Safety Assessments

Safety Case Traceability

Certificate

ECQA Training Body Certificate

In the name of the
European Certification and Qualification Association
we hereby state that the

I.S.C.N. GesmbH

Accreditation No.: SAFEUN-ECQA-TRAININGBODY-2014-019

has successfully met all the requirements for the certification as an

ECQA Certified Training Body
for the ECQA Certified Safety Manager

and is now authorized to organize courses for
this ECQA certified job role.

Krems, 31st March 2014
Date

Prof. (FH) Mag. Michael Reiner
President of ECQA

Issued by
European Certification and Qualification Association (ECQA)
Parkringgasse 1, A 3500 Krems, Austria
www.ecqa.org

VDA Verband der Automobilindustrie

Certificate
Accreditation as intacs™ Training Provider

this is to certify that

I.S.C.N. GesmbH

has successfully met the prescribed requirements for training provider accreditation as established by intacs and is hereby authorised to provide the following training courses:

intacs™ Provisional Assessor
AUTOMOTIVE SPICE®

intacs™ Competent Assessor
AUTOMOTIVE SPICE®

Accreditation valid until: 31.12.2016

Conferred by the accreditation body on
January 2016

Heinz-Günter Plegnière
Managing Director

VDA QMC
Qualitäts Management Center
im Verband der Automobilindustrie

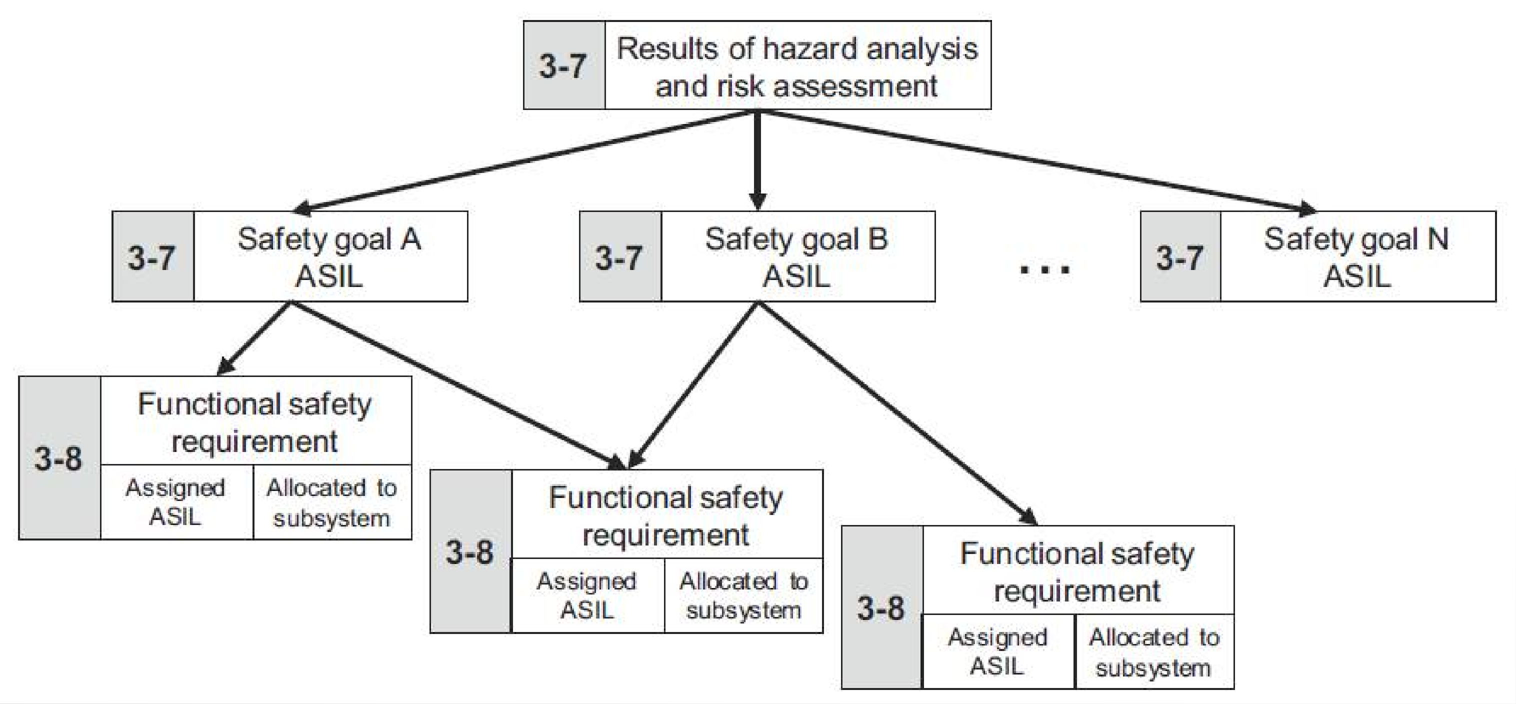
intacs.info
Accreditation No. intacs-4361-0731-70005-AS

Dr Richard Messnarz, ISCN GesmbH
Dr Christian Kreiner, TU Graz (Partner of ISCN in Safety Assessments)

EuroSPI 2017, TU Ostrava, 6.-8.9.2017

Safety Assessment - Traceability 1/2

1. **Statement about Traceability and Consistency of the Safety Case**
   - **Starting from Safety Goals**
   - **Selecting 3 complementary examples and tracing the functional, technical (system, software, hardware) safety requirements.**
   - **Checking consistency of content, decomposition e.g. ASIL D -> ASIL B(D), ASIL B(D)**
   - **Traceability to test**
   - **Reports generated to show 100% coverage of safety requirements on all levels**



Safety Assessment - Traceability 2/2

1. **Statement about Traceability and Consistency of the Safety Case**
   - **Starting from Safety Goals**
   - **Selecting 3 complementary examples and tracing the functional, technical (system, software, hardware) safety requirements.**
   - **Checking consistency of content, decomposition e.g. ASIL D -> ASIL B(D), ASIL B(D)**
   - **Traceability to test**
   - **Reports generated to show 100% coverage of safety requirements on all levels**

Each work product was assessed and the existence and coverage of requirements was rated N,P,L,F following the below described schema.

N (Not Adequate)	Deviation which cannot be corrected
P (Partially Adequate)	Deviation which can be corrected with significant effort
L (Largely Adequate)	Recommendation which can be corrected with little effort
F (Fully Adequate)	No deviation

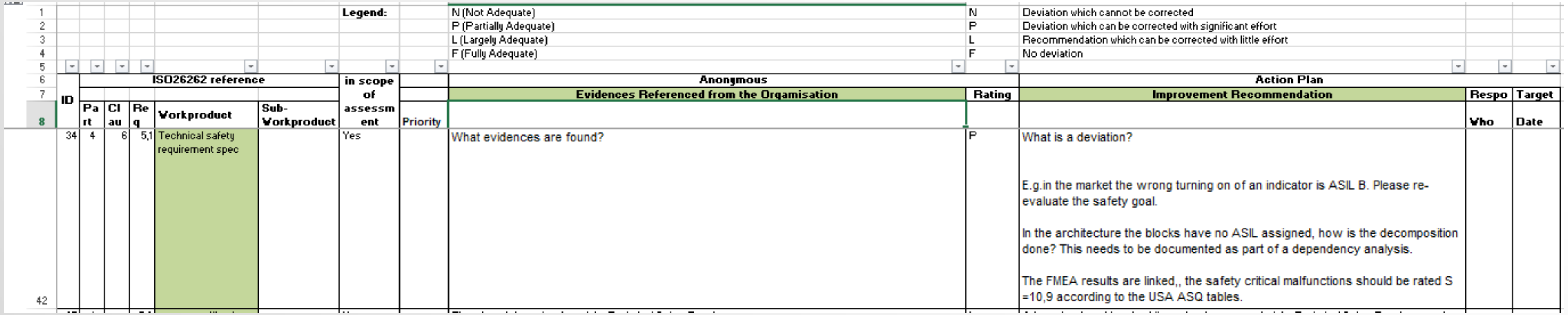
Coverage Statements:

The overall rating for traceability is L because reviews of the safety FMEA must be done to assure the coverage of linking to test cases and system test cases and to check whether missing links have an impact on the test cases.

Safety Assessment – Deviation Analysis 1/2

2. **Technical Check of**
   - Functional Safety Requirements covering the safety goals
   - Technical safety requirements implementing the functional safety requirements
   - HSI interfacing HW, SW.
   - System safety concept and architecture
   - SW Safety concept and architecture
   - HW Safety concept and architecture
   - FMEAs, FTAs, Diagnose Specifications

- **Each deviation is assigned to an ISO 26262 assessment sheet related to a clause / work product of the ISO 26262.**
- **Also the N/P/L/F rating analog ASPICE was used.**

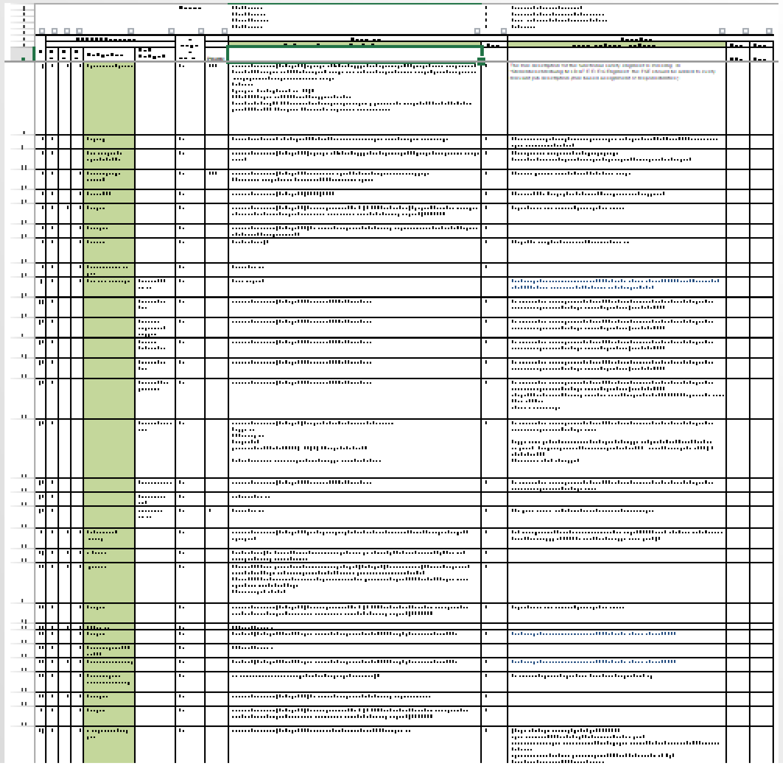


1							Legend:		N (Not Adequate)	N	Deviation which cannot be corrected		
2									P (Partially Adequate)	P	Deviation which can be corrected with significant effort		
3									L (Largely Adequate)	L	Recommendation which can be corrected with little effort		
4									F (Fully Adequate)	F	No deviation		
5													
6	ID	ISO26262 reference					in scope of assessment		Anonymous		Action Plan		
7									Evidences Referenced from the Organisation	Rating	Improvement Recommendation	Respo	Target
8		Part	Clau	Req	Vorkproduct	Sub-Vorkproduct		Priority				Vho	Date
42	34	4	6	5,1	Technical safety requirement spec		Yes		What evidences are found?	P	What is a deviation? E.g.in the market the wrong turning on of an indicator is ASIL B. Please re-evaluate the safety goal. In the architecture the blocks have no ASIL assigned, how is the decomposition done? This needs to be documented as part of a dependency analysis. The FMEA results are linked,, the safety critical malfunctions should be rated S =10,9 according to the USA ASQ tables.		

Safety Assessment – Deviation Analysis 2/2

2. **Technical Deviations Report**
   - **Detailed Report**

- **Each deviation is assigned to an element in the ISO 26262 assessment sheet and related to a clause / work product of the ISO 26262.**
- **Also the N/P/L/F rating analog ASPICE was used.**



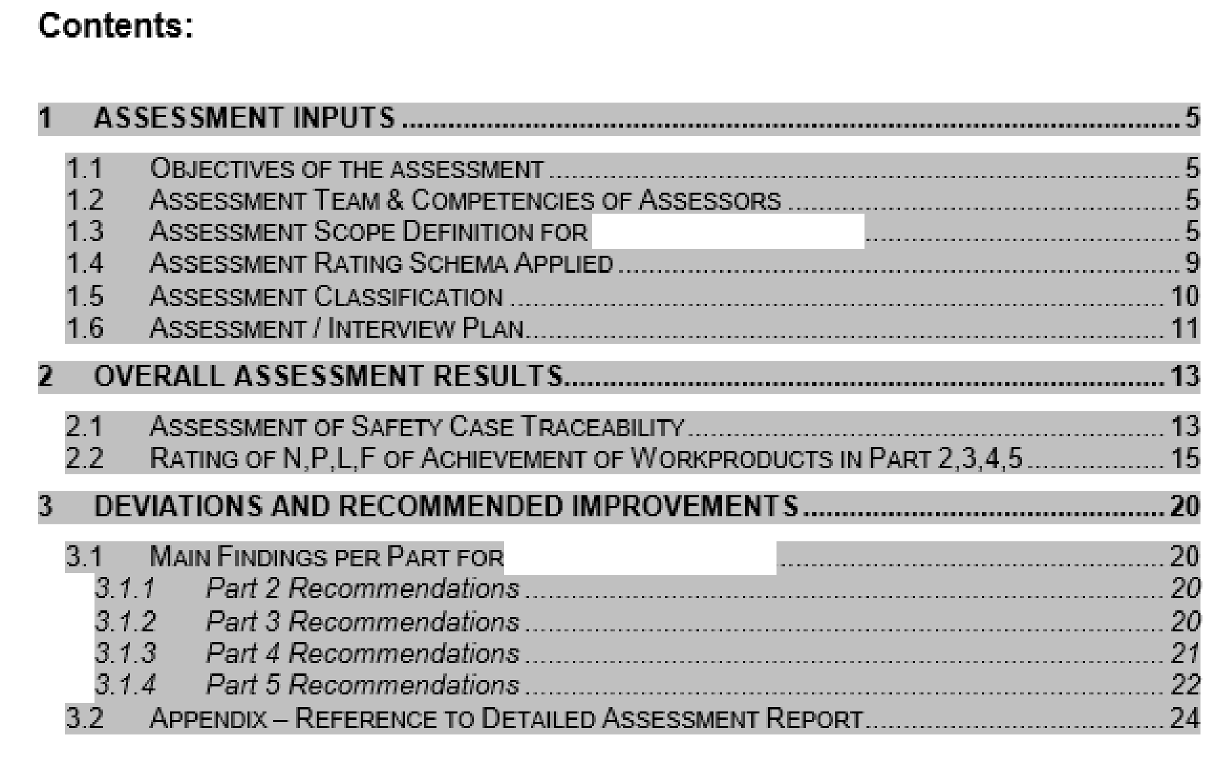
Note:
The report shown in this slide is unreadable and should only show how the structure looks like.

N .. No release
P .. Major Deviation
L .. Minor Deviation
F ... ok

Safety Assessment – Summary Report

2. Overview of Deviations by ISO 26262 Chapter

- Sorted by N, P, L, F
- An improvement plan is derived for the project



Contents:

Rating:

N .. No release
P .. Major Deviation
L .. Minor Deviation
F ... ok

Safety Assessment – Connection with ASPICE 1/3

Even if Safety Assessment is a Product Assessment it used a number of ASPICE best practices:

- **Each deviation is assigned to an element in the ISO 26262 assessment sheet and related to a clause / work product of the ISO 26262.**
- **Also the N/P/L/F rating analog ASPICE was used.**
- **ASPICE and Safety have been integrated in SOQRATES Working Group**
  - **For Safety Audits and not product based safety assessments**

Color codes:

Black – Automotive SPICE
Blue – Referenced ISO 26262 Attribute
Green

- if after blue text → Additional ISO 26262 questions,
- if after purple text → Additional SAE J3061 questions

Purple – SAE J3061 Relationship
Orange - IEC61508

Safety Assessment – Connection with ASPICE 2/3

- **ASPICE and Safety have been integrated in SOQRATES Working Group**
  - **For Safety Audits and not product based safety assessments**

SYS.2.BP1: Specify system requirements.

Use the stakeholder requirements and changes to the stakeholder requirements to identify the required functions and capabilities of the system. Specify functional and non-functional system requirements in a system requirements specification. [OUTCOME 1, 5, 7]

NOTE 1: Application parameter influencing functions and capabilities are part of the system requirements.

NOTE 2: For changes to the stakeholder's requirements SUP.10 applies

ISO 26262-4, ISO 26262-4, 6.4.1.1 The technical safety requirements shall be specified in accordance with the functional safety concept, the preliminary architectural assumptions of the item and the following system properties:

a) the external interfaces, such as communication and user interfaces, if applicable;
b) the constraints, e.g. environmental conditions or functional constraints; and
c) the system configuration requirements.

NOTE: The ability to reconfigure a system for alternative applications is a strategy to reuse existing systems.

ISO 26262-4, 6.4.1.3 If other functions or requirements are implemented by the system or its elements, in addition to those functions for which technical safety requirements are specified in accordance with 6.4.1 (Specification of the technical safety requirements), then these functions or requirements shall be specified or references made to their specification.
EXAMPLE: Other requirements are coming from Economic Commission for Europe (ECE) rules, Federal Motor Vehicle Safety Standard (FMVSS) or company platform strategies.

ISO 26262-4, 6.4.1.4 The technical safety requirements shall specify safety-related dependencies between systems or item elements and between the item and other systems.

- Are technical safety requirements in line with the functional safety requirements (Requirements, interfaces, constraints, …)?
- Are all technical safety requirements marked as safety requirements and referred to their source (ISO 26262, ECE, FMVSS, …)?
- Are semiformal notations used for ASIL C and D?

Safety Assessment – Connection with ASPICE 3/3

- **ASPICE and Safety have been integrated in SOQRATES Working Group**
  - **For Safety Audits and not product based safety assessments**

SYS.2.BP1: Specify system requirements.

Use the stakeholder requirements and changes to the stakeholder requirements to identify the required functions and capabilities of the system. Specify functional and non-functional system requirements in a system requirements specification. [OUTCOME 1, 5, 7]

NOTE 1: Application parameter influencing functions and capabilities are part of the system requirements.

NOTE 2: For changes to the stakeholder's requirements SUP.10 applies

ISO 26262-4, 6.4.2.3 For each safety mechanism that enables an item to achieve or maintain a safe state the following shall be specified:

a) the transition to the safe state;
NOTE 1: This includes the requirements to control the actuators.

b) the fault tolerant time interval;

c) the emergency operation interval, if the safe state cannot be reached immediately; and

d) the measures to maintain the safe state.

- Does the technical safety concept specify the necessary safety mechanism and control/monitoring systems to achieve all safety goals on time immediately or by warning/degradation concept, including correct prioritization and conflicting safety strategy?
- Are all relevant measures specified to detect all possible failures/failure combinations including all operation modes and interactions with other systems/items?

Safety Assessment & Audit

- **Safety Assessment (using some ASPICE Features)**
  - **Product based**
  - **Content and consistency check**
  - **High technical skills**
  - **Traceability + No Deviation in Work Products**
  - **Still we used N,P,L,F rating schema**

Each work product was assessed and the existence and coverage of requirements was rated N,P,L,F following the below described schema.

N (Not Adequate)	Deviation which cannot be corrected
P (Partially Adequate)	Deviation which can be corrected with significant effort
L (Largely Adequate)	Recommendation which can be corrected with little effort
F (Fully Adequate)	No deviation

- **Safety Audit with ASPICE+**
  - **Process based**
  - **Requirements and consistency check**
  - **Good assessor skills**
  - **Traceability + No Deviation in Processes (and Workproducts are checked not in same level of detail)**
  - **Using N,P,L,F rating schema for ASPICE processes**
  - **Using an extended safety checklist per base practice**

Questions

?

We make
your improvement work.