



Dr. Ekkehard Helmig
Attorney-at-Law

D-65193 Wiesbaden, Richard-Wagner-Straße 51 – Phone +49 611 77 87 20
e-mail Helmig@ra-Helmig.de – <http://www.ra-Helmig.de>



Operational Safe
Systems
September 25 - 27, 2018
Berlin, Germany



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



Legal is nasty: Only Sometimes ...



**We are in the same party: I am challenging as if
I were the plaintiff to avoid that your were the defendant**



You are selling the future

I am trying to follow you

Do we both have rules?

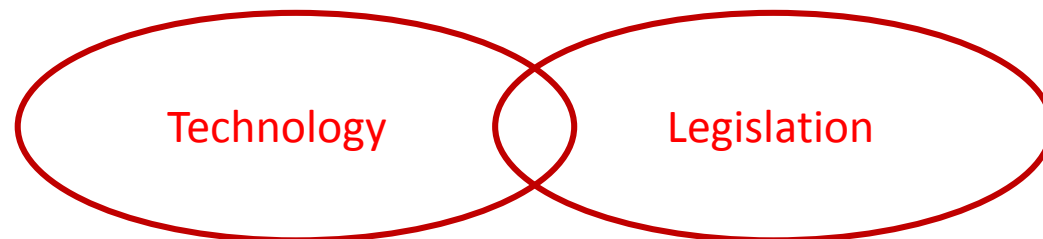
Yes, we both have rules: from yesterday and today

Rules for the future must be invented and anticipated

Lawmakers are behind the development of technologies

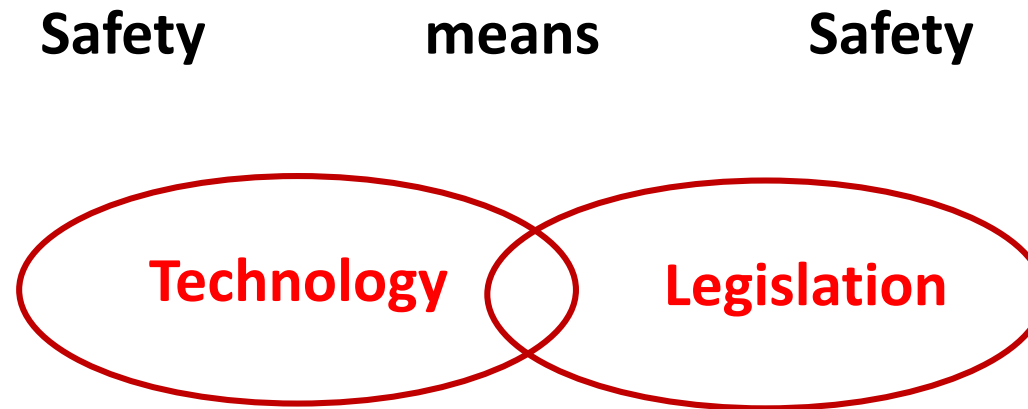
Legal and technical Standards are missed

Discussing today is: Both we are avantgarde for the future





The bridge: Technical terms are Legal Terms and vice-versa:





Again:

Discussing today is: Both we are avantgarde for the future.

But

We need answers:

Worldwide the number of safety related recalls is increasing rather than decreasing.

Where is the confidence for the trust in future technologies
Based on the knowledge of today?

Where is the confidence to verify the expectation that autonomous vehicles will
reduce the numbers of fatalities?

Insurers are sceptic. Why?



Dienstag, 11. September 2018, 10.00 Uhr

Conti feiert überraschendes Jubiläum: 50 Jahre fahrerloses Fahren

Conti celebrates surprising anniversary: 50 years Driving without a driver

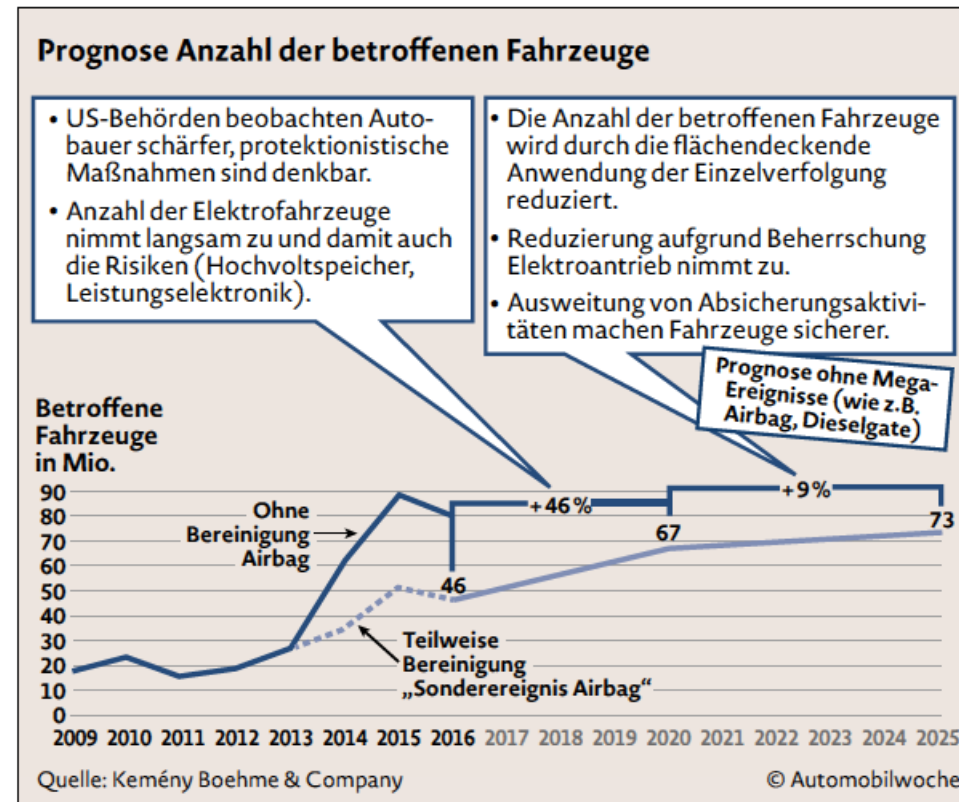


Of course, today we are advanced ...



Recalls versus future technologies

RÜCKRUFKATIONEN IN DEN USA



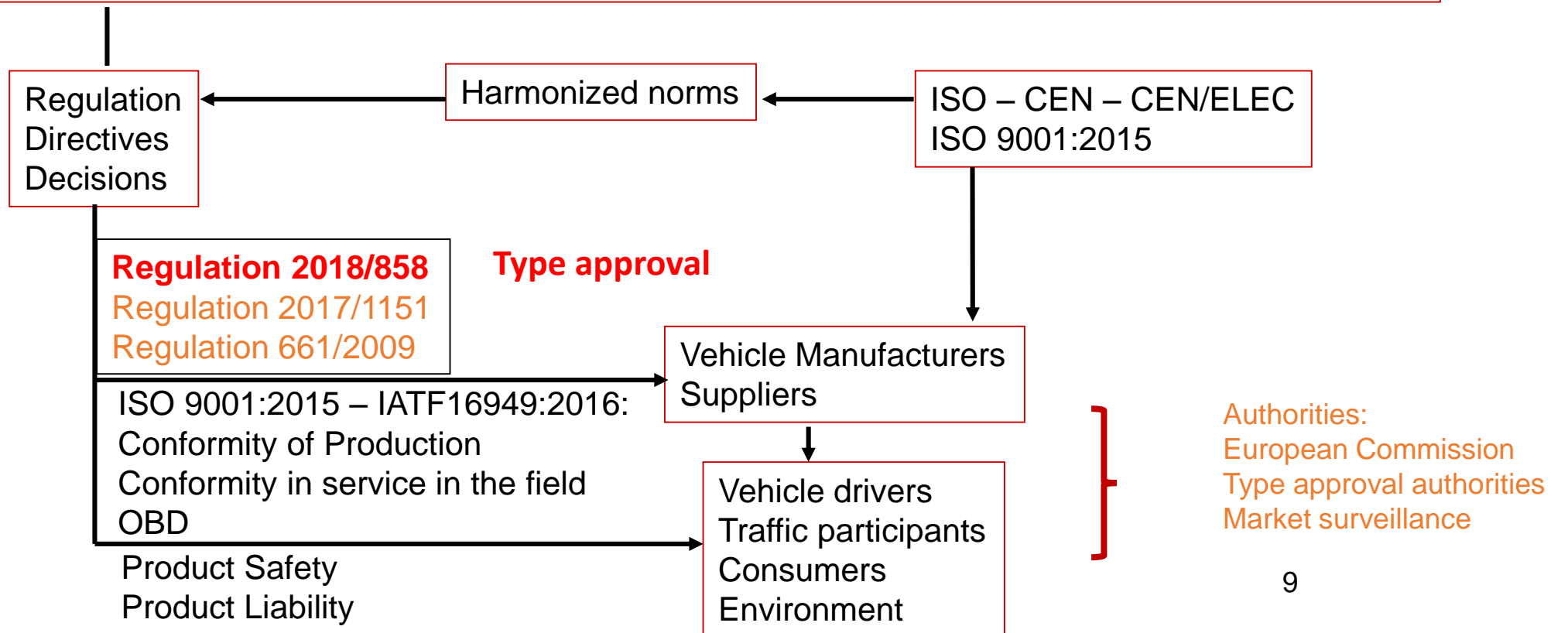


European Safety Culture European Legislation Compliance



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.





The European Lawmakers have learned from the Diesel – affaires

The cristal clear message of the European Lawmakers is the

REGULATIONS

REGULATION (EU) 2018/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 30 May 2018

on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC

(Text with EEA relevance)

Quite a challenge



The cristal clear message is:

Abiding by the laws is not a sign of weakness

Abiding by the laws is an attitude

Not abiding by the laws does not create heros.

Abiding by the laws is self protection:

The Laws provides the instruments of self protection



REGULATION (EU) 2018/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 30 May 2018

on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC

Article 5

2. Vehicles, systems, components and separate technical units shall be considered not to comply with this Regulation in the following cases in particular:
- (c) if any information given by the manufacturer in the information document is not reproducible under all the conditions set out in the relevant regulatory act by approval authorities, market surveillance authorities or the Commission.



The Power of Market Surveillance

- (34) ‘market surveillance’ means the activities carried out and measures taken by the market surveillance authorities to ensure that vehicles, systems, components and separate technical units as well as parts and equipment made available on the market comply with the requirements set out in the relevant Union harmonisation legislation and do not endanger health, safety, the environment or any other aspect of public interest protection;
- (35) ‘market surveillance authority’ means the national authority or authorities responsible for carrying out market surveillance on the territory of the Member State;

Article 8

Obligations of market surveillance authorities

1. Market surveillance authorities shall carry out regular checks to verify that vehicles, systems, components and separate technical units comply with the relevant requirements. Such checks shall be performed on an adequate scale by means of documentary checks and, where appropriate, laboratory tests and on-road tests conducted on the basis of statistically relevant samples.



The Power of the European Commission

Article 9

Compliance verification by the Commission

1. The Commission shall organise and carry out, at its own expense, tests and inspections to verify that vehicles, systems, components and separate technical units comply with the relevant requirements.

The tests and inspections shall be performed, *inter alia*, by means of laboratory tests and on-road tests, on the basis of statistically relevant samples, and shall be supplemented by documentary checks. e.g. type-approval

When carrying out those tests and inspections, the Commission shall take account of:

- (a) established principles of risk assessment;
- (b) substantiated complaints; and
- (c) any other relevant information, including information exchanged in the Forum, testing results published by recognised third parties that meet the requirements laid down by the implementing acts referred to in Article 13(10), information concerning new technologies on the market and reports resulting from on-road remote sensing.



Article 9

4. For the purpose of enabling the Commission to carry out the tests and inspections under this Article, Member States shall without undue delay make available to the Commission the necessary information related to the type-approval of the vehicles, systems, components and separate technical units that are subject to compliance verification. That information shall include at least the information included in the EU type-approval certificate and its attachments referred to in Article 28(1).

5. Manufacturers shall make available to the Commission, free of charge and without undue delay, any data which are needed for the purpose of compliance verification and which are not available in the EU type-approval certificate and its attachments referred to in Article 28(1).

Such data shall include all parameters and settings that are necessary to accurately replicate the test conditions that applied at the time of the type-approval testing. The Commission shall adopt implementing acts specifying the data that are to be made available, subject to the protection of commercial secrets and the preservation of personal data pursuant to Union and national law. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 83(2).

For the control of compliance of series vehicles



Article 12

Article 12

Online data exchange

1. The Commission and the Member States shall use the common secure electronic exchange system referred to in Article 27 for EU type-approval certificates and their attachments referred to in Article 28(1), including for any test reports as well as amendments, refusals or withdrawals of any EU type-approval.

The Commission and Member States shall use the Rapid Information System (RAPEX), established under Directive 2001/95/EC of the European Parliament and of the Council ⁽¹⁾ and the Information and Communication System on Market Surveillance (ICSMS), established under Regulation (EC) No 765/2008 for market surveillance, recalls and other relevant activities between market surveillance authorities, Member States and the Commission.



Article 13

Article 13

General obligations of manufacturers

1. Manufacturers shall ensure that the vehicles, systems, components and separate technical units that they have manufactured and that are placed on the market have been manufactured and approved in accordance with the requirements laid down in this Regulation, and in particular, those in Article 5.
2. Manufacturers shall be responsible to the approval authority for all aspects of the approval procedure and for ensuring conformity of production.
6. Manufacturers shall establish procedures to ensure that series production of vehicles, systems, components and separate technical units remains in conformity with the approved type. See Article 9
7. Manufacturers shall examine any complaints they receive relating to risks, suspected incidents or non-compliance issues with the vehicles, systems, components, separate technical units, parts and equipment that they have placed on the market.



- That means:
- Absolute completeness and integrity of the data provided for type approval
 - Absolute transparency
 - Conformity of Production in accordance with EN ISO 9001:2015
 - Absolute correctness of the Certificate of Conformity to be issued for each buyer of a vehicle
 - Continued conformity of vehicles in service over lifetime
 - Protection against hacker attacks
 - Permanant Monitoring by authorities
 - Sanctions and penalties up to € 30.000 per vehicle.



Relation between ISO 9001:2015, IATF 16949 and ISO 26262



Conformity of Production under Regulation 2018/858

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 9001:2015 and IATF 16949 are safety oriented.
They include in total all processes of ISO 26262.

See: NHTSA „Assessment of Safety Standards for Automotive Electronic Control Systems.



Article 25: Unlimited Transparency to the Authorities

4. The approval authority and technical services shall have the access to the software and algorithms of the vehicle that they consider to be necessary for the purpose of carrying out their activities.

The approval authority and technical services may also require the manufacturer to supply documentation or any additional information needed to allow the approval authority or technical services to develop an appropriate level of understanding of the systems, including the system development process and the system concept, as well as the functions of software and algorithms that are necessary to verify compliance with the requirements of this Regulation, to take a decision on which tests are required or to facilitate the execution of those tests.

Justification processes for the key aspects:

Expectation
Anticipation
Assumption
Conclusion



Conflicting or respective terms:

Expectation:	Article 2 (3, lit. f) Directive 2001/95/EC Product Liability reasonable consumer expectations concerning safety
Anticipation	ISO 26262 – 1.93: „Reasonably foreseeable event: „event that is technically possible and has credible or measurable rate of occurrence“ Directive 2001/95/EC: safe: „under normal or reasonably foreseeable conditions of use including duration ...“
Assumption	Data base derived from expectations
Conclusion	Instruments for conclusions: ISO 26262 – 1.17: confirmation measures: audit, review, assessment including „inspections (1.67)



In legal terms:

**Expectations need a solid and documented base
of all reasonable assumptions and conclusions showing
ex post
that you have anticipated all ramifications derived from
Security and Safety.**



What is the base of expectations?

**Expectation is based on assumptions of present knowledge
to be verified and proved in and by the future**

**If you raise expectations you have the responsibility that the
assumptions for the expectations have a solid base.**

**It is irrelevant whether you believe that expectations are
technically reasonable.**

**It is only relevant that the expectations you have raised are congruent
with and justified by the operation conditions performed by the driver.**



This should not have happened Something went wrong





Think: Anticipation versus recourse

Defect prevention

Prediction of capability
to develop:
That will not happen

Prediction of quality
Of Production:
We make it, yes we can



Proof of no defect

Reconstruction of des
Failure in the Development:
What did we miss?

Reconstruction of
Production process deficiencies:
Has everything been ok??



Burden of proof ante accident versus post accident



This should not have happened: Liabilities?



- (+): Drivers
- (+): Vehicle Manufacturers
- (+): Suppliers
- (+): Software Developers
- (+): Hardware Developers
- (+): IT-Providers (Connectivity)
- (+): Maintenance
- (+): Repairs



In legal terms:

Each successful hacker attack

provides

the prima facie evidence

**of a defective and an unsafe product
(e.g. Regulation 2017/1151 Article 5 (3 lit. f)).**

You

**have the burden of prove that there were no chance
to avoid the successful hacker attack.**

No excuse: It were Force Majeure





Highly diversified markets and competition: A matter of Competence

The development of hardware and software by non-automotive companies without standards for purposes even in the testing phase not designed especially for the automotive applications; availability of hardware and software at any time at any place at any needed volume and at comprehensive compatibility. Off-the-shelf sensors such as lidar and radar have a limited field of view and range (AN 02.04.2018, p. 59). They are not mature at the time.

Who has the competence to integrate all components, systems for a autonomous driving vehicle eligible in the environments of London, Berlin, Shanghai or Timbuktu?

Note: ISO 26262 -1.8 „Availability“ = „capability of a product to be in a state to execute the function required under given conditions, at a certain time or in a given period, supposing the required external resources are available.“



The proven - in use – argument (ISO 26262-8-14)

“A proven in use argument can be applied to any type of product whose definition and conditions of use are identical to or have very high degree of commonality with a product that is already released and in operation. It can also be applied to any work product related to such product.”

Proven – in use- credit (14.4.2)

Product history

Conflicting reference market policies.

ISO 26262 – 1.90: “evidence, based on analysis of field data resulting from use of a candidate, that the probability of any failure of this candidate could impair the safety goal of an item that uses it meets the requirements of the applicable ASIL.

Conflict with: ISO 26262 – 1.41: “Well-trusted” = previously used without knowing safety anomalies”



Artificial Intelligence and Machine Learning: Fascinating, but ...

Future vehicles will be better by applying need Artificial Intelligence and Machine Learning technologies. I am skeptical: It is true that AI and ML educate the hardware to enhance the scopes of application. But hardware and software have their own brains and are learning in their own processes steered by the developer according to his brain which must not necessarily be congruent. There is always -and most likely will be- a difference at the interfaces between the world of facts of AI and ML to reality. **When is a result advanced enough and who decides under which conditions?** Not to mention moral and ethics.



Legally:

AI and ML are nothing else but technologies or methods under the same pressure of verification, validation and justification as any other or method. And compliance with adequate and acceptable social criteria, moral and ethics. **Any conflict?**



Under legal considerations:

What is the relation between anticipation and an algorithm?

Does the algorithm anticipate binding social and/or legal rules, if any?

Can they make a distinction between


What should be and what will happen?

Who is driving whom?

The algorithm is causing and creating decisions according
to which criteria in which hierarchy of the systems?

Reactions of the System?

consequences or impacts?

Burden of proof post incident encompassing the vehicle manufacturer
and the entire supply chain (ISO 26262 and ISO 9001:2015)
relative to social and legal rules, and ... 



... ← Capability of the driver under environmental conditions
and infrastructure

Note: ISO 26262 – 1.19: „Controllability“ = „ability to avoid a specific harm or damage through the timely reactions of the persons involved, possibly with support from external measures.“

Driver's education:

Ford, GM and FCA have a program to educate the driver to raise the driver's alertness and to stimulate the driver's excitement for the future vehicle in his presence. The driver of today is not the driver of tomorrow. In Europe the manual for the use of the vehicle is mandatory. However, who ever has read a manual will admit, that is hardly to digest.

Driving schools: Do they need an education with simulators, taught by whom?



Autopilot:

No continuous awareness and alertness

Routine versus routine: Scope of reflection

Legal requirement:

Always expect unexpected incidents

And be ready to react idealistically

Idealistically means anticipating all alternatives



OBD – Functions and Requirements: Can we trust in OBD devices and functions?
Under European Legislation (UN-ECE 83) OBD-Systems are mandatory.

They have at least two main aspects:

Warning to the driver

Storing of data and functions for containment actions under Regulation 2018/858

Under legal aspects they must be true, of integrity, transparent, documented

The data storing, however, ist ambiguous:

It shows the conditions of driving operations

It shows correct or malfunctions of the driver's behaviour

It saves the driver or the manufacturer

The insurers are keen on all data

Note: ISO 26262 -1.25: „Diagnostic coverage“ = „proportion of the hardware element failure rate that is detected or controlled by the implemented safety mechanisms.“

ISO 26262 – 1.34: „emergency operations“ = „degraded functionality from the state in which a fault occurred until tge trabsition to a safe state is achieved as defined in the warning degradation concept.“



What about redundancies in the systems (ISO 26262- 1.60 multiple but identical implementations of a requirement)?

An airplane has always 3 systems for the same applications:

3 Auto pilots

3 hydraulic systems

3 inertial reference systems

All three systems control each other. If one of them is without defined tolerances it will be shut down in a specified process.

Redundancies might be a legal requirements for safety

Or

You need good and valid arguments for refraining from the installation of redundancy devices.



Connectivity as a matter of common language:

Let's assume that connectivity technically works and exists, is there a common language for the communication? If there were a common language, is it ensured that each vehicle and each driver knows the meaning of the language and are able to react accordingly in the appropriate manner and way to exclude accidents or, at least, to give way as expected by the other vehicle or the other vehicle in accordance to the environmental conditions which have features not necessarily designed in the connectivity technologies between the vehicles?



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 responsibility 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.



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 are identical to those stipulated under EN ISO 9001:2015 and IATF 16949 and Type-approval requirements.

The questions are always:

- Who was responsible?
- Who has signed the results?
- What was the base of any decision making?



Some requirements: They are identical with the requirements of ISO 9001:2015

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.





Summary:

Operational Safe Systems must meet legal criteria
Meeting Safety criteria must be evidenced to the authorities
Evidence means transparency and integrity of all data
The authorities are the watchdogs of integrity

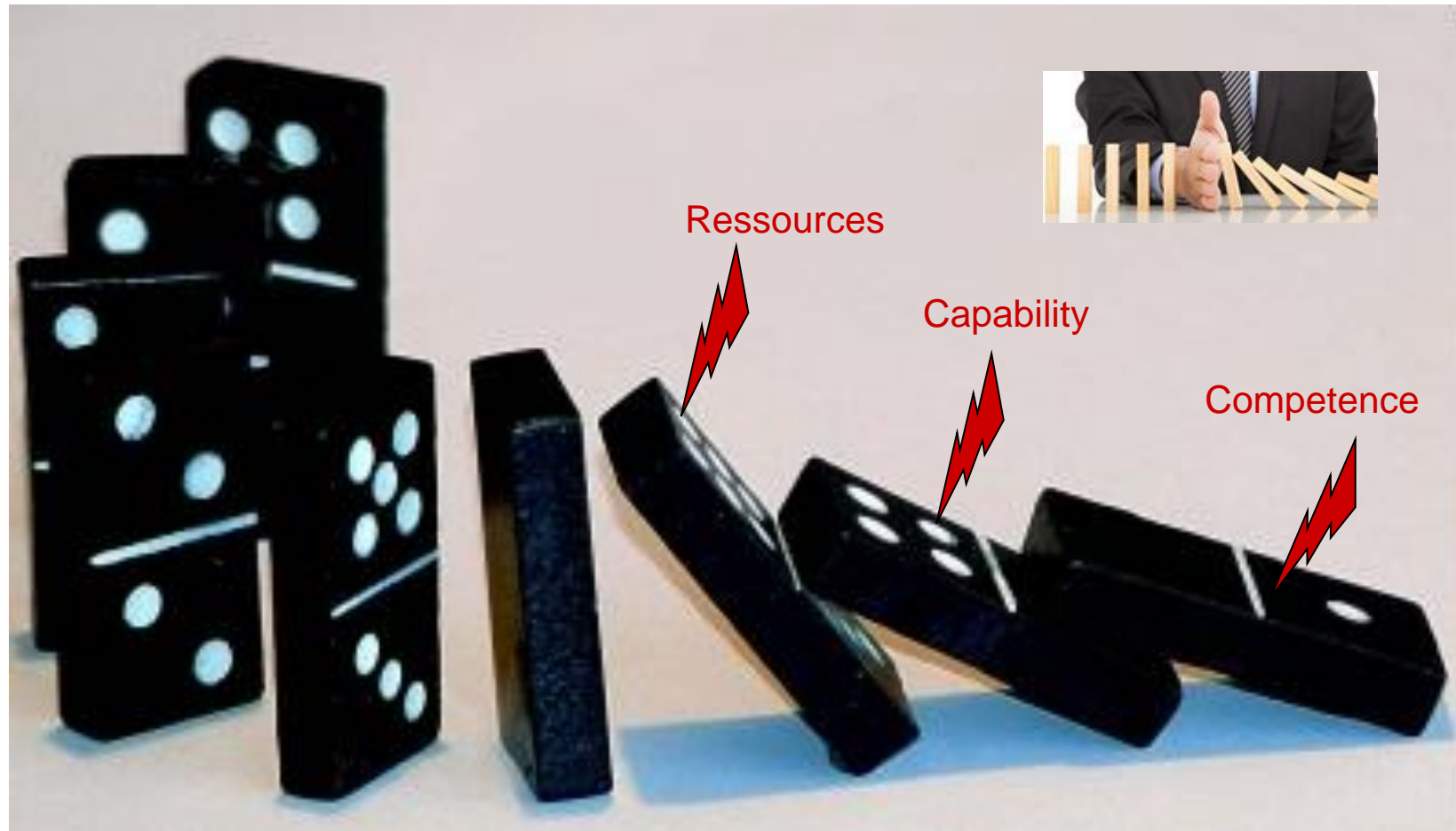
Expectation, assumption, anticipation and conclusion must follow rules
ISO 26262 provides rules but no solutions
Conformity with ISO 26262 does not necessarily mean safety

Processes to obtain safety must be secured under ISO 9001:2015
(Conformity of Production)
The processes of ISO 26262 are processes under ISO 9001:2015
Compliance with both must be guaranteed by the Certificate of Conformity

Under ISO 9001:2015 and ISO 26262 responsible peoples must be named
Responsible mean responsibility.



The Domino - Effect





Dr. Ekkehard Helmig
611 77 87 20
Attorney-at-Law

D-65193 Wiesbaden, Richard-Wagner-Strasse 51 – Phone +49

e-mail Helmig@Ra-Helmig.de – <http://www.Ra-Helmig.de>

