2980 considerations for ISO 26262 ASIL hazard classifications. 2015.

[9] Automotive SPICE process reference model process assessment model version 3.1 - VDA QMC Working Group 13 / Automotive SIG [online] [accessed 2019-09-18]. Available from: http://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICE_PAM_31.pdf

[10] IATF 16949:2016 Quality management system - AIAG [online] Available from: https://www.aiag.org/quality/iatf16949

[11] WARD, D. D., CROZIER, S. E., The uses and abuses of ASIL decomposition in ISO 26262 In: 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012 : proceedings [online] [accessed 2019-09-23]. 2012. ISBN 978-1-84919-678-9. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6464473
[12] ISO 26262, Part 9: Automotive Safety Integrity Level (ASIL) - oriented and safety - oriented analysis. 2018.