Functional Safety Case with FTA and FMEDA Consistency Approach

Richard Messnarz(✉) and Harald Sporer

ISCN GesmbH, Graz, Austria
rmess@iscn.com

Abstract. Based on the hazard and risk analysis of ISO 26262 possible malfunctions are analysed for different situations and rated by Severity, Exposure, and Controllability which leads to a QM, or ASIL A-D ranking. For each ASIL A-D case a safety goals is formatted. And for each safety goal with a rating of ASIL C or ASIL D an FTA (Fault Tree Analysis) and FMEDA (Failure Modes Effects and Diagnostics Analysis) are methods which are highly recommended. Both methods calculate an overall FIT (Failure in Time) and both consider a diagnostic coverage. In this paper an approach is described of how to assure in FTA (top down analysis) and FMEDA the same overall FIT calculated (bottom up analysis). The paper creates a use case scenario for the example "Function 2" in ISO 26262:2011 part 5 Annex E. The example used in the ISO 26262:2011 part 5 Annex E. [1] does not contain background information on system level. This paper adds the missing background information and shows how the system safety concept decisions are mapped onto hardware architecture decisions.

Keywords: Automotive SPICE 3.1 · Functional safety · ISO 26262
FTA · FMEDA · Use case of an ABS brake system

1 Scenario Background - The H&R and Safety Goals

Figure 1 illustrates the item definition of the ABS brake system [1, 2, 6, 13].

A typical item drawing shows the input layer, the calculation layer, and the actuation and output layer. Also the interfaces to the vehicle are included. Additionally the functional concept of the item is considered.

Functional Concept:
Name: Anti-lock braking system (ABS)

Allows the driver to maintain steering control in situations like heavy braking or on slippery surfaces by preventing significant wheel slip. The system constantly monitors the rotational speed of each wheel. When it detects a wheel rotating significantly slower than the others (a condition indicative of impending wheel lock) it actuates the valves within the brake hydraulics to reduce hydraulic pressure to the brake at the affected wheel, thus reducing the braking force on that wheel. The wheel then turns faster; when the wheel is turning significantly faster than the others, brake hydraulic pressure is increased so the braking force is reapplied and the wheel slows. This process is repeated continuously, and can be detected by the driver via brake pedal pulsation.

X. Larrucea et al. (Eds.): EuroSPI 2018, CCIS 896, pp. 387–397, 2018.
https://doi.org/10.1007/978-3-319-97925-0_32

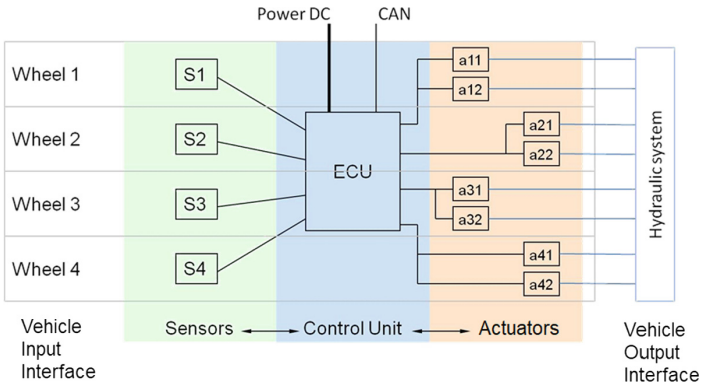

Fig. 1. Item definition ABS brake system - electrohydraulic

In the Hazard and Risk Analysis malfunctions are rated for different driving situations using categories, such as severity, exposure and controllability. Tables from the norm help to identify the proper ratings.

Severity is S3 when a rear, front or side crash is possible a medium speed (which includes the high speed as well), on a scale of S1–S3.

Exposure E4 is given when the system that can cause the hazardous malfunction is active at every drive, or is used at more than 10% of the operating hours in the car. Therefore braking is listed as E4, on a scale of E1–E4.

And a car is seen as being uncontrollable if steering or braking does not work. So also here the ABS brake would be rated usually at C3 (on a scale of C1 – C3). In case of the highest ratings S3, E4, C3 the risk graph of the norm delivers the highest ASIL (Automotive Safety Integrity Level) ASIL – D (on a scale of A-D).

Figure 2 shows a typical line of the H&R (Hazard and Risk Analysis) with ratings for severity, exposure and controllability, the derived ASIL level and a safety goal. In fact the safety goal with the ASIL rating is then the input to the system safety concept design [1–12, 17, 18].

	B) Hazard identification (EXAMPLE)		A) Situation (EXAMPLE)	C) Classification (EXAMPLE)			D) Determination of ASIL and safety goals (EXAMPLE)	
Fkt	**Failure**	**Conseq.**		**S**	**E**	**C**	**ASIL**	**Safety Goal**
ABS	p_min	No braking force at the wheels	…	S3 …	E4 …	C3 …	ASIL D	The ABS-system must not limit the reliability of the braking system. Reducing the braking pressure more and/or longer than necessary must be avoided.
	p_max	wheels can block (destabi-lizing possible)	…					
	p<	Inadequate braking -> stopping distance too long / longer than expected by driver	…					

Fig. 2. Hazard and risk analysis – ASIL rating – safety goals

2 Scenario Background - the System Safety Concept and Design Decisions

The brake pedal is pressed and the brake pedal input is input to an ECU (Electronic Control Unit). The ECU has a connection to an electric motor of a pump that then produces the corresponding pressure in the hydraulic system to create a brake force at the wheel. A traditional hydraulic brake with no electronic would produce only some 40–50% of the pressure (measured in Pounds per square inch) than electronic supported brakes can do (up to ca. 2000 PSI).

The ABS (Anti-Lock Braking System) includes valves in the hydraulic system that allow to decrease the pressure on single wheel. An inlet valve can close and a further outlet valve can decrease the pressure by releasing the hydraulic fluid and redirect it back to the hydraulic tank.

Figure 3 shows the system concept of an electro-hydraulic brake system. The brake pedal signal is used as an input to calculate a demanded brake force which is converted to a demanded pressure in PSI. The brake ECU then actuates an electric pump (electric motor of the pump) to create the demanded PSI pressure in the 2 hydraulic channel systems (braking at front wheel, braking at rear wheels). Two separated brake channels are needed so that in case of failure at least either the front wheel or the rear wheel will brake. For the control cycle in the ECU PTS (Pressure and Temperature Sensors) are needed to measure the achieved pressure. Temperature is needed as well because the fluid changes the viscosity depending on the temperate. The system also is based on characteristic curves where brake pressure is translated to brake force at the wheels in the calculation models of the software.

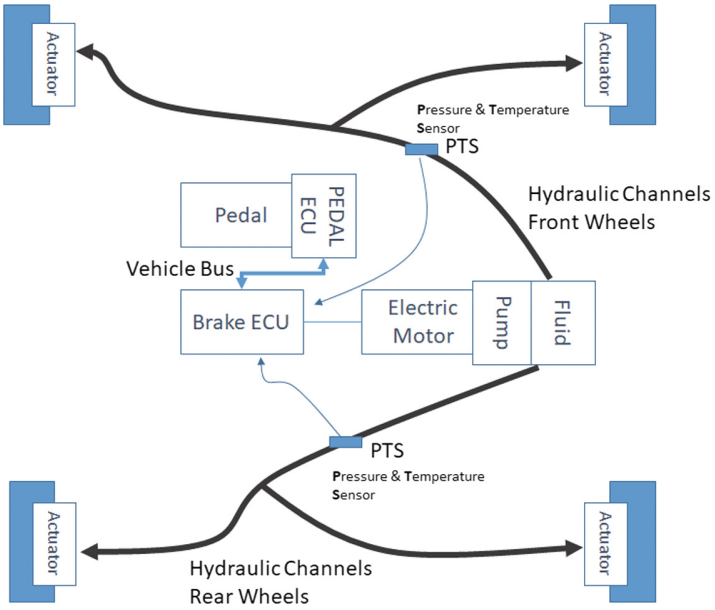

Fig. 3. System concept electro – hydraulic brake system

Figure 4 shows the integration of the ABS brake system concept where by closing an inlet valve the brake pressure built up can be stopped and additionally by using an outlet valve the pressure can be reduced by redirecting the hydraulic fluid back to the brake fluid cycle/container. Figure 4 only shows the concept for one wheel, the same is operating on all 4 wheels. The ABS pump includes 4 separate hydraulic channels and the valves per channel.

Safety Concept and Decomposition Assumptions

The hazard and risk analysis led to an ASIL – D rating. This ASIL – D is then inherited for the functional signal flow that has to assure functional safety of the system [5, 7, 8]. The hazardous fault (malfunction) is that the inlet valve incorrectly closes and the outlet valve incorrectly opens. In this case no brake pressure could be built up on a wheel. Moreover, if one wheel for a longer time has no brake force while the other wheels are braking the car will steer in an uncontrollable way.

The safety critical path is that incorrect position of the valves will be recognised by the ABS ECU with ASIL D. Therefore the control valves, the read back of valves, the ECU inherit an ASIL D rating.

Fail Safe Concept

The ABS system has to be developed in a fail safe mode where if no electric power is supplied any more by the ABS (ABS is deactivated) the inlet valve is fail safe open and the outlet valve is fail safe closed. This means that a deactivation of the ABS system leads to a normal electro-hydraulic brake like in Fig. 3.

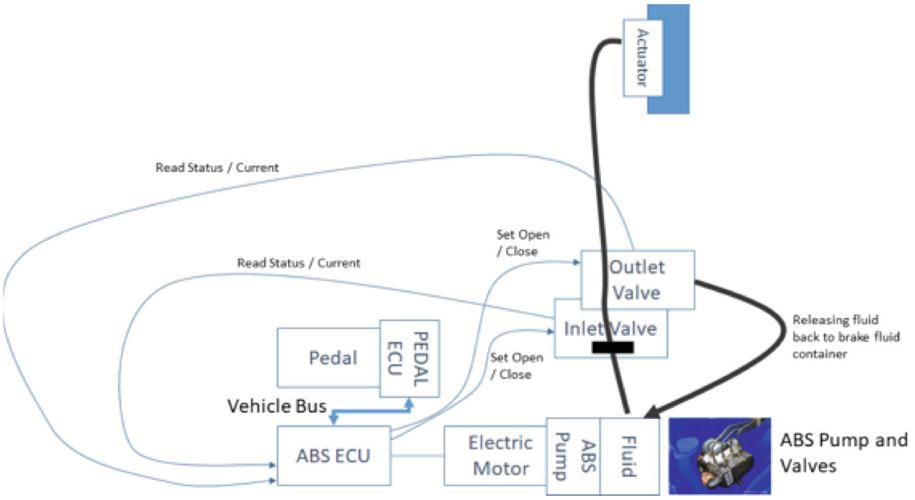

Fig. 4. System concept ABS brake system

Diagnostic Coverage

The actuation of the valves must be read back by an ADC. To reach a higher diagnostic coverage of 99% (as it is used in the example for FMEDA and FTA below) the underlying electro-hydraulic brake system can provide pressure and temperature sensor

values, plus a mathematical model demanded brake force versus achieved PSI value in the hydraulic system. This means that if the inlet valve incorrectly closes and the output valve incorrectly opens the PTS sensors (see Fig. 1) would see a sudden decrease in the pressure for a period longer than a threshold ms time.

Additionally the mathematical model of expected brake force (deceleration of wheel speed) can be compared with the real deceleration as a second independent path. Both parallel independent diagnose functions allow a plausibility check and a 99% diagnostic coverage assumption.

Decomposition Assumptions

In the functional safety norm a high ASIL rated system can be decomposed into 2 parallel independent ASIL B channels. An ASIL B could further be decomposed into two ASIL A. The brake pedal position must be provided at ASIL D. Usually this is provided over CAN by two independent brake pedal position signals, both being rated ASIL B.

The ABS ECU contains 2 cores, one controls the valves and one is measuring the PTS sensors. Both can compare (expected pressure by PTS versus valves position) and both can deactivate the ABS function. This usage of a mathematical model for plausibility check would allow a decomposition of the µCs but in the example below we just assume to reach ASIL D with no decomposition of the cores.

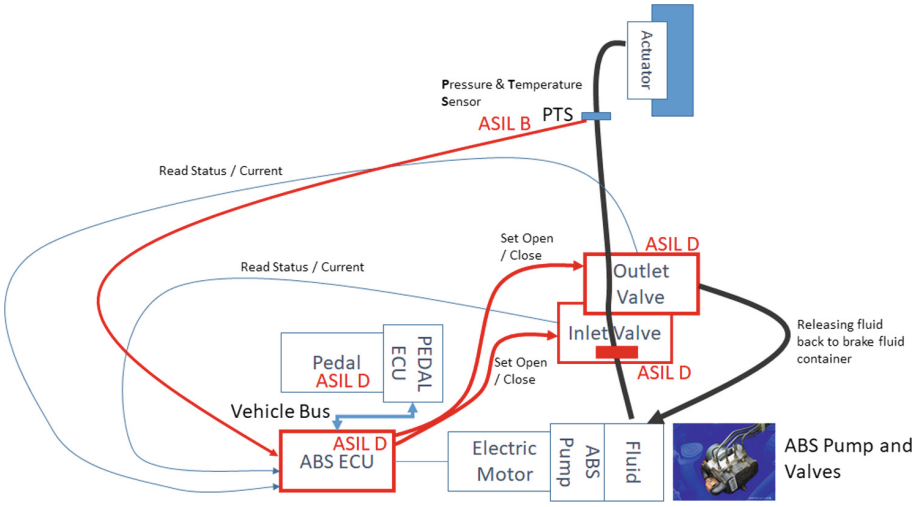

Fig. 5. System concept ABS brake system with an ASIL assignment

3 Application of Consistent FTA and FMEDA

Figure 5 shows the ASIL D rated parts of the system which are impacted by the safety goal described in Fig. 2 above. Each ASIL rating of a safety goal defines a hardware architecture metric for single point faults to be achieved. ASIL D relates to 10^{-8} which means 1 hazardous fault not detected and avoided in 10^{8} operating hours in the fleet.

Figure 6 below shows the example schematic used in ISO 26262:2011 part 5 [1] to explain hardware architecture metrics calculation. In the chapters before we added the ABS background system concept considerations which were not published in the norm but are required to fully understand the use case.

In Sect. 1 the hazard analysis and risk assessment (HARA) is shown. The safety goal "The ABS-system must not limit the reliability of the braking system. Reducing the braking pressure more and/or longer than necessary must be avoided." was classified with ASIL D. According to the hardware design safety analysis methods defined in [1] a deductive and an inductive analysis is highly recommended. Within automotive industry projects this is usually carried through by the application of a fault tree analysis (FTA) and a failure modes, effects and diagnostic analysis (FMEDA).

To showcase the correlation between the inductive design analysis FMEDA and the deductive design analysis FTA one channel out of a four channel ABS has been extracted. The main parts (see Fig. 6) considered in the following ABS use case are

- inductive sensor I1, measuring the front left wheel speed
- coils of inlet valve I61 and outlet valve I71, integrated into the hydraulic circuit of the front left wheel brake
- ABS warning lamp L1
- microcontroller µC
  - reading wheel speed via In1
  - controlling inlet and outlet valves via Out 1 and Out 2
  - reading valve's status via InADC1 respectively InADC2
  - switching on/off ABS warning lamp via Out 3
- watchdog WD, introduced as system monitoring device for the microcontroller

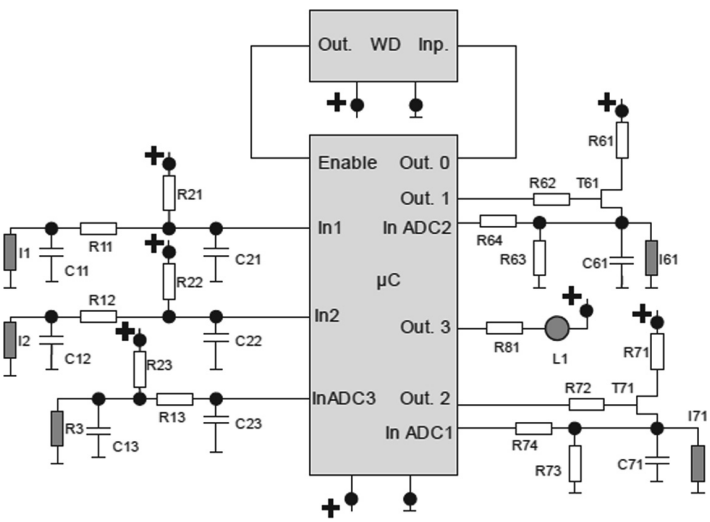

Figure E.1 — Example diagram

Fig. 6. Example HW schematic ABS brake system valve control [1]

As mentioned above the described use case is based on "Function 2" from ISO26262 Annex E [1]. To meet the requirements for the selected vehicle function ABS the description can be restated as following.

The function has one input (wheel speed measured via sensor I1 generating pulses) and two outputs (inlet valve controlled by I61 and outlet valve controlled by I71) and its behaviour is to decrease hydraulic pressure at the brake calliper in case of a potential brake lock/wheel lock.

Low pressure has been identified as a possible hazard during the (HARA) that can lead to a missing break force at the wheels. Due to a failure within the hard- or software the inlet and outlet valves could be controlled in a way that arouses the described hazard. More details about the hazard analysis and risk assessment can be found in Sects. 1 and 2 above.

From an electro-mechanical point of view the inlet and outlet valves are designed to enable a fall back scenario in case of an ABS failure. That is, when no current is supplied at the coils, the inlet valve remains open and the outlet valve remains closed.

Figure 8 shows the typical FMEDA done for single point fault metrics for the hardware parts effected. Each part has FIT (failure in time measured in faults per 10^9 operating hours in the fleet), failure modes which can be a hazard (with percentage of occurrence), and a diagnostic coverage. The single point fault FIT is calculated with the formula:

$$Fit\ of\ part\ *\ Percent\ Occurrence\ of\ hazardous\ failure\ mode * (1 - Diagnostic\ Coverage).$$

The calculation in line for T61 short cut in Fig. 8 is therefore $5 \times 0{,}5 \times (1-0{,}9) = 0{,}25$. The 5,86 is the sum of the single point FIT of the affected parts.

Component Name	**Failure rate/FIT [10^{-9}]**	**Safety-related component** to be considered in the calculations?	**Failure Mode**	Failure rate distribution	Failure mode that has the potential to **violate the safety goal** in absence of safety mechanisms?	**Safety mechanism(s)** allowing to prevent the failure mode from violating the safety goal?	**Failure mode coverage** wrt. violation of safety goal	**Residual or Single-Point Fault failure rate/FIT**
T61	5	YES	open	50%				
			short	50%	x	SM3	90%	0,25
T71	5	YES	open	50%				
			short	50%	x	SM5	90%	0,25
R62	2	YES	open	90%	x	SM3	90%	0,18
			closed	10%				
R72	2	YES	open	90%	x	SM5	90%	0,18
			closed	10%				
uC	100	YES	All	50%	x	SM4	90%	5
			All	50%				
								5,86 FIT

Fig. 7. Example extract from the HW FMEDA

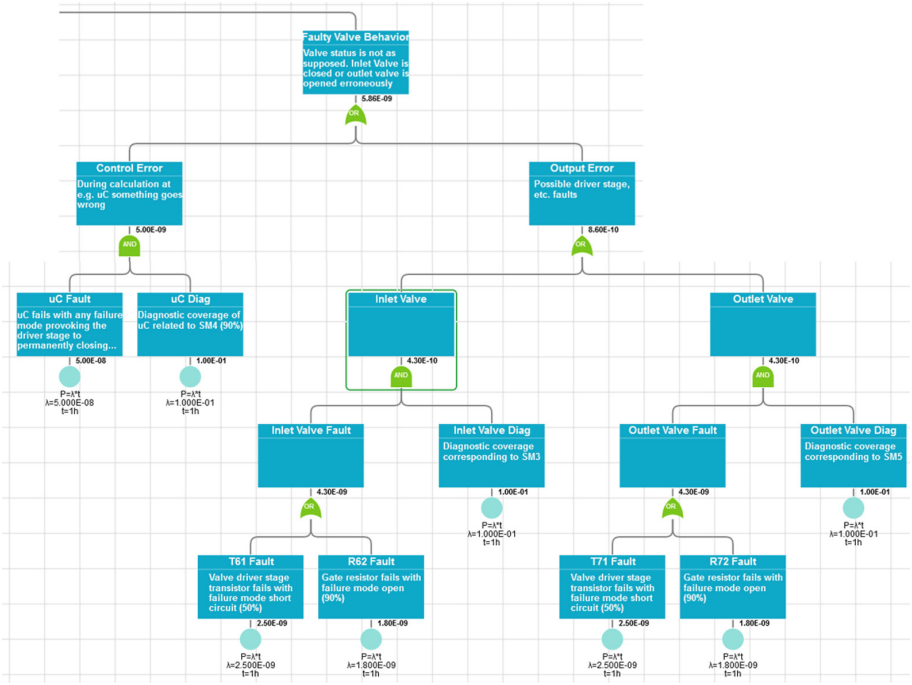

Fig. 8. Example fault tree consistent with the example shown in the HW FMEDA

Note: While for ASIL D a diagnostic coverage of 99% must be achieved the example "Function 2" in ISO 26262:2011 part 5 Annex E only used 90% diagnostic coverage. To stay consistent with the norm example we used 90% for the below calculations, although in the real case 99% should be applied (as described in section 2).

The diagnostic coverage of 90% used in Figs. 7 and 8 has been used in the norm example for wrong closing of the inlet valve can be detected by a decrease of pressure by the PTS sensor over a threshold of ms time.

Figure 9 shows a selected part of Fig. 8 (see the square in Fig. 8) which shows the necessary FTA design pattern to come up with same FIT for the safety goal in the calculation. Looking at Fig. 9 you see that the faults of the hardware are events connected by OR since if one fails the hazard will appear. The diagnose function is added to the FTA with an AND gate because the fault only becomes a hazard if the system diagnostic coverage of 90% (therefore multiplication with 1-09 = 0,1 = 10^{-1}) does not detect it.

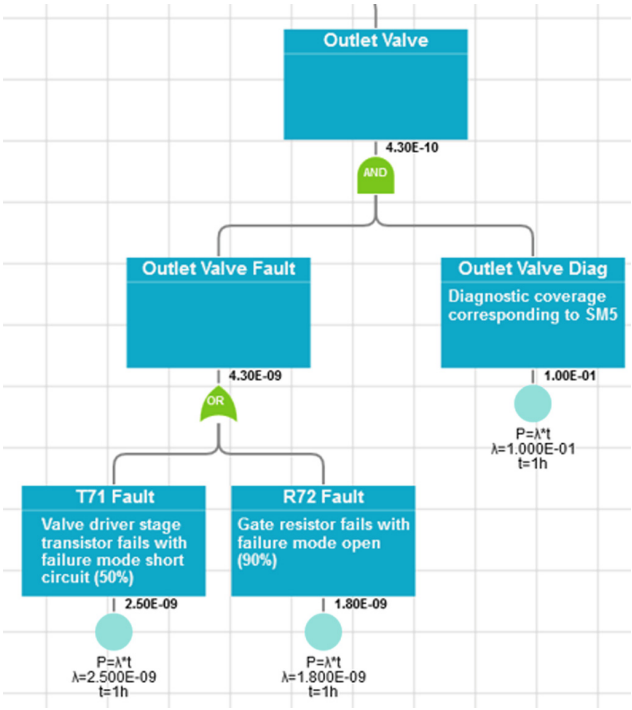

Fig. 9. Example fault tree – pattern combining diagnose coverage with FIT

FMEDA and FTA deliver same FIT results only if such design patterns are used and consistently compared. So if a further diagnostic coverage is considered in the FNEDA the FTA has to be updated correspondingly. FMEDA (bottom up) and FTA (top down) are different approaches, and still both should stay consistent and reach the FIT goals.

4 Expected Impact and Outlook

The example used in the ISO 26262:2011 part 5 Annex E. [1] does not contain background information on system level. This paper adds the missing background information and shows how the system safety concept decisions are mapped onto hardware architecture decisions. This can help readers of the ISO 26262:2011 and also the 2nd norm edition in 2018 to better understand the example of hardware architecture metrics in the context of a system use case.

Also the norm just mentions that FMEDA and FTA need to be done in ASIL – C and ASIL – D case but there is no example of how to achieve in both approaches the dame FIT goal. The paper adds such a consistency criteria.

This consistency approach is also explained in the SafEUr project materials and training developed together with the SOQRATES working party [5–8].

5 The SPI Manifesto Revisited

The SPI manifesto [14–16] describes values and principles which need to be considered to make improvements work in an organisation. One of the approaches is to start with an assessment and to derive an improvement list. This is then used to set up an improvement program.

The principle "**Use dynamic and adaptable models as needed**" means that depending on the need of organisations specific models can be adapted. The safety norm is such a new model which is needed in the Automotive domain.

The principle "**Base improvement on experience and measurements**" means that best practice experiences need to be shared and the usage must be tracked and measured. Since the model was developed in a group of Tier 1 in the SOQRATES working group the model development was based on such an experience and best practice sharing approach.

Also the measurement of FIT (Failure in Time) allows to design systems where the probability of a hazard decreases $< 10^8$ operating hours in cars. This is an important improvement concept for systems that can provide hazards, such as cars, planes, trains, etc.

An additional principle proposed for the SPI manifesto is: "**Observe new trends and state of the art practices on the market and adopt**". The product liability law and the RAPEX (www.rapex.com) database changed the market because hazardous faults as well as legal violations in cars lead to a mandatory recall action and all cars must be repaired. This creates huge cost and thus new state of the art standards like functional safety, cybersecurity etc. became an important issue.

Acknowledgements. We are grateful to the members of the SOQRATES [4] working group who have contributed: Alastair Walker (LORIT), Alexander Much (Elektrobit), Frank König, Martin Dallinger, Thomas Wegner (ZF Friedrichshafen AG), Armin Riess (BBraun), Dietmar Kinalzyk (HELLA), Ralf Mayer (BOSCH Engineering), Gerhard Griessnig (AVL), Andreas Gruber (ZKW), Rainer Dreves, Ivan Sokic, Stephan Habel (Continental), Christian Schlager, Thomas Stiglhuber (Magna Powertrain ECS), Andreas Riel (ISCN/Grenoble INP), Helmut Zauchner, Christoph Karner (KTM), Andreas Gruber (ZKW), Georg Macher (AVL), Bernhard Sechser (Methodpark), Lutz Haunert (G&D), Damjan Ekert (ISCN), Richard Messnarz (ISCN).

We are also grateful to the European Commission which has funded some of the initiatives that funded the development of skills in the Automotive sector. ISCN is a member of AQUA (Knowledge Alliance for Quality in Automotive Engineering, 2013–2015) [17, 18], and AQU (Automotive Quality Universities, 2015–2017), and the BLUEPRINT project DRIVES (2018–2021).

References

1. ISO - International Organization for Standardization: ISO 26262 Road vehicles Functional Safety Part 1-10 (2011)
2. Haken, K.L.: Grundlagen der Kraftfahrzeugtechnik. Carl Hanser Verlag, München (2013). ISBN 978-3-446-43527-8

3. ISO – International Organization for Standardization: ISO CD 26262-2018 2nd Edition Road vehicles Functional Safety (to appear)
4. SOQRATES: Task Forces Developing Integration of Automotive SPICE, ISO 26262 and SAE J3061. http://soqrates.eurospi.net/
5. Messnarz, R., Kreiner, C., Riel, A.: Integrating automotive SPICE, functional safety, and cybersecurity concepts: a cybersecurity layer model. Softw. Qual. Prof. **18**, 13 (2016)
6. Messnarz, R., Kreiner, C., Riel, A., et al.: Implementing functional safety standards has an impact on system and sw design - required knowledge and competencies (SafEUr). In: Software Quality Professional (2015)
7. Macher, G., Sporer, H., Brenner, E., Kreiner, C.: Supporting cyber-security based on hardware-software interface definition. In: Kreiner, C., O'Connor, R.V., Poth, A., Messnarz, R. (eds.) EuroSPI 2016. CCIS, vol. 633, pp. 148–159. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44817-6_12
8. Macher, G., Messnarz, R., Kreiner, C., et al.: Integrated safety and security development in the automotive domain, Working Group 17AE-0252/2017-01-1661. SAE International, June 2017
9. Redmill, F.: Understanding the use, misuse and abuse of safety integrity levels. In: Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK, 8–10 February 2000
10. Much, A.: Automotive security: challenges, standards and solutions. Softw. Qual. Prof. **18** (4) (2016)
11. Messnarz, R., et al.: Integrating functional safety, automotive SPICE and six sigma – the AQUA knowledge base and integration examples. In: Barafort, B., O'Connor, R.V., Poth, A., Messnarz, R. (eds.) EuroSPI 2014. CCIS, vol. 425, pp. 285–295. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43896-1_26
12. Kreiner, C., et al.: Automotive knowledge alliance AQUA – integrating automotive SPICE, six sigma, and functional safety. In: McCaffery, F., O'Connor, R.V., Messnarz, R. (eds.) EuroSPI 2013. CCIS, vol. 364, pp. 333–344. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39179-8_30
13. ABS Brake System, wikipedia. https://en.wikipedia.org/wiki/Anti-lock_braking_system
14. Korsaa, M., et al.: The SPI manifesto and the ECQA SPI manager certification scheme. J. Softw.: Evol. Process **24**(5), 525–540 (2012)
15. Korsaa, M., et al.: The people aspects in modern process improvement management approaches. J. Softw.: Evol. Process **25**(4), 381–391 (2013)
16. Messnarz, R., et al.: Social responsibility aspects supporting the success of SPI. J. Softw.: Evol. Process **26**(3), 284–294 (2014)
17. Larrucea, X., Mergen, S., Walker, A.: A GSN approach to SEooC for an automotive hall sensor. In: Kreiner, C., O'Connor, R.V., Poth, A., Messnarz, R. (eds.) EuroSPI 2016. CCIS, vol. 633, pp. 269–280. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44817-6_23
18. Larrucea, X., Walker, A., Colomo-Palacios, R.: Supporting the management of reusable automotive software. IEEE Softw. **34**(3), 40–47 (2017). https://doi.org/10.1109/MS.2017.68