Functional Safety Certification from Automotive to Medical

Alastair Walker
EuroAsiaSPI 2016
Graz University of Technology
14.09- 16.09.16
Overview

• One weakness in the medical device standards at present is they tend to focus on items such as software in isolation
• Standards such as IEC 60601-1, ISO 14971 and IEC 62304, provide information that is not particularly coherent and for engineering teams there is no clear guidance on how to assess, mitigate and ultimately reduce risks in ME SYSTEMS and ME EQUIPMENT (small percentage of the various medical device types)
• Due to the wide variety of medical devices and the associated standards. The guidance on developing ME EQUIPMENT/ME SYSTEMS hardware and software lags behind some other industry sectors.

• **IEC 60601-1 Definitions**
• ME EQUIPMENT - electrical equipment having an APPLIED PART or transferring energy to or from the PATIENT or detecting such energy transfer to or from the PATIENT
• ESSENTIAL PERFORMANCE - performance of a clinical function, other than that related to BASIC SAFETY, where loss or degradation beyond the limits specified by the MANUFACTURER results in an unacceptable RISK
• Programmable Electrical Medical System (PEMS) - ME EQUIPMENT or an ME SYSTEM containing one or more PROGRAMMABLE ELECTRONIC SUBSYSTEMS (PESS)
• For the above, follow IEC 60601-1 Section 14
PEMS Architectural Requirements

• PEMS Architecture Specification IEC 60601-1 Section 14.8
• COMPONENTS WITH HIGH-INTEGRITY CHARACTERISTICS;
• fail-safe functions;
• redundancy;
• diversity;
• partitioning of functionality;
• defensive design, e.g. limits on potentially hazardous effects by restricting the available output power or by introducing means to limit the travel of actuators.
• allocation of RISK CONTROL measures to subsystems and components of the PEMS;
  NOTE Subsystems and components include sensors, actuators, PESS and interfaces.
• failure modes of components and their effects;
• common cause failures;
• systematic failures;
• test interval duration and diagnostic coverage;
• maintainability;
• protection from reasonably foreseeable misuse;
Risk Assessment

- Automotive – Hazard Analysis and Risk Assessment undertaken at the project outset
- Automotive – Safety analyses performed at system, hardware and software levels
- Medical – ISO 14971, throughout the project
- ISO 14971 Risk mitigation
  - Inherent good design
  - Risk control measures
  - Accompanying document
- ISO 14971 Approaches to estimating risk
  - Use of relevant historical data;
  - Prediction of probabilities using analytical or simulation techniques;
  - Use of experimental data;
  - Reliability estimates;
  - Production data;
  - Post-production information;
  - Use of expert judgment
- ISO 14971 Risk data
  - Quantitative preferred over qualitative
Architectural Decomposition

- ISO 26262 Decomposition (Prior to HW or SW definition)

- ME EQUIPEMENT Initial Classification

  System
  No Classification

  Hardware
  No Classification

  Software
  Class A to C
  Can lead to HW Risk Measures
The proposed risk assessment model in ISO 14971 is less rigorous than in ISO 26262 Hazard Analysis and Risk Assessment than in that controllability is not considered.

<table>
<thead>
<tr>
<th></th>
<th>Negligible</th>
<th>Minor</th>
<th>Serious</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td></td>
<td></td>
<td></td>
<td>R1</td>
<td>R2</td>
</tr>
<tr>
<td>Probable</td>
<td>R1</td>
<td>R2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td></td>
<td>R4</td>
<td></td>
<td>R5</td>
<td>R6</td>
</tr>
<tr>
<td>Remote</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td></td>
<td></td>
<td>R3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Classification

The proposal would be to classify the ME SYSTEM/ME EQUIPMENT based on it’s potential to cause HARM, at systems level. Like the software classification defined in IEC 62304 the ME SYSTEM/ME EQUIPMENT would be graded accordingly.

<table>
<thead>
<tr>
<th>ME SYSTEM Class</th>
<th>Classification</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>The ME SYSTEM/ME EQUIPMENT can contribute to a HAZARDOUS SITUATION and the resulting possible HARM is death or SERIOUS INJURY</td>
<td>At this point risk control measures are not assessed. These are considered during the ME SYSTEM/ME EQUIPMENT development process. The aim of this stage is to define the ME SYSTEM/ME EQUIPMENT classification</td>
</tr>
<tr>
<td>B</td>
<td>The ME SYSTEM/ME EQUIPMENT can contribute to a HAZARDOUS SITUATION and the resulting possible HARM is non-SERIOUS INJURY.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>The ME SYSTEM/ME EQUIPMENT cannot contribute to a HAZARDOUS SITUATION</td>
<td></td>
</tr>
</tbody>
</table>
W-Model for System Development

- ISO 26262 uses a W-model for item development
- IEC 62304 defines a software V-model, this could be extended to a W-model for ME EQUIPMENT/ME SYSTEM development
PEMS Relation to IEC 62304

Key:
Boxes represent typical development lifecycle activities
Solid Arrows indicate typical deliverables transferred into/out of activities
Dotted arrows indicate deliverables just to the Risk Management File

Outputs from problem resolution process
Inputs to problem resolution process
Hardware Considerations

• Hardware Classification

As with the system level, the hardware implementation of ME SYSTEM/ME EQUIPMENT should be classified Class A to Class C. This would then also correlate with the IEC 62304 software activities and provide the mechanism to decompose the hardware classification via software risk control mechanisms, which is complementary to the process already used for software in IEC 62304. Ultimately both processes would be defined and assessed at the system level.

• Hardware Metrics

For ME EQUIPMENT/ME SYSTEMS of Class B and C a sensible approach would be to evaluate all potential SINGLE FAULT CONDITIONS and taking the exercise further, latent faults to ensure they meet the requirements of the defined target figures in a similar fashion to that in ISO 26262

<table>
<thead>
<tr>
<th>ME EQUIPMENT/ME SYSTEM Class</th>
<th>Single Fault Metric</th>
<th>Latent Fault Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>≥97%</td>
<td>≥90%</td>
</tr>
<tr>
<td>B</td>
<td>≥80%</td>
<td>≥60%</td>
</tr>
<tr>
<td>A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
IEC 62304 already has a well defined V-model for the software lifecycle. However certain areas could be enhanced

• Software security – testing for cybersecurity weaknesses. Define techniques and methods to enable an effective implementation (Class A, B and C)
• Software tool qualification – assessment of the suitability of the tools for the specific project (Class C only)
• Systematic failures – use of static analysis tools for (Class B and Class C)
• Memory management and memory overflows (Class B and Class C)
Conclusions

- Relevant only to a small percentage of medical devices. Safety relevant or safety critical medical devices i.e. ME EQUIPMENT/ME SYSTEMs with ESSENTIAL PERFORMANCE
- Clearer guidelines on risk analysis for ME EQUIPMENT/ME SYSTEMs required e.g. ME EQUIPMENT Functional Safety standard
- Definition of ME EQUIPMENT/ME SYSTEMs classification at systems level, so the architecture can be defined implementing the necessary features both in HW and SW
- Use IEC 62304 classification definition at system and hardware levels
- Use of hardware metrics based on level of severity
- Improved guidelines on designing for diversity and redundancy, identifying diagnostic coverage and minimising common cause failures
- Enhancements in IEC 62304 to much current best practice