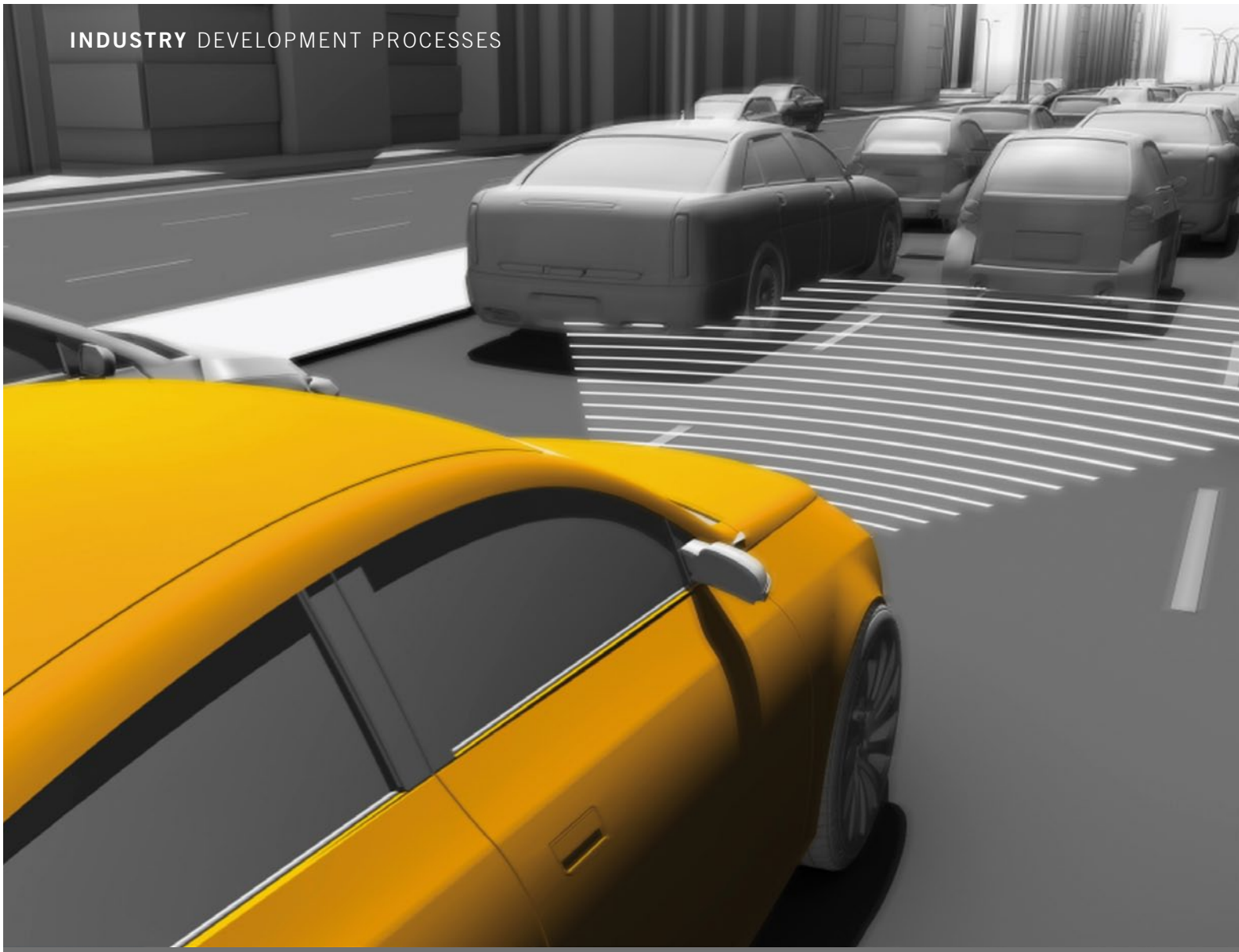


HAZARD ANALYSIS AND FUNCTIONAL SAFETY CONCEPT ACCORDING TO ISO 26262 FOR DRIVER ASSISTANCE SYSTEMS

In July 2009 the standard ISO / DIS 26262 was published describing the state of the art for the development of safety-relevant vehicle functions. Starting point for all safety activities according to ISO 26262 are hazard analysis and risk assessment of the considered function. Continental sketches the approach to the hazard analysis for the function Adaptive Cruise Control and exemplifies a functional safety concept.

AUTHOR

DR. JOHANNA SCHAFFNER
is Functional Safety Manager ADAS, Continental, Chassis & Safety Division, in Lindau (Germany).

HISTORY

In July 2009 the standard ISO/DIS 26262 [1] was published that describes the state of the art for the development of safety-relevant electrical/electronic (E/E) vehicle functions. If it cannot be proven in another way that a safety-related product was developed according to the state of the art, then the application of ISO 26262 is mandatory. Systems for passenger cars that will be brought on the market after the final publication of the standard – presumably mid of 2011 – must then be developed according to the norm, because ISO 26262 does not allow for any transition period.

Starting point for all safety activities according to ISO 26262 are hazard analysis and risk assessment of the considered function. By means of this analysis the risk potential of the vehicle function is determined without taking into account any safety measures. The result is described via the so-called Automotive Safety Integrity Level, in short ASIL. Corresponding to the outcome of the hazard analysis, safety goals are defined that must be fulfilled by an adequate functional safety concept.

To get an orientation concerning the risk potential of driver assistance functions, a group of experts from various automotive suppliers exemplarily determined the ASIL of some driver assistance systems. For driver assistance functions that have an impact on the vehicle dynamics quickly a high ASIL assignment arises when analyzing the unprotected function, i.e. the function without any safety measures. However, from the assignment of the vehicle function it cannot immediately be concluded the ASIL assignment of a sub-function like a sensor function. The safety relevance of the sub-function is resulting from the design of the functional safety concept. Typically, there are degrees of freedom available that can be used to implement sub-functions with a high ASIL assignment on a suitable system component and thus to achieve a cost-efficient solution. In the following, the approach for the hazard analysis is shown for the function Adaptive Cruise Control (ACC) and a functional safety concept is exemplified. The derived safety measures are allocated in the vehicle architecture. In this way it is illustrated which safety measures can be realized on which system component (sensor, engine control unit, brake control unit), and in particular which ASIL assignment is resulting for an ACC sensor function when using an appropriate decomposition. The explanations in this article are exemplary. There is no claim of completeness of risk assessment and safety measures.

HAZARD ANALYSIS

The hazard analysis methodology is defined in ISO 26262-3, chapter 7. Below, the approach is sketched. Basis is the description of the unprotected vehicle function including the selected system boundary, the so-called item definition. Item definition Adaptive Cruise Control [2]:

: distance control with regard to the preceding vehicle
: if no vehicle is preceding: velocity control to a value that can be set by the driver
: the ACC function is considered from environmental sensing to the actuation of brake and engine
: the ACC function is considered in the speed range v_min ≤ v ≤ maximum velocity, ACC during reversing is excluded (v min for example 25 km/h).

In the hazard analysis possible failures of the function in different driving scenarios and operation modes are examined. Here the failure effects are of interest, not the failure causes (Of course, failure causes play an important role in Functional Safety. In the hazard analysis, however, they are not yet in the focus. Causes are examined later in the safety lifecycle, i.e. during the safety analyses, for instance in an FMEA). The analysis is performed on a functional level without taking into account the concrete technical realization of the function in the vehicle. The failure effects are evaluated for each driving scenario using the parameters S, E, C. S stands for Severity, i.e. for the expected injury to persons in an accident. E describes the Exposure, i.e. the probability that the analyzed scenario does occur. C indicates the Controllability, that is, the ability of the involved persons to save the situation. ❶ shows which values for the three parameters shall be chosen. Informative examples can be found in ISO 26262-3, annex B. For each driving situation each of the parameters has to be determined. The risk assessment follows from the combination of the selected parameters. It is described by the so-called Automotive Safety Integrity Level

Class S	**S0**	**S1**	**S2**	**S3**	
Description	No injuries	Light + moderate injuries	Severe + life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries	
Class E	**E0**	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability
Class C	**C0**	**C1**	**C2**	**C3**	
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable	

❶ Choice of parameters S, E, C according to ISO/DIS 26262-3

Failure	Scenario	Failure effect	S	Comment to S	E	Comment to E	C	Comment to C	ASIL	Safety goal
Erroneous deceleration due to ACC	: Driving on highway with high velocity : Follower vehicle in short distance	Unintentional braking, worst case: maximum deceleration to standstill	3	Life-threatening injuries in front-rear crash with $\Delta v >$ 40 km/h	3	E4: Driving on highway E3: Follower vehicle in critical distance	3	Difficult to control or uncontrollable	C	Avoid dangerous unintentional braking
...										

❷ Excerpt of the ACC hazard analysis worked out by a group of experts

NO.	SAFETY GOALS	ASIL
SG1	Avoid dangerous unintentional braking	C
SG2	Avoid dangerous unintentional braking with vehicle destabilization	B
SG3	Avoid dangerous unintentional acceleration	B
SG4	Prevent ACC activation when reversing	A
SG5	Prevent ACC activation for 0<v<v_min	A
...	...	...

❸ Selected safety goals of the ACC hazard analysis

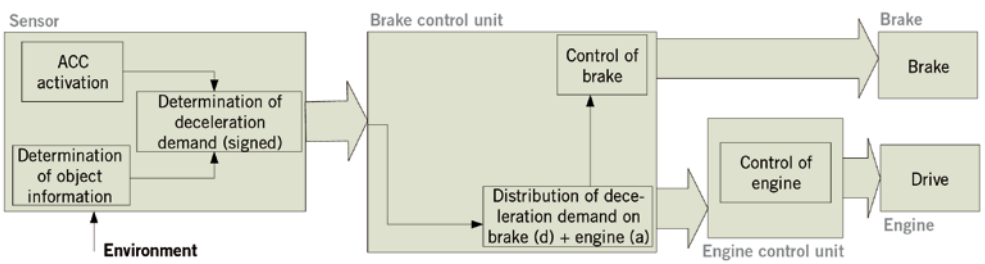
(ASIL) that is structured in four steps from A to D. ASIL A means the lowest degree of safety-relevance ASIL D the highest one. If a scenario is evaluated as non-safety-relevant according to ISO 26262, the term QM is used.

The ACC function can fail in different ways. For instance, the function can be activated or deactivated unintentionally; undesired braking, undesired accelerating, etc. can occur (Here, the probability that the vehicle function fails is NOT meant, but the probability for the occurrence of the driving situation). These cases can be illustrated in tables, they are detailed further and then evaluated. An extract for unintentional braking is depicted in ❷. Each scenario is assigned to a safety goal and a safe state which the function in case of a failure must take. The safety goal inherits the ASIL assignment of the scenario, ❸. For the ACC function the safe state is reached as soon as the function is deactivated and the driver is informed.

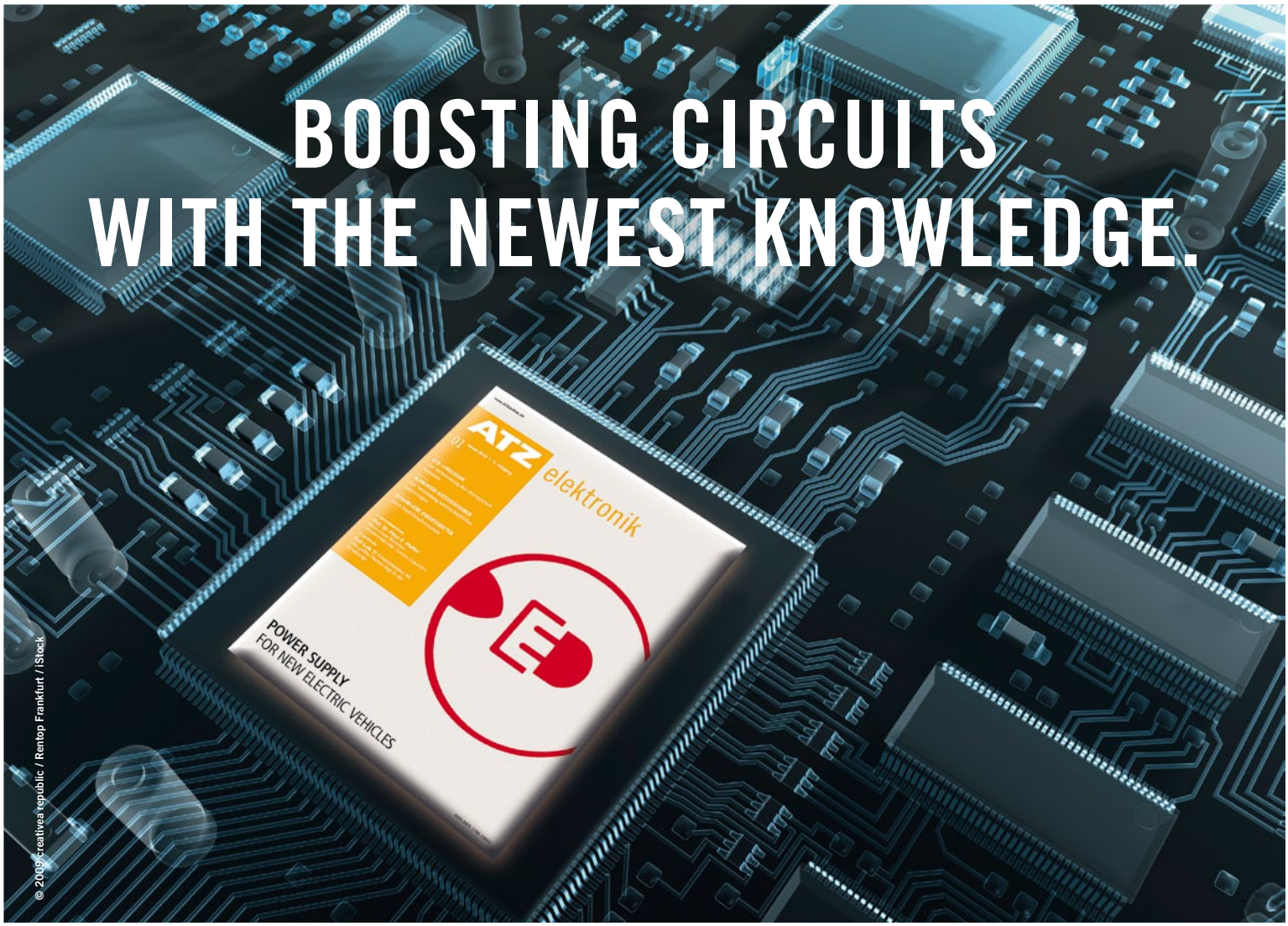
FUNCTIONAL SAFETY CONCEPT

Each safety goal must be completely fulfilled by one or several safety measures. These measures inherit the ASIL classification of the safety goal and thus they are assigned – according to the ASIL – requirements of ISO/DIS 26262 concerning type and quality of the development. In the standard, the safety concept is formulated on various abstraction levels. Starting point is the functional safety concept that defines safety measures on a functional level and that takes into account preliminary architectural assumptions only. From this, the technical safety concept is derived that is provided for the concrete system design. In the last step, safety requirements on HW and SW level are detailed. In the following, several possibilities for a functional safety concept for an ACC function are described.

Special for driver assistance systems is the fact that for their realization these functions have to be broken down in subfunctions and that they have to be distributed on different architectural components. Basically, the ACC function is divided into object detection, calculation of deceleration (signed), distribution of deceleration demand on brake and engine, realization of the demands. The system architecture is depicted in ❹.



❹ Sketch of a system architecture for the realization of the ACC function



PUT LEADING TECHNICAL KNOWLEDGE INTO GEAR NOW AND TRY ATZ ELEKTRONIK FOR FREE.

Electronics drive innovation and electronic knowledge drives careers. So take the test drive now and discover **ATZ elektronik**. Geared for professionals who seek unique in-depth information from testing to electric mobility, and much more. One free issue is reserved for you today. Simply fill in the form below and fax it to us.
More information at: www.ATZonline.de/leseprobe/atze

ATZ elektronik

YES, I WOULD LIKE TO TRY A FREE ISSUE OF ATZ ELEKTRONIK 311 10 503

Please send me the next issue of **ATZ elektronik** free of charge, without obligation. If I wish to continue receiving the magazine, I do not need to do anything. I will continue to receive the magazine at the price of only **€ 111.00** not including shipping fees. The subscription can be cancelled at anytime after receipt the previous issue. Any remaining portion of your subscription fees for issues not delivered will be refunded. CANCELLATION GUARANTEE: This agreement can be cancelled in writing within 14 days. To comply with the time limit, punctual dispatch (post mark) shall suffice. Mail to: Springer Automotive Media, Leserservice PF 18, Abraham-Lincoln-Straße 46, 65189 Wiesbaden.

COMPANY

FIRST AND LAST NAME

POSITION

DEPARTMENT

ADDRESS

POSTAL CODE / CITY

TELEPHONE

E-MAIL

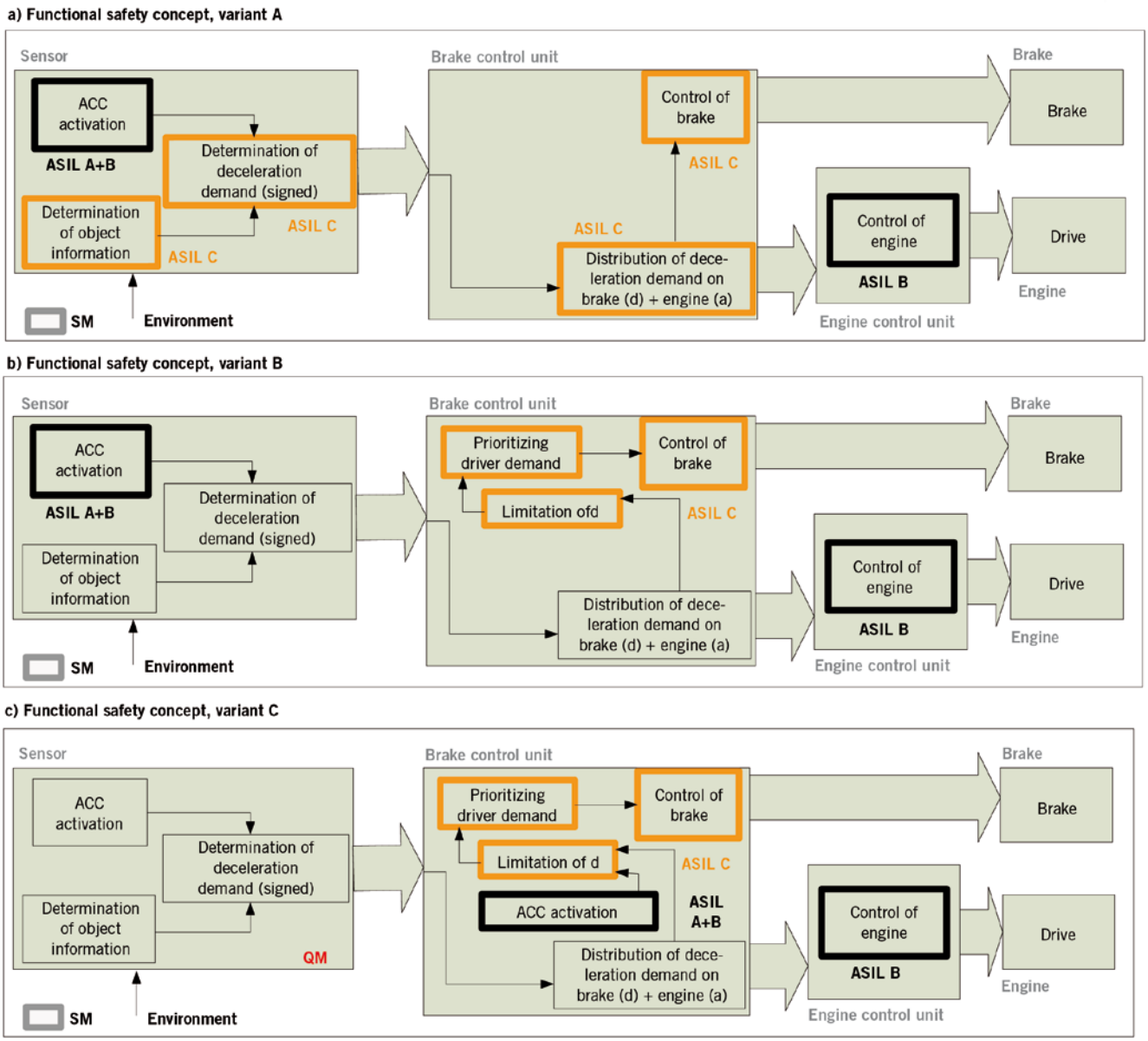
DATE / SIGNATURE

Simply fill in the form and fax it to **+49 (0) 611.78 78 – 4 07**
or send it via E-mail at **SpringerAutomotive@abo-service.info**

NO.	SAFETY MECHANISMS, VARIANT A	ASIL
SM1	Safeguard object information	C
SM2	Safeguard calculation of deceleration (signed)	C
SM3	Safeguard distribution of deceleration / acceleration demand for brake / engine	C
SM4	Safeguard realization of deceleration / acceleration demand on brake / engine, resp.	C and B, resp.
SM5	Safeguard ACC activation: ACC active only if 0<v_min<v	A
...	...	...

❺ Possible safety measures, variant A of the functional safety concept in ⑦

Faults and failures on all sensors and control units can lead to the violation of the safety goals. However, when deriving safety measures, there are often degrees of freedom available that can be used to find a cost-efficient solution. A first possibility would be to require that faults on each system component may not lead to a dangerous failure, see the safety measures in ❺. ❻ (variant A, of the functional safety concept) shows the distribution of these measures in the system architecture. In



❻ Variants of the functional safety concept for the ACC function

DOI: 10.1365/s38314-011-0005-x

NO.	SAFETY MECHANISMS, VARIANTS B AND C	ASIL
SM1	Safeguard deceleration demand d by limitation of value on d_max	C
SM2	Safeguard prioritization of driver demand (driver must be able to override ACC)	C
SM3	Safeguard ACC activation: ACC active only if ABS/ESC is available	B
SM4	Safeguard acceleration demand a by limitation of value on a_max	B
SM5	Safeguard ACC activation: ACC active only if 0<v_min<v	A
...	...	...

❼ Possible safety measures, variants B and C of the functional safety concept

this design, the ACC sensor (e.g. radar) and the brake control unit are assigned safety measures with ASIL C, the engine control unit measures with ASIL B. Does this mean that for the realization of an ACC function actually a sensor is required that is "ASIL C capable"? Variant A is – fortunately for the cost-efficient realization of ACC – not the only solution to fulfil the safety goals. Also the measures listed in ❼ are thinkable. These safety measures do not prevent unintentional braking, but unintentional dangerous braking so that the driver can still control the situation. In ⑦ (variant B), a possible distribution is illustrated where the ASIL-requirements for the sensor are less strict. In ⑦ (variant C), the safety measures are placed on the brake control unit. As the ESC function is also assigned a high ASIL and as the HW- and SW-platform of the brake control unit are designed accordingly, the allocation of the ACC safety measures on the brake control unit does not mean much additional effort. That is, if the sensor is embedded in a suitably derived functional safety concept, then no safety-relevant sub-functions must be implemented on it. Precondition of course is that during a distributed development like for driver assistance functions all development partners must contribute to functional safety. Therefore, the agreement on the functional safety concept and the binding distribution of responsibilities in the development of safety measures in a Development Interface Agreement (ISO/DIS 26262-8, chapter 5) are absolutely necessary.

SUMMARY

An excerpt of the hazard analysis according to ISO/DIS 26262 for an unprotected ACC function is presented. The safety goal with maximum ASIL C assignment is determined as "Avoid dangerous unintentional braking". To realize the safety goals on vehicle level several functional safety concepts can be developed. If it is possible to exploit the existing design of control units for the allocation of safety measures in a suitable way, a high development effort for the sensor development owing to functional safety requirements can be avoided. Therefore, it is important that already at the begin of the development the functional safety concept of a vehicle function is defined and agreed between automotive supplier and manufacturer in a suitable way.

REFERENCES

[1] ISO/DIS 26262, Road Vehicles – Functional Safety, part 1-10, 2009

[2] ISO 15622, Intelligent Transport Systems – Adaptive Cruise Control Systems, 2010

THANKS

These results have been worked out by a group of experts. The author thanks for their contribution: Rolf Adomat, Manager ADAS System Development, Continental, Lindau; Andreas Bisping, HW Functional Safety, Hella, Lippstadt; Volker Braschel, Functional Safety Consultant, TRW, Koblenz; Lothar Brossette, System-FMEA Electronic Brake Systems, Continental, Frankfurt/Main; Dr. Susanne Ebel, Process Expert Functional Safety, Bosch, Leonberg; Dr. Bernhard Schürmann, R&D Director Ultrasonic Systems, Valeo, Bietigheim-Bissingen.

ABBREVIATION	EXPLANATION
ABS	Anti Blocking System
ACC	Adaptive Cruise Control
ASIL	Automotive Safety Integrity Level
DIS	Draft International Standard
ESC	Electronic Stability Control
FMEA	Failure Modes and Effects Analysis
ISO	International Organization for Standardization
QM	Quality Management
SG	Safety Goal
SM	Safety Measure
v	Vehicle speed