ISO 26262 in Practice – Resolving Myths with Hazard & Risk Analyses

Pierre Metz
Brose Fahrzeugteile GmbH & Co. KG, Hallstadt, Germany

Stefan Kriso
Robert Bosch GmbH, Germany

Peter Grabs
intendis GmbH & Co. KG, Germany

Content

1. Recollection: Objectives of HRA and understanding of S,E,C

2. Myths resolved

Hazard Analysis & Risk Assessment (HRA)

- **Method for determining safety-relevance acc. to ISO 26262-3**

- **Objectives:**
  - Determining safety goals against identified hazards
  - Deriving their ASIL acc. to the determinations along 3 dimensions:
    - Exposure (E0 to E4)
    - Severity (S0 to S3)
    - Controllability (C0 to C3)

- **HRA shall assume the absence of safety measures and warning mechanisms!**

Controllability	Exposure	Severity			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

Severity

- ***NOT***:

  Percentage classifications of potential direct *and cascaded/propagated* injuries that may be sustained in accidents, as a result of a hazard, to the driver, passengers, and other road users.

- **BUT**:

  Percentage classifications of the potential direct ~~and cascaded/propagated~~ injuries …

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
AIS 0 and less than 10% probability of AIS 1-6	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5-6

Exposure

- ***NOT***:

  Probability of product fault/failure occurrences that lead to the hazard.

- **BUT**:

  Probability of a human's *exposure* to a hazard *in terms of time and location* in particular scenarios during *expectable* (mis-)use cases.

E0	E1	E2	E3	E4
Incredible	Very low probability	Low probability	Medium probability	High probability
Never	Less often than once a year	A few times a year	Once a month or more often	Almost every drive
0%	Not specified	<1% of average operating time	1%-10% of average operating time	>10%

Controllability

- ***NOT***:

  Ability to mitigate, or prevent, the hazard itself.

- **BUT**:

  Probability of being able to withdraw oneself from the severity impact, thereby avoiding or alleviating the injury, once exposed to a hazard.

  May *not* reflect: warning concepts, implementations of safety goals

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
	99% or more of all drivers	90% or more of all drivers	Less than 90% of all drivers

Content

1. Recollection: Objectives of HRA and understanding of S,E,C

2. Myths resolved

Myth 1 – The higher the ASIL, the higher the risk

<u>Correction:</u> risk and ASIL are not the same thing

- **Risk**
  - "Combination of the probability of occurrence of harm and the severity of that harm" (26262-1)
  - Risk = f (frequency, C, S) while frequency = E x λ (26262-3, Annex B)

- **ASIL**
  - Four classes by which requirements of ISO 26262 are categorized into the dimenions 'product-', 'process-', and 'method-orientation'
  - Thereby represent expectations for finding a technical solution in order to finally reduce residual product risk
  - Are assigned to safety goals

Myth 2 – The possibility of a dead individual means S3

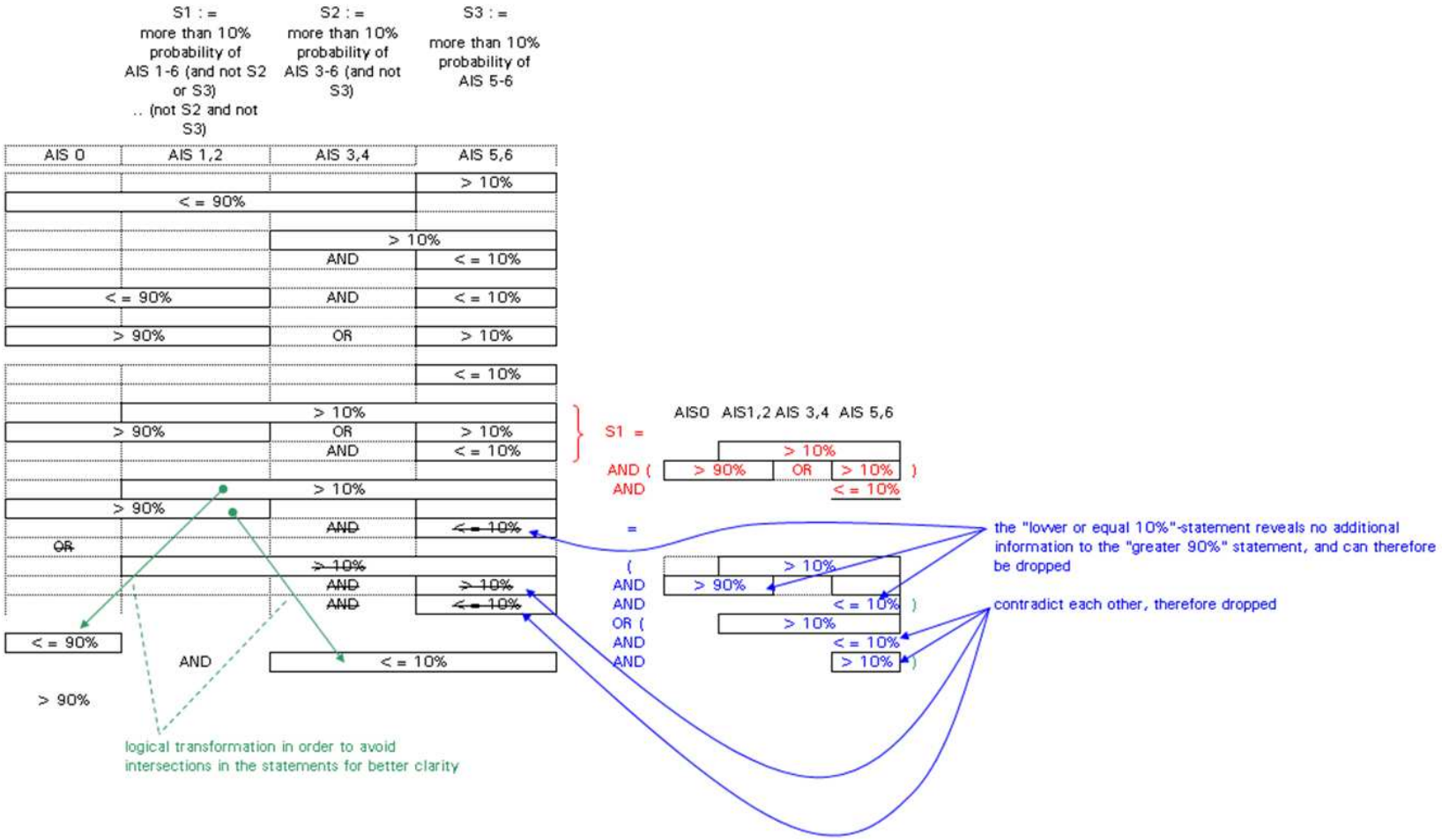
Correction

- S3 says "life-*threatening*", i.e. not necessarily death
- 26262-3, Table B.1 implies:

	S0	S1	S2	S3
	No injuries	light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 and less than 10% probability of AIS 1-6 Damage that cannot be classified safety-related	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5-6

	AIS 0	AIS 1,2	AIS 3,4	AIS 5,6
S3				> 10%
S2	≤ 90%			≤ 10%
S1	≤ 90%		≤ 10%	
S0	> 90%			

For further reading: deduction for the above, if of interest



Myth 3 – S3 severity implies the necessity of ASIL D

brose
Technik für Automobile

Correction

- **Severity is not to be mistaken with the ASIL itself**
- **ASIL D is implied only if the following applies *at the same time*:**
  - Severity of S3
  - Controllability of C3 (i.e. vast majority of driver and/or participants cannot avoid the harm once exposed to the hazard)
  - Exposure (temporally and physically) to the hazard of E4

Controllability	Exposure	Severity			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

intedis

BOSCH

Myth 4 – Severity and Controllability can be judged by one's own considerations and everyday experience only

<u>Correction</u> – the following sources need to be considered primarily:

(1) market & field experiences incl. statistics
(2) testing and validation results (e.g. road trials)
(3) law
(4) cultural context

Examples for (3)

- **Window regulators:**
  Forces ≤ 100 N are safe[1]

- **Indicators/flasher (German: "Blinker"):**
  German traffic regulations (StVO) say that indicators do not replace the driver's responsibility for anticipation and care

Example for (4)

- **Indicators/flasher (German: "Blinker")**
  In some countries (e.g. Italy, India) flashers are not even always used (cultural reasons) → utmost care is taken → lower C

Therefore, the authors of this paper do not fully agree with ASIL B for indicators[2]

[1] USA & Canada FMVSS 118, Europe & Japan 74/60/EWG 2000/4/EG, Australia ADR 42/03, Brasilia CONTRAN 762/1992

[2] A.Biermeyer, Hella, " Share Knowledge For E/E Improvements In the field of Lighting", IQPC ISO 26262 conference, Munich, 2012

Myth 5 – Properties of geographical regions, or driving situations, can depend on the perspective of the analyzing party, or designated market (1/2)

- **Examples**[*]
  - Parking brake failure in a **downhill situation** (S2, C3), but
    - **E4** in the Alpes
    - **E0** at the coast
  - Door/closure system failure when **vehicle is drowning** (S1, C2), but
    - **E1** in the Alpes
    - **E2** for the Netherlands
  - Oversteering DTA (S3, C3) on **snowy roads**
    - **E1** for Dubai
    - **E3** for Sweden

[*)] See also M.Klauda, Bosch, "ISO 26262 – Was kommt da auf uns zu?", Elektronik im Kraftfahrzeug, Baden-Baden, 12.-13.10.11, pages 11,15

Myth 6 – Properties of geographical regions, or driving situations, can depend on the perspective of the analyzing party, or designated market (2/2)

- **Don'ts**
  1. The HRA shall not be limited to certain perspectives or designated markets
  2. Neither "just the lowest" nor "just the highest" E shall be selected
  3. Do not just calculate an arithmetic mean
- **Dos**
  1. Evaluate S,E,C of each hazard for each situation/ scenario/ market/ environment
  2. Deliberately derive (and document) a weighted mean/average
  3. Evaluate this weighted average against current technical state-of-the-art
- ***Note however***:

  "A very detailed list of operational situations for one hazard, with regard to the vehicle state, road conditions and environmental conditions, can lead to a very granular classification of hazardous events.
  This … can lead to a consequential reduction of the respective classes of exposure, and thus to an inappropriate lowering of the ASIL …" (ISO 26262-3)

Myth 7 – Exposure addresses the probability of the scenario only

- **Example child lock in door system**
  - E4: end of queue at traffic lights or end of traffic jam
  - S3: (pessimistic)
  - C2: some grown-ups are able to draw child back if quick enough = ASIL C

- **Correction**
  - Exposure has to consider *any* coincidence associated with the hazard!

- **Corrected example:**
  - **E2**: … **& child old enough to be able to physically unfasten seat belt and to push door open, and child then actually running behind car, or entering other lane, and then actually colliding with other vehicle**
  - S3: …
  - C2: … = **ASIL A**

Myth 8 – Items/systems ‘classified‘ as QM are not safety-relevant

brose
Technik für Automobile

Correction:

- **Every product has risk! … and zero risk is generally impossible!**
- **Acc. to 26262 risk is classified acc. to S,E,C**
- **Any system shall be analyzed against hazard potential and risk**

Therefore,

- **a resulting risk class of QM can still reveal S3, E4, or C3, respectively**
- **QM then means that**
  - there is no obligation (but the freedom) to define safety goals acc. to, nor to comply with, ISO 26262
  - however, a QM system needs to be in place which, in turn, requires the addressing and mitigation of product risk (irrespective of ISO 26262)…
  - …and, thus, other types of safety beyond FuSa

e.g.
- safety against environmental influences
- usage safety (German: “Gebrauchssicherheit“)

intedis

BOSCH

Myth 9 – When making HRAs consistent with FMEAS, B = 10 cases must receive an ASIL

- **Fact:**
  - FMEA: harm to individuals → B = 10
    - e.g. smoking motor because of hazardous vapour
    - e.g. poor thermal insulation of a hybrid-electric power train

- **Falsely perceived implication*:**
  - B = 10 cases represent a hazard in terms of safety goal violation
  - Hence, B = 10 cases always are to receive ASIL A or higher

- **Therefore, B = 10 cases…**
  - may still lead to a QM classification acc. to ISO 26262
    (e.g. smoking motors receive C0 as the vehicle can generally be left upon realizing smoke, smell, and heat)
  - which may indeed lead to a high probability of death may still not be in the scope of functional safety (e.g. poor electrical insulation of a hybrid-electric power train)

*) "harm to individuals" → B = 10" is an implication and not an identity, i.e. acc.to propositional logic .
from A → B = TRUE does not follow B → A = TRUE

Myth 10 – In a FMEA, violation of legal norms are mostly classified B = 9 or 10, and, therefore must receive an ASIL

brose
Technik für Automobile

Correction:

- **A violation of a legal norm is, in the first place, a formal and legal issue and does not necessarily have functional safety relevance.**

- **Examples:**
  - CO2 emission ≥ threshold
  - §54 StVZO says indicators ("Blinker") shall reveal a rate of 1.5 +/– 0.5 Hz
  - §57(3) StVZO says an odometer ("Wegstreckenzähler") shall have a max. deviation of +/– 4%
  - 2002/95/EG (RoHS) prohibits the use of lead; violating this does not have any functional influence.

➔ **Therefore, violations of legal requirements do not necessarily represent a hazard.**

intedis

BOSCH

Myth 11 – 26262-2 should come with a list of pre-classififed (into ASIL) systems and vehicle funcions

Correction:

- **A reconciled worldwide pre-classification is not possible**

Why?

- 26262-2 requires the item to be exactly defined (system context, non-functional characteristics, precise functionalities, technology used etc.). Hence, a “braking system“ for OEM x is not necessarily “the same“ as for OEM y
- The evaluation of a particular driving situation (e.g. wet vs. dry roards) may differ across geographical regions (e.g. Ireland experiencing ‘all seasons of the year in one day‘ vs. Spain)
- The evaluation of controllability may differ across geographical regions (e.g. experiences with icy roads when living in the Alpes vs. Dubai)
- Further, any technical standard is meant to abstract from concrete technology and process/method frameworks in order to be applicable to, and acceptable in, any context worldwide.

- **Thus, pre-classifications would reduce freedom of interpretation that is crucial as otherwise a ‘standard‘ would not be able to serve as a consolidated state-of-the-art.**

Thank your for your attention.

...Questions?

pierre.metz@brose.com

peter.grabs@intedis.com

stefan.kriso@de.bosch.com

Acknowledgements to:
- Berthold Carl, Brose Fahrzeugteile GmbH & Co. KG
- Adam Schnellbach, Magna Powertrain AG
- Andreas Töpperwein, Preh GmbH