Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

What We Are Talking About

ISO 26262 Functional Safety – Road Vehicles Workshop

Legal requirements and considerations in the application of ISO 26262

Responsibilties under the regime of ISO 26262

March 23, 2015
Dr. Ekkehard Helmig

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Ad personam:

- Attorney-at-Law with main focus on the automotive supplier industry
- Until 2003 European Counsel of an US-based power-train supplier
- Until 2002 Board member of Deutsche Gesellschaft für Qualität e.V. (DGQ) (German Society of Quality)
- Member of a working group of Clepa, the Association of European Automotive Suppliers in Brussels
- Counsel of European automotive suppliers
- Publications, Trainings

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

The goals of ISO 26262

- To make vehicles safer
- To avoid accidents
- To enhance the controllability
- To justify the trust of the driver

in the item of Functional Safety

The proof that all these goals have been achieved must be provided retrospectively when a hazardous event has happened. At that time people have a better knowledge or pretend to have a better knowledge about the reasons that the occurrence of the hazardous event could have been avoided.

And then they ask for responsible peoples and their individual roles.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Voices from the international discussion:

Question:
Is Functional Safety enough for Safety?

Reasoning:
„For a safety system, the correct behavior ist not easy to define.
It very much defines the safety of the system, and ISO 26262 does not provide any kind of guidelines, about how the behavior of the Vehicle should be to provide safety.“

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

It is true:
ISO 26262 does not provide safety.

However:
The statement that safety is provided and the vehicle
therefore is safe is expected by and sold to the customer, based on

- Audits
- Reviews
- Assessments

} Confirmation maeasures

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Functional Safety is a property of the item which can be verified (ISO 26262 -2-6.4.5.2. Note) by

Audits
Reviews
assessments under responsibilty of the Functional Safety Manager.

5.1.3.1 General

Three types of confirmation measures are defined within ISO 26262 to confirm the achievement of functional safety of the item. These are:

— the functional safety audit, which confirms the correct execution of the functional safety processes; 2-6.4.8

— the functional safety assessment, which confirms the steps taken to design, develop and execute a product design to ensure that the item achieves functional safety; and 2-6.4.9

— confirmation reviews, which confirm that applicable work products have achieved their specific goals for the development cycle. 2-6.4

3-7.4.5.1: To be performed by a person or persons from different Departments or organizations than the developer of the item.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Some requirements:

2-6.4.8 The appointed person for the functional safety audit shall provide a report that contains an evaluation of the implementation of the processes required for functional safety.

2-6.4.9.3: The appointed person for the functional safety assessment shall provide a report that contains a judgment of the achieved Functional safety.

2-6.4.9.6: including a recommendation for acceptance, conditional acceptance or rejection of the functional safety of the item.

2-7.4.2.1:The organization shall appoint a person with the responsibility and the corresponding authority to maintain the functional safety of the item after release for production.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Blue Print of NHTSA* for questions and answers

*National HighwayTraffic Safety Administration

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

U.S Transportation Secretary Foxx Announces Order to Preserve Defective Takata Air Bag Inflators for Ongoing Federal Investigation

NHTSA 07-15
Wednesday, February 25, 2015
Contact: Gordon Trowbridge, 202-366-9550, Public.Affairs@dot.gov

WASHINGTON – U.S. Transportation Secretary Anthony Foxx today announced that the National Highway Traffic Safety Administration (NHTSA) issued an order requiring Takata to preserve all air bag inflators removed through the recall process as evidence for both NHTSA's investigation and private litigation cases. The order also ensures NHTSA's access to all data from the testing of those removed inflators.

"This department is focused on protecting the American public from these defective air bags and at getting to the bottom of how they came to be included in millions of vehicles on U.S. roads," Foxx said. "This preservation order will help us get the answers we need to accomplish those goals."

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: General Order to Manufacturers (1):

REQUEST

1. File a report that describes, in detail, all completed, ongoing or planned testing of Takata inflators outside of the HAH Region. At a minimum, your report must include, but should not be limited to, the following:

   a. All documents regarding or relating to the testing contained in your report;

   b. The location of the testing; the dates of the testing; whether the testing is completed, in progress, or planned; anticipated date of completion of testing; the nature and objective of the testing; and, testing protocols;

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: General Order to Manufacturers (2):

c. A roster of all vehicles where the inflator was tested which includes: the model; model year; vehicle build date; VIN; the vehicle's registration history, by location; inflator serial number; inflator type; dealership location with zip code where the inflator unit was returned; whether any deaths, injuries or claims are associated with the inflator in the vehicle; and, product specifications for the air bag and inflator modules in each vehicle.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: General Order to Manufacturers (3):

d. If testing of inflators has been completed, describe in detail the results of the testing and the conclusions you have reached based upon the test results. If your conclusion is that a safety defect does not exist in inflators outside of the HAH Region, describe in detail the basis for that conclusion and when the decision was made and by whom. Provide a copy of all documents to or from any person(s) related to the conclusion that no safety defect exists in inflators outside of the HAH Region.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: General Order to Manufacturers (4):

e. Sub-part (e) is directed to BMW, Chrylser, Ford, GM, Honda, Mazda, Mitsubishi, Nissan, Subaru and Toyota: State in your report whether or not Takata has performed testing of inflators used in your vehicles outside of the HAH Region. If so, describe in detail what Takata has communicated to you about the testing and/or test results. Produce all documents related to Takata's testing, test results and your communications, internal and external, related to the testing. State whether you have requested additional information from Takata concerning its testing of inflators outside of the HAH Region which you believe would assist in your determination of whether a defect exists. Identify and describe any information, documents or categories of information and documents that you reasonably believe that Takata has or reasonably should have concerning inflators or testing of inflators used in your vehicles that Takata has not provided you and which you believe would assist you in testing inflators to determine whether a safety defect exists in inflators outside of the HAH Region.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: General Order to Manufacturers (4):

f. Provide the name, title and complete contact information for each and every manager or supervisor (at all levels of management or supervisory responsibility) involved in your investigation and decision-making process concerning rupturing air bag inflators manufactured, in whole or in part, by Takata.

g. Provide the name, title and complete contact information for each and every person who prepared and provided input and/or data included in the report contained in Request No. 1, including but not limited to inside or outside counsel, accountants, engineers, employees and other professionals.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: Special Order Takata (1):

REQUESTS

1. Explain the process by which Takata manufactures propellant for the Takata Inflators. Your response should include a summary of the step-by-step process from the time the chemical compounds are received at Takata's Moses Lake, Washington facility (or any other facility at which Takata receives chemical compounds) to the time the propellant wafers are shipped to the Takata Inflator manufacturing facilities.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: Special Order Takata (2):

5. Produce a chronology identifying each point in time that Takata made a change to the chemical composition of the propellant used in the Takata Inflators from January 1, 2000 to the present. Your response shall include the precise date and time on which the change was made, the Takata Inflators affected by the change, the nature of the change made to the propellant formula, and the reason(s) for that change.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: Special Order Takata (3):

7. Produce the names, titles, and complete contact information for each and every Takata employee who was involved in the decision to change the propellant formula.

8. Produce the names, titles, and complete contact information for each and every Takata employee who developed the propellant formula used in the Recalled Inflators.

9. Produce the names, titles, and complete contact information for each and every Takata employee who developed the propellant formula used in the Replacement Inflators.

10. Produce the names, titles, and complete contact information for each and every Takata employee who formulated the propellant used in the Recalled Inflators.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

NHTSA: Special Order Takata (4):

11. Produce the names, titles, and complete contact information for each and every Takata employee who formulated the propellant used in the Replacement Inflators.

12. Produce the names, titles, and complete contact information for each and every Takata employee who tested the propellant used in the Recalled Inflators.

13. Produce the names, titles, and complete contact information for each and every Takata employee who tested the propellant used in the Replacement Inflators.

14. Produce all documents that refer to, relate to, discuss or concern the propellant used in the Takata Inflators; including, but not limited to, any studies or testing of the propellant formulas.

15. Produce all documents that refer or relate to concerns or allegations (regardless of whether or not such concerns or allegations were substantiated) by any Takata employee or contractor, or any motor vehicle manufacturer, that ammonium nitrate is too volatile or that there is otherwise a problem with using ammonium nitrate in the propellant for the Takata Inflators.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Are you prepared to answer all these questions?

- **Do you have an "internal NHTSA"?**
- **You need a plan**
- **You need documents**
- **You need responsible peoples**
- **You need a Development Interface Agreement (DIA)**

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Verification and Validation of

assumptions
and
assessments

} All data are available or detectable

are performed **post** hazardous event or accident.

Remember:

Technician (Defendant)

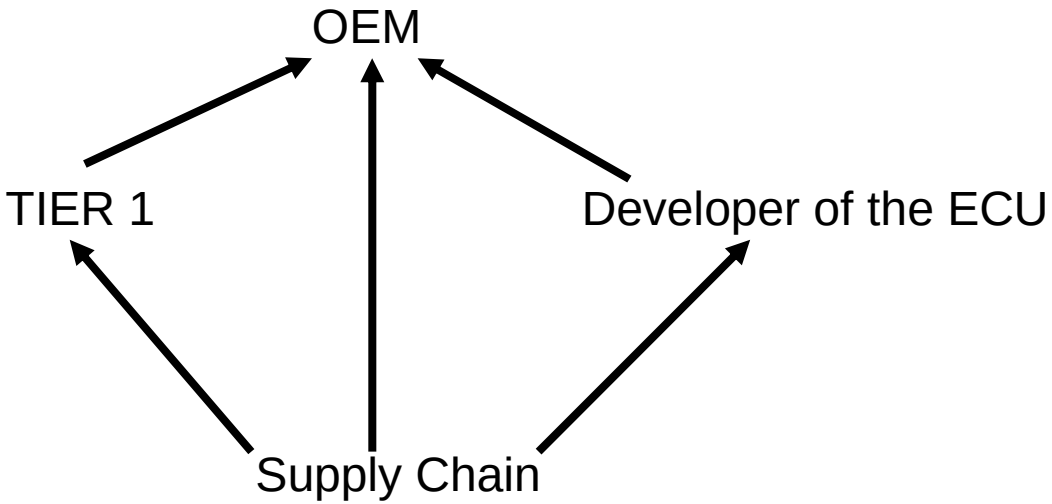
Driver (plaintiff)

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Case study and experiences:

New suspension - system



Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

The Development Interface Agreement is vital for each Participant

Due to European comprehensive Safety Culture it must be Consistent under safety perspectives and not cost considerations.

The OEM has the leadership on the validations level of the vehicle.

The suppliers have the leadership in the technology.

Together they have the responsibility for safety expectations of the driver and all other traffic participants.

1-136: Unreasonable risk: Risk judged to be unacceptable in a certain Context according to valid societal moral concepts.

Do you share all relevant information to your supply chain?
Is there the readiness of the OEM to listen to the supplier?
Have both the same integrity of assumptions?
Do they have the congruence of their goals?
Do they have the same language?
Do they have the same competence?
Is there an open communication?

Dr. Ekkehard Helmig
Rechtsanwalt

65189 Wiesbaden, Welfenstrasse 2
Telefon: 0611 77 87 20 – Fax: 0611 77 87 211
e-mail helmig@notar-helmig.de – http://www.notar-helmig.de

The number of suppliers is decreasing: Higher pressure

Automotive Suppliers

Less suppliers – more specific parts and systems

Challenge for competence

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

European Safety Culture European Legislation

Article 169 of the Lisbon Treaty

1. In order to promote the interests of consumers **and to ensure a high level of consumer protection**, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organize themselves in order to safeguard their interests.

Regulation
Directives
Decisions

Harmonized norms

ISO – CEN – CEN/ELEC
ISO 9001
ISO 65108
ISO 26262

Directive 2007/46/EC
Regulation 371/2010
ISO 9001 – ISO/TS 16949

Vehicle Manufacturers
Suppliers

Independence must
Correlate with all
Legal requirements

Product Safety
Product Liability

Vehicle drivers
Traffic participants
Consumers
Environment

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Legal Background and legal requirements

The Vienna Convention of 1968:
Article 8 requires that the driver of a vehicle must have the permanent control on his vehicle

Supporting European Legislation – European Safety Culture

Directive 2007/46/EC Type approval

Directive 2001/95/EC General Product Safety

Directive 85/374/EC Product Liability

Regulation 661/2009:
Type approval and general safety requirements

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Regulation 661/2009 Article 4

OBLIGATIONS OF MANUFACTURERS

Article 4

General obligations

1. Manufacturers shall demonstrate that all new vehicles sold, registered or put into service within the Community are type-approved in accordance with this Regulation and its implementing measures.

2. Manufacturers may choose to apply for type-approval with regard to all the systems, and the installation of all the components and separate technical units covered by this Regulation, or for type-approval with regard to one or more systems and the installation of one or more components and one or more separate technical units covered by this Regulation. Type-approval in accordance with the UNECE Regulations listed in Annex IV shall be considered as EC type-approval in accordance with this Regulation and its implementing measures.

3. Manufacturers shall demonstrate that all new systems, components and separate technical units sold or put into service within the Community are type-approved in accordance with this Regulation and its implementing measures.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Regulation 661/2009 Article 5

General requirements and tests

1. Manufacturers shall ensure that vehicles are designed, constructed and assembled so as to minimise the risk of injury to vehicle occupants and other road users.

Acceptable risk

2. Manufacturers shall ensure that vehicles, systems, components and separate technical units comply with the relevant requirements set out in this Regulation and its implementing measures, including the requirements relating to:

(a) vehicle structure integrity, including impact tests;

(b) systems to aid the driver's control of the vehicle, including steering, braking and electronic stability control systems;

Controllability

(c) systems to provide the driver with visibility and information on the state of the vehicle and the surrounding area, including glazing, mirrors and driver information systems;

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Article 6 of Directive 85/374/EC:

"A product is defective when it does nor provide the safety which a person is entitled to expect, taking all circumstance into account, including:

a) the presentation of the product;
b) the use it could reasonably be expected that the product would be put;
c) the time when the product was put into circulation."

Error
Fault
Failure

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 December 2001 on general product safety

Objective — Scope — Definitions

Article 1

1. The purpose of this Directive is to ensure that products placed on the market are safe.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Directive 2001/95/EC General Product Safety

General safety requirement, conformity assessment criteria and European standards

Article 3

1. Producers shall be obliged to place only safe products on the market.

2. A product shall be deemed safe, as far as the aspects covered by the relevant national legislation are concerned, when, in the absence of specific Community provisions governing the safety of the product in question, it conforms to the specific rules of national law of the Member State in whose territory the product is marketed, such rules being drawn up in conformity with the Treaty, and in particular Articles 28 and 30 thereof, and laying down the health and safety requirements which the product must satisfy in order to be marketed.

ISO 26262 3-7.4.2.1.1 vehicle is used correctly and incorrectly in a foreseeable way.

Safety case

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Directive 2007/46/EC of the European Parliament and of the Council
Establishing a framework for the approval of motor vehicles and their trailers,
And of systems, components and separate technical units intend for
Such vehicles

Article 4

Obligations of Member States

1. Member States shall ensure that manufacturers applying for approval comply with their obligations under this Directive.

2. Member States shall approve only such vehicles, systems, components or separate technical units as satisfy the requirements of this Directive.

Decision 768/2008 Conformity Assessment Procedures and Rules

Market Surveillance – Public Recall Procedures

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Directive 2007/46/EC

Article 12

Conformity of production arrangements

1. The Member State which grants an EC type-approval shall take the necessary measures in accordance with Annex X to verify, if need be in cooperation with the approval authorities of the other Member States, that adequate arrangements have been made to ensure that production vehicles, systems, components or separate technical units, as the case may be, conform to the approved type.

Article 29

Vehicles, systems, components or separate technical units in compliance with this Directive

1. If a Member State finds that new vehicles, systems, components or separate technical units, albeit in compliance with the applicable requirements or properly marked, present a serious risk to road safety, or seriously harm the environment or public health, that Member State may, for a maximum period of six months, refuse to register such vehicles or to permit the sale or entry into service in its territory of such vehicles, components or separate technical units.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Directive 2007/46/EC

Article 31

Sale and entry into service of parts or equipment which are capable of posing a significant risk to the correct functioning of essential systems

1. Member States shall permit the sale, the offer for sale or entry into service of parts or equipment which are capable of posing a significant risk to the correct functioning of systems that are essential for the safety of the vehicle or for its environmental performance, only if those parts or equipment have been authorised by an approval authority in accordance with paragraphs 5 to 10.

Article 32

Recall of vehicles

1. Where a manufacturer who has been granted an EC vehicle type-approval is obliged, in application of the provisions of a regulatory act or of Directive 2001/95/EC, to recall vehicles already sold, registered or put into service because one or more systems, components or separate technical units fitted to the vehicle, whether or not duly approved in accordance with this Directive, presents a serious risk to road safety, public health or environmental protection, he shall immediately inform the approval authority that granted the vehicle approval thereof.

Non-automotive devices or components interacting with items under ISO 26262 may conflict.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

REGULATIONS

COMMISSION REGULATION (EU) No 371/2010

of 16 April 2010

replacing Annexes V, X, XV and XVI to Directive 2007/46/EC of the European Parliament and of the Council establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive)

'*ANNEX X*

CONFORMITY OF PRODUCTION PROCEDURES

0. **Objectives**

0.1. The conformity of production procedure aims to ensure that each produced vehicle, system, component and technical separate unit is in conformity with the approved type.

0.2. Procedures include inseparably the assessment of quality management systems, referred to below as "initial assessment" and verification of the approval subject and product-related controls, referred to as "product conformity arrangements".

Is functional safety part of your QMS
Confirmation activities

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Directive 2007/46/EC Annex X in the version of Regulation 371/2010

1.3.1.1. When considering the extent of the initial assessment to be carried out, the approval authority may take account of available information relating to:

(a) the manufacturer's certification described in point 1.3.3 below, which has not been qualified or recognised under that point;

(b) in the case of component or separate technical unit type-approval, quality system assessments performed in the component or separate technical unit manufacturer's premises by vehicle manufacturer(s), according to one or more of the industry sector specifications satisfying the requirements in harmonised standard EN ISO 9001:2008.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

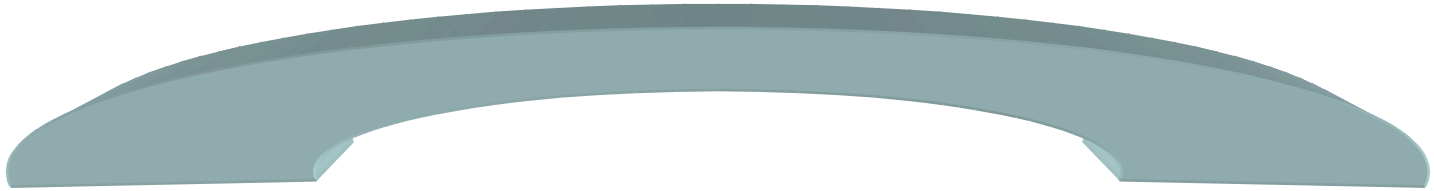
ISO 26262 does not address the nominal performance of an E/(E system (2-1)

No equation:
„Compliance with ISO 26262 = Vehicle Safety“

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Relation of ISO/TS 16949 and ISO 26262



Compliance with ISO 26262 is no property of the vehicle

Compliance with ISO 26262 only means adherence to stipulated processes Of ISO 26262.

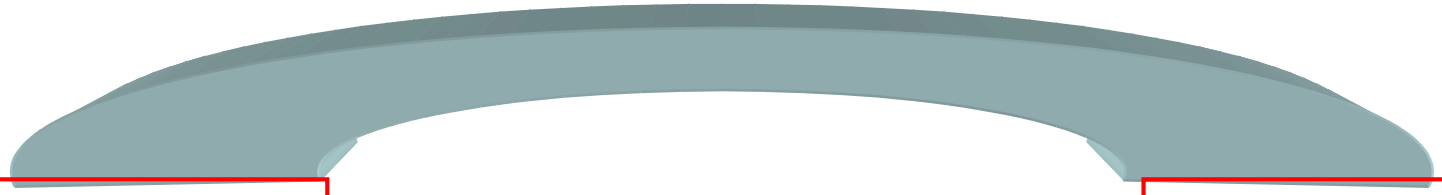
Processes of ISO 26262 are always processes under the regime of the Certified Quality management system. ISO 26262 does not encompass all all processes of ISO/TS 16949 (2-6.3.1).

ISO/TS 16949 is a Quality management system that ensures the conditions for the manufacturing of products without defects but does not produce such products.

Dr. Ekkehard Helmig
Rechtsanwalt

65189 Wiesbaden, Welfenstrasse 2
Telefon: 0611 77 87 20 – Fax: 0611 77 87 211
e-mail helmig@notar-helmig.de – http://www.notar-helmig.de

All processes of ISO 26262 must be integrated in system under ISO/TS 16949



ISO/TS 16949

Integration of ISO 26262

7.1 Planning of product realization
7.2.1 Determination of requirements related to product
7.2.2 Review of requirements related to the product
7.2.3 Customer communication
7.3 Design and development
7.3.1 Design and development planning
7.3.2 Design and development input
7.3.3 Design and development output
7.3.4 Design and development review
7.3.5 Design and development verification
7.3.6 Design and development validation
7.3.7 Control of design an development changes
7.4.1 Purchasing process
7.5. Production and service provisions
7.5.2 Validation of processes

Concept

Development

Production

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Scope of responsibilities when independence is required.

3-7.1: Hazard analysis and risk assessment (+ determination of Safety goals and ASIL determination):
to identify and to categorize the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risks.

4-11.4.2.1: Documentation of functional safety for release for production.

Names and signatures of persons responsible for the release.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

The **Functional Safety Manager** is not defined in ISO 26262:

So each person performing or conducting processes relevant for the application of ISO 26262 under ISO/TS 16949 must be deemed a Functional Safety Manager unless identified to the contrary.

The **Safety Manager** (1-109) is a **role**, not a person in the development phase (2-6.4.2.4) to organzise

- Planning and coordination of the functional safety activities
- Responsibility for maintaining the safety plan and monitoring progress
- Including DIA

.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

2-6.4.2.3: The **Project Manager** shall verify that the Organization has provided the required resources for the Functional safety activities.

The Project Manager shall ensure that the Safety Manager is appointed.

No defined hierarchy. Sole discretion of the OEM and the supplier.

2.6.4.7.2: Access to and support by the persons and organizational entities that carry out safety activities.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

2-5.4.2.8: The organization shall ensure that the person performing or supporting the safety activities are given sufficient authority to fulfill the responsibilities.

2-5.4.3.1: The organization shall ensure that the persons involved in the execution of the safety lifecycle have sufficient level of skills, Competence and qualification to their responsibilities.

Conclusions:
The functions of any responsible person within the context of performing compliance within ISO 26262 must be defines in the Quality Management System Manual, eligible for being audited under ISO/TS 16949 or e.g. VDA 6.1 and VDA 6.3.
The functions must comply with the processes at least on the highest levels of the confirmation measures.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Table 1 — Required confirmation measures, including the required level of independency

Confirmation measures	Degree of independency[a] applies to ASIL				Scope
	A	B	C	D	
Confirmation review of the hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5) Independence with regard to the developers of the item, project management and the authors of the work product	I3	I3	I3	I3	The scope of this review shall include the correctness of the determined ASILs and quality management (QM) ratings of the identified hazards for the item, and a review of the safety goals
Confirmation review of the safety plan (see 6.5.1) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the item integration and testing plan (see ISO 26262-4) Independence with regard to the developers of the item, project management and the authors of the work product	I0	I1	I2	I2	Applies to the highest ASIL among the safety goals of the item

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Confirmation review of the validation plan (see ISO 26262-4) Independence with regard to the developers of the item, project management and the authors of the work product	I0	I1	I2	I2	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the safety analyses (see ISO 26262-9:2011, Clause 8) Independence with regard to the developers of the item, project management and the authors of the work products	I1	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the software tool qualification report[b] (see ISO 26262-8:2011, Clause 11) Independence with regard to the persons performing the qualification of the software tool	—	I0	I1	I1	Applies to the highest ASIL of the requirements that can be violated by the use of the tool

Notation is misleading: Independence and responsibility cannot be partial or reduced.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Table 1 (*continued*)

Confirmation measures	Degree of independency[a] applies to ASIL				Scope
	A	B	C	D	
Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14) Independence with regard to the author of the argument	I0	I1	I2	I3	Applies to the ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate
Confirmation review of the completeness of the safety case (see 6.5.3) Independence with regard to the authors of the safety case	I0	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Functional safety audit in accordance with 6.4.8 Independence with regard to the developers of the item and project management	—	I0	I2	I3	Applies to the highest ASIL among the safety goals of the item
Functional safety assessment in accordance with 6.4.9 Independence with regard to the developers of the item and project management	—	I0	I2	I3	Applies to the highest ASIL among the safety goals of the item

[a] The notations are defined as follows:
- —: no requirement and no recommendation for or against regarding this confirmation measure;
- I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;
- I1: the confirmation measure shall be performed, by a different person;
- I2: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior;
- I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

[b] A software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle.

Independence is subject to the ASIL. There are at least two crucial aspects:
- You need independence in the determination of the ASIL
- You need independence based thereon in the assessments for the integrity of the confirmation measures.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Adversarial to the requirements

Examples for evaluating a safety culture

Table B.1 — Examples for evaluating a safety culture

Examples indicative of a poor safety culture	Examples indicative of a good safety culture
Accountability is not traceable	The process assures that accountability for decisions related to functional safety is traceable
Cost and schedule always take precedence over safety and quality	Safety is the highest priority
The reward system favours cost and schedule over safety and quality	The reward system supports and motivates the effective achievement of functional safety The reward system penalizes those who take shortcuts that jeopardize safety or quality
Personnel assessing safety, quality and their governing processes are influenced unduly by those responsible for executing the processes	The process provides adequate checks and balances, e.g. the appropriate degree of independence in the integral processes (safety, quality, verification, validation and configuration management)
Passive attitude towards safety, e.g. — heavy dependence on testing at the end of the product development cycle, — management reacts only when there is a problem in the field	Proactive attitude towards safety, e.g. — safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

The required resources are not planned or allocated in a timely manner	The required resources are allocated Skilled resources have the competence commensurate with the activity assigned
"Groupthink" "Stacking the deck" when forming review groups Dissenter is ostracised or labelled as "not a team player" Dissent reflects negatively on performance reviews "Minority dissenter" is labelled or treated as a "troublemaker", "not a team player" or a "whistleblower" Concerned employees fear repercussion	The process uses diversity to advantage: — intellectual diversity is sought, valued and integrated in all processes — behaviour which counters the use of diversity is discouraged and penalised Supporting communication and decision-making channels exist and the management encourages their usage: — self-disclosure is encouraged — disclosure of discovery by anyone else is encouraged — the discovery and resolution process continues in the field
No systematised continuous improvement processes, learning cycles or other forms of "lessons learned"	Continuous improvement is integral to all processes

Social, personal, competence conflicts Integrity at risk

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

9 Safety validation

9.1 Objectives

The first objective is to provide evidence of compliance with the safety goals and that the functional safety concepts are appropriate for the functional safety of the item.

The second objective is to provide evidence that the safety goals are correct, complete and fully achieved at the vehicle level.

9.2 General

The purpose of the preceding verification activities (e.g. design verification, safety analyses, hardware, software, and item integration and testing) is to provide evidence that the results of each particular activity comply with the specified requirements.

The validation of the integrated item in representative vehicle(s) aims to provide evidence of appropriateness for the intended use and aims to confirm the adequacy of the safety measures for a class or set of vehicles. Safety validation does cover assurance, that the safety goals are sufficient and have been achieved, based on examination and tests.

What is a representative vehicle?
What is the benchmark of **sufficient** ?
Where is the link to the driver?

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Table 3 — Classes of controllability

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

NOTE 2 The evaluation of the controllability is an estimate of the probability that the driver or other persons potentially at risk are able to gain sufficient control of the hazardous event, such that they are able to avoid the specific harm. For this purpose, the parameter *C* is used, with the classes C1, C2 and C3, to classify the potential of avoiding harm. It is assumed that the driver is in an appropriate condition to drive (e.g. he/she is not tired), has the appropriate driver training (he/she has a driver's licence) and is complying with all applicable legal regulations, including due care requirements to avoid risks to other traffic participants. Some examples, which serve as an interpretation of these classes, are listed in Table B.4. Reasonably foreseeable misuse is considered.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Functional Safety aims to safe lifes, health and environment

The focus is on the driver steering the vehicle: Requirement of controllability

The evaluation of the controllability is the assessment of the probability, that the driver is capable to control the hazardous event to avoid specific harms.

What do you know about the driver? The driver does not know what you know from and what your are expecting from him, his skills and his behaviour

The benchmark of the norm is the average driver.

The controllability of each hazardous event, by the driver or other traffic participants, shall be estimated based on a defined rationale of each hazardous event (ISO 26626-3-7.4.3.7)

Does the rational you have defined reflect secured knowledge of the driver?

Information must be provided to the driver.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

B.4 Examples of controllability (chances to avoid harm)

The determination of the controllability class, for a given hazard, requires an estimation of the probability that the representative driver will be able to retain or regain control of a vehicle if a given hazard were to occur.

This probability estimation involves the consideration of the likelihood that representative drivers will be able to retain or regain control of the vehicle if the hazard were to occur, or that individuals in the vicinity or the situation will contribute to the avoidance of the hazard by their actions. This consideration is based on assumptions about the control actions necessary by the individuals involved in the hazard scenario to retain or regain control of the situation, as well as the representative driving behaviours of the drivers involved (which may be related to the target market, individuals' age, eye-hand coordination, driving experience, cultural background, etc.).

NOTE Controllability estimations can be influenced by a number of factors including the cultural background of the analyst, the target market for the vehicle, or driver profiles for the target market.

How is the cultural background defined and reflected in the concept of the item?
How is it possible to reflect this scenario?

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Integrity of confirmation measures for work products

What provides evidence?

Which documentation is required?

„Safety cases are often based on estimated and predicted System and operator behaviour rather than observed evidence.“

Over time the predicted behaviour might be challenged by further developments, disclosure of errors or shifting regulatory context (ISO 26262 -10-5.3.4)

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Legal Benchmark:

Newest state of science and technology.

Science is not addressed in the norm.

Science includes the science of the driver
not „only“ of technologies.

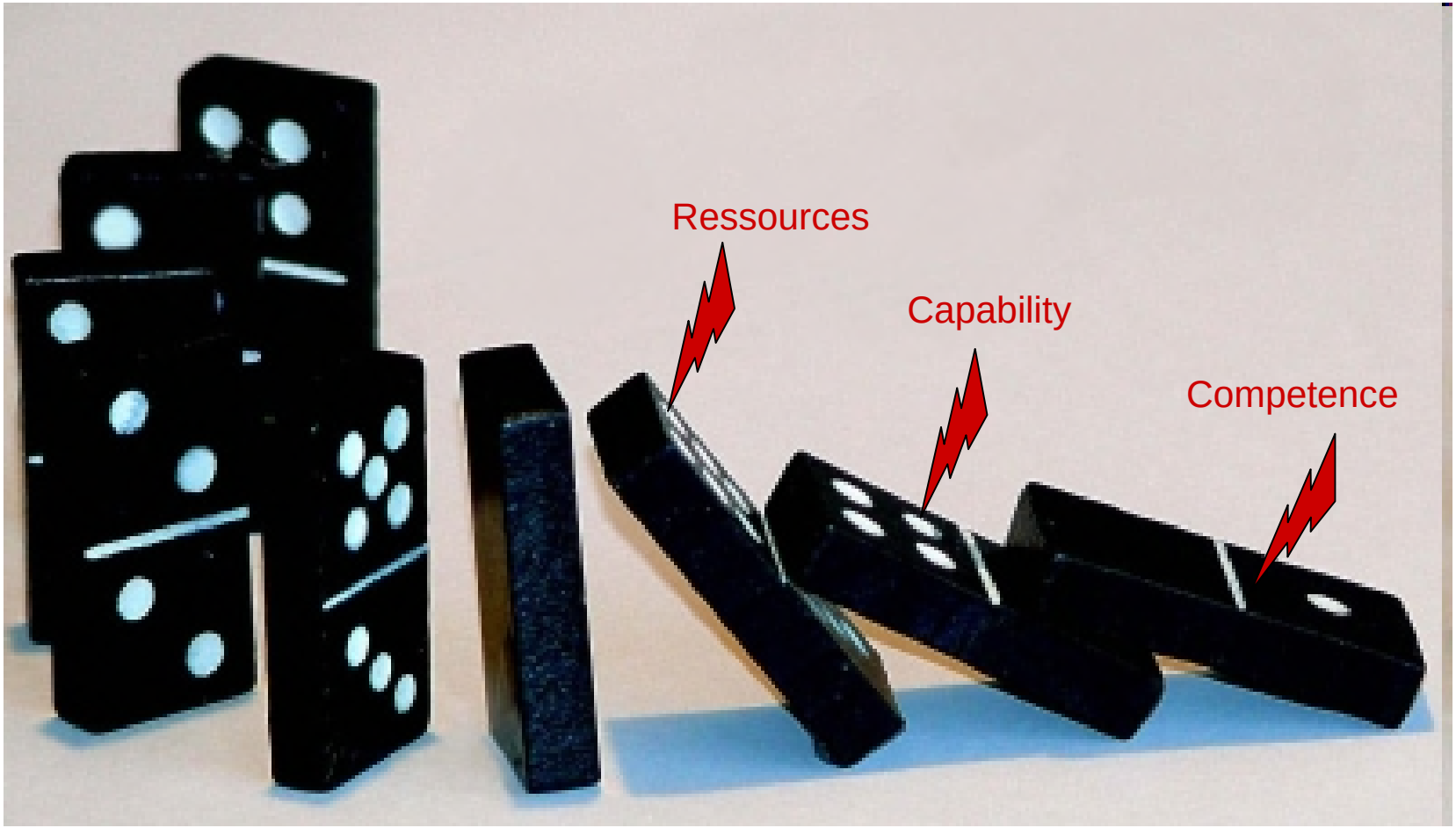
Best practices of the industry are legally irrelevant.

Misleading:
ISO 26262:10-4.1
The requirements for hardware development and software development are adapted for the state-of-art in the automotive industry. There is no such state-of-the art.

Dr. Ekkehard Helmig
Rechtsanwalt

65189 Wiesbaden, Welfenstrasse 2
Telefon: 0611 77 87 20 – Fax: 0611 77 87 211
e-mail helmig@notar-helmig.de – http://www.notar-helmig.de

The Domino - Effect



Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de

Conclusions:

•Adherence to ISO 26262 is following process discipline

•ISO 26262 is a framework for virtual products

•Virtual products must be validated in physical devices

•Validation of physical devices on vehicle level

•Relevant is the expectation of the driver

•Integrity of audits, reviews and assessments

•All data required post hazardous events must be retraceable in the previous work products.

The validity is based on the independence of responsible persons who are deemed to be the guarantors of the integrity of all assumptions, data and judgments complying with the reasonable expectations of the driver.

Dr. Ekkehard Helmig
Attorney-at-Law

D-65189 Wiesbaden, Welfenstrasse 2 – Phone +49 611 77 87 20
e-mail Helmig@Helmig-Regula.de – http://www.Helmig-Regula.de