Experiences with ISO-26262 Tool Chain Classification from an IT-Perspective

2013-04-09
Agenda

- Brief presentation about PROMETO
- Our view on Tool Classification / Tool Qualification
- Practical example of “Confidence in the use of software tools”
- Summary
Agenda

- Brief presentation about PROMETO
- Our view on Tool Classification / Tool Qualification
- Practical example of “Confidence in the use of software tools”
- Summary
Introducing PROMETO
PROMETO signifies confidence

PROMETO is a customer-oriented, competent and dedicated solution provider

Who are our customers?
Primary manufacturer and engineering service providers for electronic systems, components and tools.

What does PROMETO offer?
Solutions - especially to optimise your procedures, infrastructure and technology.

What are the benefits for the customer?
Working together with PROMETO enables our customers to develop electrical systems faster and with less risk.
Unique Selling Points / Exposé

- We build bridges between the other departments and IT
- We build bridges between the different development disciplines
- We build bridges between development and management

Functional safety (extract from projects)
- Process construction within development; respectively supplier management
- White papers, webinars
- Reference platforms
- Training
- Events
- Development guidance
PROMETO and Fraunhofer – a strong team

PROMETO works in close contact with Fraunhofer IPT in Paderborn.

Together we arrange conferences und training for example:

- Introduction to tool qualification
- Functional safety for software developers
- Functional safety for hardware developers
- Functional safety for system engineers
- Safety manager qualification
Agenda

- Brief presentation about PROMETO
- Our view on Tool Classification / Tool Qualification
- Practical example of “Confidence in the use of software tools”
- Summary
Excel is one of the most commonly used tools. In the example shown the values should be subtracted from the initial value:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>initial value</td>
<td>0,9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0,1</td>
<td>subtracted from the initial value results in</td>
<td>0,8</td>
<td>0,8</td>
</tr>
<tr>
<td>4</td>
<td>0,2</td>
<td>deducted from the last value results in</td>
<td>0,6</td>
<td>0,6</td>
</tr>
<tr>
<td>5</td>
<td>0,1</td>
<td>deducted from the last value results in</td>
<td>0,5</td>
<td>0,5</td>
</tr>
<tr>
<td>6</td>
<td>0,1</td>
<td>deducted from the last value results in</td>
<td>0,4</td>
<td>0,4</td>
</tr>
<tr>
<td>7</td>
<td>0,2</td>
<td>deducted from the last value results in</td>
<td>0,2</td>
<td>0,2</td>
</tr>
<tr>
<td>8</td>
<td>0,1</td>
<td>deducted from the last value results in</td>
<td>0,1</td>
<td>0,1</td>
</tr>
<tr>
<td>9</td>
<td>0,1</td>
<td>deducted from the last value results in</td>
<td>1,11022E-16</td>
<td>0</td>
</tr>
</tbody>
</table>

The result calculated by Excel is mathematically correct, however it presumes the use of floating point arithmetic.
Classification / Qualification

Classification

Possibility that a tool can introduce or fail to detect errors
Confidence in prevention and detection measures
Classification of the tool into confidence levels

In context of development activities:
• tool functions
• their use cases
• possible failures

Qualification

TCL1
Qualification not required

TCL2
Qualification Method TCL2

TCL3
Qualification Method TCL3

Legend: TI = Tool Impact  TD = Tool Error Detection  TCL = Tool Confidence Level
Qualification methods

Depending on the derived **TCL** and the **ASIL** of the product under development an **appropriate combination** of the qualification methods has to be chosen.

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TRL 2</th>
<th>ASIL C + TRL 3</th>
<th>ASIL D + TRL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

+ recommended / ++ highly recommended
Depending on the derived TCL and the ASIL of the product under development an appropriate combination of the qualification methods has to be chosen.

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TCL 2</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a  Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>b  Evaluation of the tool development process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c  Validation of the software tool</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d  Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
</tr>
</tbody>
</table>

+ recommended / ++ highly recommended

- In the event of version changes not applicable
- Lack of historic data leads to mistrust
- With regards to ASIL C + TCL3 and ASIL D Project there is difficulty in providing the necessary evidence
Qualification methods
What are the decision criteria?

Depending on the derived TCL and the ASIL of the product under development an appropriate combination of the qualification methods has to be chosen.

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TCL 2</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

+ recommended / ++ highly recommended

- Assessor to be sent to every tool provider?
- With regards to ASIL C + TCL3 and ASIL D Project there is difficulty in providing the necessary evidence
Qualification methods
What are the decision criteria?

Depending on the derived TCL and the ASIL of the product under development an appropriate combination of the qualification methods has to be chosen.

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TCL 2</th>
<th>ASIL C + TCL 3</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

+ recommended / ++ highly recommended
Depending on the derived TCL and the ASIL of the product under development an appropriate combination of the qualification methods has to be chosen.

Qualification methods

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TCL 2</th>
<th>ASIL C + TCL 3</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

+ recommended / ++ highly recommended

- Suitable up to ASIL D, however
- High effort for the tool provider
- Limited availability of such tools
### Qualification methods

*Conclusion: no choice?*

<table>
<thead>
<tr>
<th>Qualification methods</th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C + TCL 2</th>
<th>ASIL C + TCL 3</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

It means a lot of effort, however it is the only solution that is always applicable!?
## Qualification methods

*Conclusion – our suggestion*

### Qualification methods

<table>
<thead>
<tr>
<th></th>
<th>ASIL A + TCL 2/3</th>
<th>ASIL B + TCL 2/3</th>
<th>ASIL C TCL 2</th>
<th>ASIL C TCL 3</th>
<th>ASIL D + TCL 2/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Increased confidence from use</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>b Evaluation of the tool development process</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>c Validation of the software tool</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>d Development in accordance with a safety standard</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

**Choice dependant on the product group and position in the supply chain**
Agenda

- Brief presentation about PROMETO
- Our view on Tool Classification / Tool Qualification
- Practical example of “Confidence in the use of software tools”
- Summary
Standards

- Standards reflect what the majority of experts should do.

- Standards are often lagging – this can be seen in day to day practice.

- In the case of tool qualification the authors admit to succumbing to the temptation of writing something that is not often found in daily practice.
Reliability of the hard drives

Stories stemmed from practice

- Unrecoverable Bit Error Rate
  - 1 error per $10^{16}$ read accesses (Professional)
  - 1 error per $10^{14}$ read accesses (Mainstream)

Converted: 1 read error per 13,5 TByte of read data

⇒ With today’s amounts of data, the occurrence of corrupt data is usual and to be expected.
⇒ ISO 26262 does not sufficiently reflect these kind of IT related constraints
Tool Qualification

Responsibilities (from our experience)

**Methods**

- Initiators for Tool Qualification

**Processes**

- Development: Set to neutral; however own tools are often installed

**Tools**

- IT:
  - Product safety according to ISO 26262 is not firmly adhered to in day to day business
  - Tool Qualification acts as a catalyst for tool consolidation
Small organisation

Electronics
< 50 developers

~ 50 different development tools

Classification: ~ 4 man days
Qualification: ~ 2 tools

Benefits:
- correcting the tool portfolios
- proof of compliance

Large organisation

Mechatronic
< 500 developers

~ 400 different development tools

Classification: ~ 6 man weeks
Qualification: ~ 8 tools

Benefits:
- correcting the tool portfolios
- reduction of handling costs through format loyalty
- proof of compliance
For all organisations the topic of stipulated standards is an alien one, which is a reflection of the lack of clarity concerning responsibilities.

All organisations use to some extent different tools for the same purpose - this tendency is even more apparent for larger organisations.

All organisations use the standardisation to remedy the “tool zoos” which are often a trigger for hefty economic discussions.

For most people concerned product safety is not identifiable, but they consider it a formal necessity.
Agenda

- Brief presentation about PROMETO
- Our view on Tool Classification / Tool Qualification
- Practical example of “Confidence in the use of software tools”
- Summary
Conclusion

- The topic of “Confidence in the use of software tools” makes basic commercial common sense.
- The authors who write the standards have not taken the industrial practice into account, but succumb to the temptation of creating something new.
- The result then appears deficient in many respects.
- The companies however, not only apply the standards but also need to consider the “tool zoos” which have grown over time.
»Since human beings themselves are not fully debugged yet, there will be bugs in your code no matter what you do.«

Chris Mason, Microsoft

Thank You!
Thank you Tool Qualification Symposium 2013, Munich

We look forward to prospering together with you!
Contact us

PROMETO GmbH
Elsener Str. 92-94
D-33102 Paderborn
GERMANY

Phone: +49 (0)5251 / 14851 60
Fax: +49 (0)5251 / 14851 61

info@prometo.de
www.prometo.de
Copyright notice

• Image used on the cover sheet and also in the slide footers: PROMETO GmbH

• Unless specified otherwise, all further images used within this presentation derive from Microsoft Office Online. PROMETO does not own the rights of use. The use of the media by a recipient should only be done by obtaining the necessary rights of usage separately. Details can be found in §18 under: http://explore.live.com/microsoft-service-agreement?mkt=de-de&CTT=114

• The copyright for the car-image used on the Fraunhofer slide is owned by 3ddock (Fotolia).