Integrated Automotive SPICE & Functional Safety Assessment Trials
EU Project SafEur Collaboration

Dr Richard Messnarz
Chair EuroSPI www.eurospi.net
Vice President European Certification and Qualification Association www.ecqa.org
Founding Member INTACS www.intacs.info
JRC Leader European Innovation Manager
Director ISCN www.iscn.com
Contents

- Integrated Model
- Integrated Assessment
- Experiences
- Next Steps
Company Profile

- ISCN Ltd Ireland (Coordination Office) founded 1994 in Ireland
  - Development offices in Austria
    - ISCN Regionalstelle founded 1997
    - I.S.C.N. GesmbH founded 2001
  - Further Consulting Offices in ISCN Group
    - SIBAC, Mittelbiberach (near Ulm), Germany
    - Performing Technologies, Vienna Austria
- EuroSPI Conference and Network Coordinator since 1994
- Vice President and Technology Provider for the European Certification and Qualification Association since 2005
- SPICE Assessments and Improvement Project since 1994
Company Profile

- Accredited iNTACS™ training provider for ISO/IEC 15504 and Automotive SPICE®
- Accredited VDA-QMC training provider and partner
- Moderator of the German SOQRATES initiative, where 23 leading Germany companies share knowledge concerning process improvement.
- EU Research Projects since 1995
Integrated Model 1

Customer Requirements
- e.g. Requirement:
  In case of system temperature > 120 degrees celsius the system must reduce the power by a degradation function

Hazard Analysis
- Identification and classification of safety risks and hazards.
- e.g. Safety Goal: no uncontrolled actuation
- Risk: uncontrolled actuation can happen with > 130 degrees Celsius

FMEA / FMEDA
- Analysis of hazards and safety risks and measures by FMEA and FMEDA
- e.g. Measure: redundant temperature control and definition of degradation mode characteristics or safe state

System Requirements Specification

System Requirements
- e.g. temperature control function, degradation characteristic function

Safety Requirements
- e.g. two temperature signals, plausi check, independent temperature control (Level 2 diagnosis)
Integrated Model 2

System Requirements Specification

System Requirements
- e.g. temperature control function, degradation characteristic function

Safety Requirements
- e.g. two temperature signals, plausi check, independent temperature control (Level 2 diagnosis)

System Architectural Design

System Architecture
- System components
- Interfaces
- Functions
- Mechanical Design
- General SW Application
- Architecture
- ECU Block Diagram
- Etc.

Safety Architecture
- e.g. plausi check in every 30 ms of the 2 temperature values, due to different position the tolerance is 5 degree Celsius deviation, if exceeded of 5 minutes, the safe state will be switched

Technical Safety Concept
Integrated Model 3

System Requirements Specification
- System Requirements
  - e.g. temperature control function, degradation characteristic function
- Safety Requirements
  - e.g. two temperature signals, plausi check, independent temperature control (Level 2 diagnosis)

System Architectural Design
- System Architecture
  - System components
    - Interfaces
    - Functions
    - Mechanical Design
    - General SW Application Architecture
    - ECU Block Diagram
    - Etc.
- Safety Architecture
  - e.g. plausi check in every 30 ms of the 2 temperature values, due to different position the tolerance is 5 degree Celsius deviation, if exceeded of 5 minutes, the safe state will be switched

HW Requirements
- Specification of HW
  - e.g. safety : temp. sensor 1 of type x on circuit board in position z; temp. sensor 2 of type x at amplifier module

Sensor Requirements
- Specification of sensors including the e.g. temperature sensors

HW – Software Interface Spec.
- Signal Specifications
  - e.g. safety : temp. signal 1 on pin 24, type = analogue, value range = 0.1 .. 2 V, temp rage = -40 to 130 °C resolution is 0,25 °C, update cycle of 10 ms

SW Requirements
- Specification of SW
  - e.g. Input Module: temp. sensor 1 is read from Pin 24 and using the Scaling : Temp in Celsius = [(Vout in mV) - 500] / 10 a degree celsius is calculated, and the var s_temp1 is updated in a cycle of 30 ms.

SW Safety Requirements
- Independent L2 Diagnosis Application to plausi check s_temp1 and s_temp2 variables in a cycle of 30 ms with a tolerance of 5°C, and if over a period of 5 minutes the difference sustains outside the tolerance the independent diagnosis switches to a safe state.
Integrated Model 4

Uncontrolled deceleration
NGS System
Fahrzeuge
Angewandte starke Verzögerung des Fahrzeugs

Too low gear actuated
NGS System
ZB Getriebe
NGS
Nutzlos niedriger Gang wird eingeleitet

Too low gear actuated
Diagnose Funktion
NGS System
Diagnosefunktionen
Zu niedriger Gang wird freigegeben

Wrong wheel speed
CAN-Signale Rahmenw
Init-Wert/Altwert Errorflag WhlRPM_RR-
Signal

Wrong rpm output shaft & Error Flag
NGS System
Sensor Signale Rahmenw
Falsches Internes_N3_drehzahlsignal mit
error flag

Wrong rpm output shaft & not plausible
NGS System
Sensor Signale Rahmenw
Falsches Internes_N3_drehzahlsignal
unplausible

Wrong rpm output shaft & plausible
NGS System
Sensor Signale Rahmenw
Falsches Internes_N3_drehzahlsignal
plausible

No rpm output shaft & over a sequence of cycles a constant
NGS System
Sensor Signale Rahmenw
Kein Internes_N3_drehzahlsignal

dauernhaft 0

Safety AK Presentation – Dr Richard Messnarz
Integrated Assessment

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Evidences</th>
<th>Export</th>
<th>Calculate</th>
<th>Learning</th>
<th>Settings</th>
<th>Help</th>
<th>Logout</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQ.3 Contract Agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.4 Supplier Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.11 Technical Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.12 Legal and Administrative</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.13 Project Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.14 Request for Proposals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACQ.15 Supplier Qualification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1 Requirements Elicitation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.2 System Requirements Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3 System Architectural Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.2 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.3 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.4 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.5 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.4 Software Requirements A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.5 Software Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.6 Software Construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.7 Software Integration Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.3.BP7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Identify the safety-relevant hardware and software parts. Treat all the hardware and software as safety-relevant where a safety-relevant system is intended to realise both safety and non-safety functions unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not affect the safety-related functions).

ISO 26262 Part: 6.6 Specification of software safety requirements
Chapter: 6.6.4.2
The specification of the software safety requirements shall be derived from the technical safety requirements and the system design (see ISO 26262-4-: 7.4.1 and ISO 26262-4-: 7.4.5) and shall consider the system and hardware configuration.
## Table ENG 3-1 Methods and measures for analysing system design

<table>
<thead>
<tr>
<th></th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

- Deductive analysis
- Inductive analysis

## Table ENG 3-2 Methods and measures for separating subsystems

<table>
<thead>
<tr>
<th></th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case 1 - Automatic gear system for high speed vehicles

- Needed 5 instead of 3 days
- Safety also requires to audit specific architectures, functions, and methods applied.
- The effort for reporting was the same as with Automotive SPICE, only the type of report was Excel
- The biggest problem was that the additional content displayed in the functional safety view in the assessment tool was very hard to interpret without very detailed understanding of the functional safety standards. A normal SPICE assessor with no safety background would be overwhelmed.
Case 2 - Automatic gear system for heavy trucks

The assessment based on an extended HIS scope needed **5 instead of 3 days**. The assessors needed to go very deep into the details because safety also requires to audit specific architectures, functions, and methods applied. The cooperation with the certifier **TÜV worked very well. They stated that about 90% of their checklist was covered** in these additional checks during the Automotive SPICE assessments. The report was done as a normal word based Automotive SPICE report and the **TÜV delivered their checklist in parallel**.
• Currently rework of assessment tool to provide more easy guidance to assessors
• Join the working party

• 28.-29.6. in Vienna, 18.9. in Graz
Acknowledgment

This presentation was developed within the international consortium “ECQA Certified Functional Safety Manager”:

- Graz University of Technology, Austria, www.tugraz.at
- International Software Consulting Network Ltd., Ireland, www.iscn.com
- Methodpark Software AG, Germany, www.methodpark.de
- Sibac GmbH, Germany, www.sibac.de
- Spinet Oy, Finland, www.spinet.fi

- The development was partly funded by the EU under:
  Leonardo da Vinci programme 518632-LLP-1-2011-1-AT-LEONARDO-LMP

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.