dHealth 2020 – Biomedical Informatics for Health and Care
G. Schreier et al. (Eds.)

doi:10.3233/SHTI200105

Improving Medical Risk Management Using Automotive Standards

Alastair WALKER[a,1]
[a] *Lorit Consultancy GmbH, Salzburg, Austria*

Abstract. This paper provides a strategy for assessing systems through pulling on some of the techniques introduced in the ISO 26262: 2018[1] automotive functional safety standard. This will help improve and simplify the risk assessment and development activities of safety relevant medical devices. The approach is systems focussed and relates to medical devices that would come under the remit of IEC 60601-1[2], hence are defined as ME EQUIPMENT or ME SYSTEMS (medical electrical equipment that transfers energy to or measuring energy from the patient). The approach described demonstrates the great advantage of cross-sectoral learning and the efficiencies that can be created from doing so.

Keywords. functional safety, ME SYSTEM, ME EQUIPMENT, risk analysis, HARM

1. Introduction

Medical device standards focus on items such as software in isolation – this is a weakness that can lead to significant issues. Often medical devices are systems supporting electronic hardware, mechanical components, software and firmware, hence a systems approach is required to generate the optimal design solution and minimise the risk of HARM.

Currently engineers are tasked with developing medical devices, that have the potential to kill a patient, without a comprehensive set of guidance documents. Learning from other industries can greatly assist in providing clarity. In this case, techniques used in the automotive industry can help improve risk assessment and functional safety in the medical device sector.

At present standards such as IEC 60601-1, ISO 14971[6] and IEC 62304, provide information that is not particularly coherent; providing no clear guidance on how to assess, mitigate and ultimately reduce risks in ME SYSTEMS and ME EQUIPMENT. Despite efforts to improve the situation, the guidance on developing ME EQUIPMENT/ME SYSTEMS hardware and software lags behind other sectors.

This paper introduces aspects of ISO 26262 into the development of ME EQUIPMENT/ME SYSTEMS to provide clearer guidelines for developing systems, hardware and software to meet the functional safety requirements. This strategy cannot address all products across the industry sector but is relevant to a group that is often more complex in design.

[1] Corresponding Author: Alastair Walker, Lorit Consultancy GmbH, E-Mail: alastair.walker@lorit-consultancy.com

2. Methods and Results

2.1. ME SYSTEM/ME EQUIPMENT Functional Safety Considerations – System Level

The proposal is to classify the ME SYSTEM/ME EQUIPMENT based on its potential to cause HARM, at systems level. Like the software classification defined in IEC 62304 the ME SYSTEM/ME EQUIPMENT would be graded accordingly. See Table 1.

Table 1. ME SYSTEM/ME EQUIPMENT Classification

ME SYSTEM Class	Classification	Comments
C	The ME SYSTEM/ME EQUIPMENT can contribute to a HAZARDOUS SITUATION and the resulting possible HARM is death or SERIOUS INJURY	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
B	The ME SYSTEM/ME EQUIPMENT can contribute to a HAZARDOUS SITUATION and the resulting possible HARM is non-SERIOUS INJURY.	
A	The ME SYSTEM/ME EQUIPMENT cannot contribute to a HAZARDOUS SITUATION	

At present ISO 14971 introduces different techniques to risk assess products but does not give specific guidance on these. As already defined in ISO 26262, the methods and techniques to develop, assess and verify the ME EQUIPMENT/ME SYSTEM implementation can be scaled against the classification of the product.

2.2. Adding a ME SYSTEM/ME EQUIPMENT Hazard Analysis and Risk Assessment to ISO 14971

The task of establishing the ME SYSTEM/ME EQUIPMENT level of risk could be modelled on ISO 26262-3 hazard analysis and risk assessment (HARA), where the Automotive Safety Integrity Level (ASIL) and safety goals are determined. Using a system FMEA approach, the potential risk of harm could be established for the ME SYSTEM/ME EQUIPMENT and the corresponding ME SYSTEM/ME EQUIPMENT safety class applied. ISO 14971 requires the assessment and management of risk as shown in Figure 1.

The first two stages, i.e. risk analysis and risk evaluation, should be applied initially in the form of a system FMEA to classify the ME SYSTEM/ME EQUIPMENT and then subsequently in design FMEAs. Used during the development process these two FMEA processes complement and feed into one another.

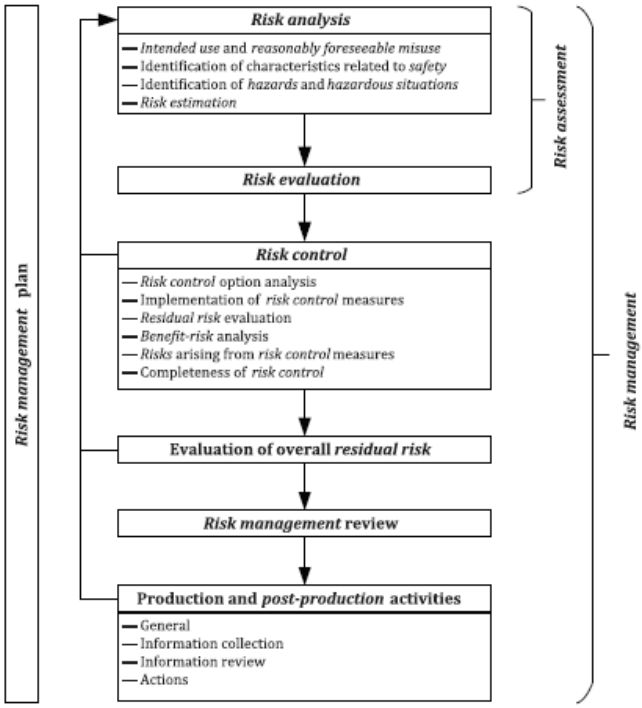

Figure 1. ISO 14971 Risk Management Process

2.3. Methods for Estimating Risk

ISO 14971 gives guidance on risk estimation based on a severity versus probability of HARM table (can be either qualitative or quantitative). Table 2 illustrates a typical table for acceptability where risks on the bottom left are acceptable, top right are not acceptable and area in between is to be risk reduced where possible to achieve acceptability. ISO 14971 goes further in suggesting the use of quantitative data if available, however there is no mandatory requirement to use quantitative evidence nor are any target metrics given on acceptability against potential risk of HARM.

Table 2. ISO 14971 Risk Assessment Process. Risks are (+) … acceptable, (o) … to be risk reduced where possible to achieve acceptability, (-) … not acceptable.

	Negligible	Minor	Serious	Critical	Catastrophic
Frequent	(+)	(o)	(-)	(-)	(-)
Probable	(+) R1	(o) R2	(o)	(-)	(-)
Occasional	(+)	(o) R4	(o)	(-) R5	(-) R6
Remote	(+)	(+)	(o)	(o)	(-)
Improbable	(+)	(+)	(+) R3	(o)	(o)

The model used for risk analysis and evaluation in ISO 26262 is superior to that in ISO 14971. The HARA process utilises a FMEA approach and at design level for all ASIL a FMEA process is highly recommended for system design analysis.

For ME SYSTEM/ME EQUIPMENT classification, the process in Table 2 may be deemed to be acceptable for Class A, but for Class B and Class C a three element FMEA should be used, so that the controllability can also be assessed and graded (see Table 3). Controllability as part of the initial risk assessment ensures that teams are focused on the potential ability to manage the risks of HARM in the ME EQUIPMENT/ME SYSTEM.

Table 3. Example FMEA with Controllability for ME EQUIPMENT/ME SYSTEM Risk Assessment.

Item	Severity	Occurrence	Controllability	Original RPN
Controller losses treadmill speed regulation	10	3	10	300
Mitigation	**Severity**	**Occurrence**	**Controllability**	**Modified RPN**
Monitor speed via a second device and slowly halt	10	3	2	60

2.4. ME SYSTEM/ME EQUIPMENT Decomposition

Safety class decomposition is addressed in two different areas of ME SYSTEM/ME EQUIPMENT development; IEC 60601-1 section 14.8 where the Programmable Electrical Medical System (PEMS) architecture is defined and IEC 62304 section 4.3. Both of these have failings due to the guidance, or lack of, on how or when this should be addressed. The technique defined in ISO 26262-9 section 5.4 to decompose ASILs down to lower ASIL ratings as indicated in Figure 2 is far more practical.

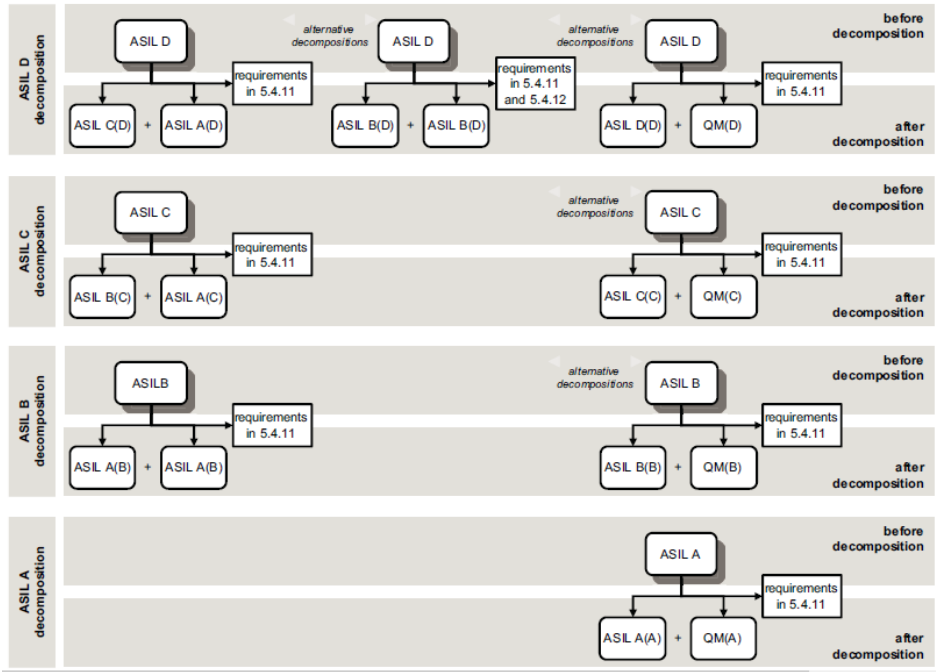

Figure 2. ISO 26262 ASIL Decomposition

In the case of ME EQUIPMENT/ME SYSTEMS the decomposition would be represented by a simpler mapping, as the aim here is to decompose a Class C down to Class B and Class B to Class A. Class A would be treated with a criticality similar to QM/ASIL A in ISO 26262.

As indicated in Figure 2 a key aspect of ISO 26262 decomposition is to show that there is sufficient independence between decomposed ASIL components. Equally for ME EQUIPMENT/ME SYSTEM decomposition, freedom from interference between elements would be an essential requirement.

2.5. ME SYSTEM/ME EQUIPMENT Development Lifecycle

The process for ME SYSTEM/ME EQUIPMENT development should follow the W-model used in ISO 26262 as indicated in Figure 3.

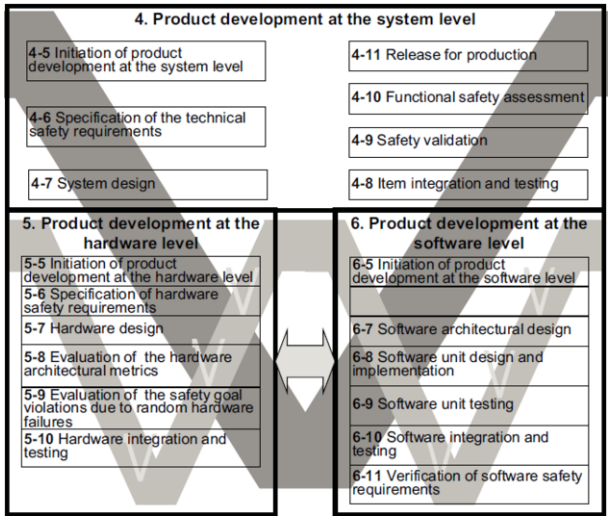

Figure 3. ISO 26262 W-Model for System Development

In this manner the hardware and software architectural requirements are traceable back to the system requirements and the decomposition decisions taken at system level then transpose themselves into the hardware and software architecture.

IEC 62304 already defines not only a software V-model, but illustrates how this related to PEMS development see Figure 4.

2.6. ME SYSTEM/ME EQUIPMENT Hardware Functional Safety Considerations

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.

As with the proposal at system level or the definition in IEC 62304 for software class, specific activities could be highly recommended based on the hardware classification.

2.7. Hardware Metrics

There are distinct advantages in the approach taken in ISO 26262 for quantitatively evaluating hardware reliability, that although introduced as a topic in ISO 14971 and IEC 60601-1 is not defined as a requirement nor are there guidelines on the acceptability criteria.

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, see Table 4. Using industry recognised guidance for component reliability e.g. international standards IEC TR 62380[8] or SN 29500[9], the failure rates for the safety relevant circuits can be calculated. The limits in Table 4 correspond to those for ASIL C and ASIL B in ISO 26262.

Table 4. Hardware Metric Target Values

ME EQUIPMENT/ME SYSTEM Class	Single Fault Metric	Latent Fault Metric
C	≥97%	≥90%
B	≥80%	≥60%
A	N/A	N/A

$$Single\ Fault\ Metric = 1 - \sum_{SR}(\lambda_{SF} + \lambda_{RF}) / \sum_{SR}(\lambda) \quad (1)$$

$$Latent\ Fault\ Metric = 1 - \sum_{SR}(\lambda_{LP}) / \sum_{SR}(\lambda - \lambda_{SF} - \lambda_{RF}) \quad (2)$$

with λ … failure in time rate (FIT) taken from the relevant industry source, SR … safety relevant, SF … Single Fault, LP … Latent Fault, RF … Residual Fault

As with ISO 26262 an assessment of the diagnostic coverage of the components and circuit would be required to assess the percentage of any FIT rate that is safety relevant.

ISO 26262 goes further than the suggestion in this paper, by calculating the metrics for residual risks e.g. probabilistic metric for random hardware failures (PMHF). This may be an over-complex step for ME EQUIPMENT/ME SYSTEMS however for a critical Class C device it could provide an excellent method for quantitatively assessing residual risk.

IEC 60601-1 permits the use of COMPONENTS WITH HIGH-INTEGRITY CHARACTERISTICS to achieve a SINGLE FAULT SAFE design. Knowing if a component is or is not suitable to meet these requirements is not easily identified from IEC 60601-1. Applying the Single Fault Metric of Table 4 to specific components, manufacturers would able to design and supply components with a Class B or Class C rating (assuming we chose to classify Class A as N/A), this would be akin to ISO 26262 ASIL rated components and reduce the level of work for ME SYSTEM/ME EQUIPMENT manufacturers during the component selection and development activities.

The exercise of calculating single fault and latent fault metrics would support the activities of component failure mode definition and diagnostic coverage, referenced in IEC 60601-1 section 14.8 when generating a PEMS architecture specification.

2.8. Software Functional Safety Considerations

IEC 62304 addresses items necessary for an effective software life-cycle model. The life-cycle model and how it relates to the PEMS activities is indicated in Figure 4.

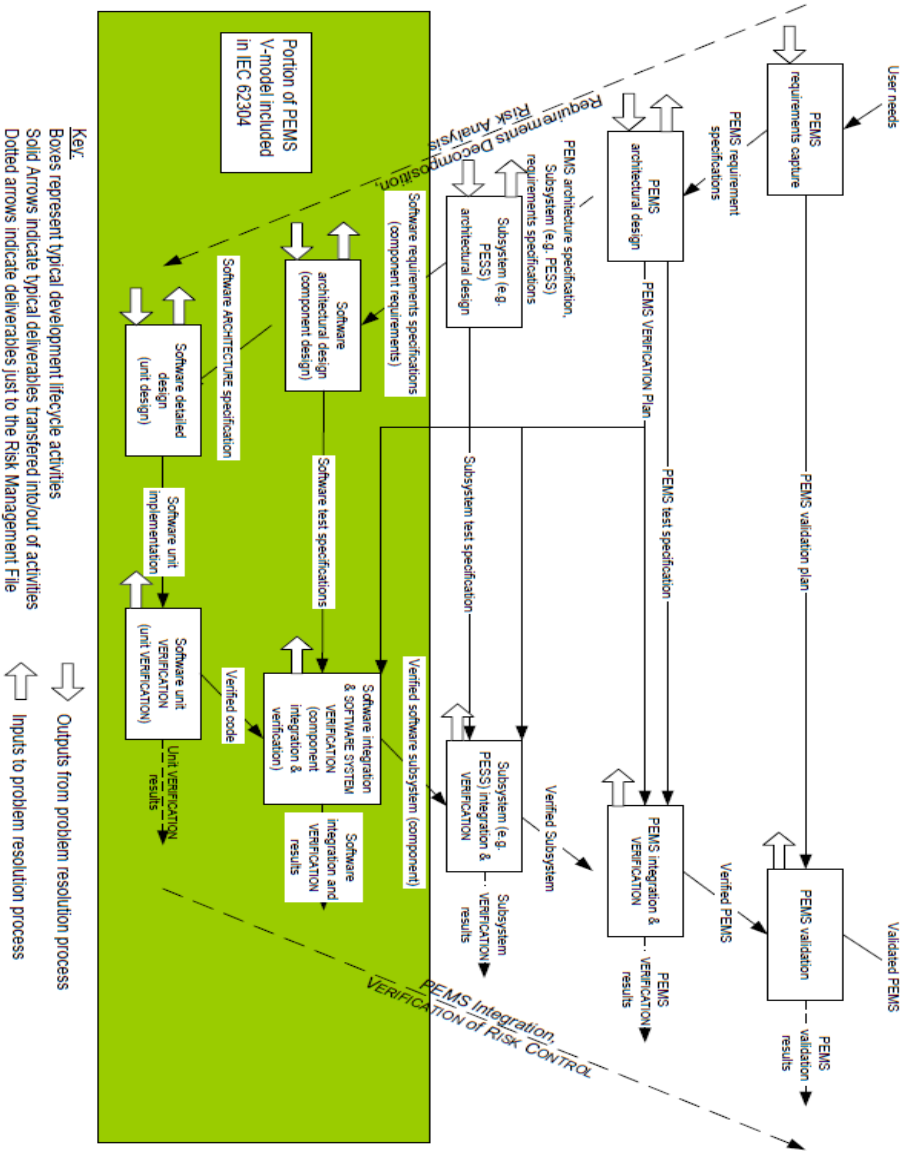

Figure 4. PEMS - IEC 62304 Software V-Model

There are areas of IEC 62304 at present (V1.1 released 2015) that still do not adequately cover aspects required in developing functionally safe software and ultimately ME SYSTEMS/ME EQUIPMENT:

- 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)

When implementing guidelines at system and hardware levels, enhancements should also be added for software. The US Food and Drug Administration have produced cybersecurity guidelines [7], and these could be used as reference source.

3. Conclusion

From the practical experiences of international standards in other industries, as described in this paper, there is plenty of scope and opportunity to enhance the guidance in the current key medical device standards IEC 60601-1, ISO 14971 and IEC 62304, based upon the processes defined in ISO 26262.

For functional safety professionals the necessary steps to fulfil the guidelines of ISO 14971 are relatively easily understood, but for an industry that does not really embrace the term functional safety and where many of the development and quality personnel have no or limited safety relevant design experience, clearer guidelines and a more systems orientated approach may help to improve the safety of products and reduce the confusion in developing products to the current standards.

References

[1] ISO 26262:2018 Road vehicles – Functional safety
[2] IEC 60601-1:2012 (Ed 3.1) Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
[3] IEC 62304:2015 (Ed 1.1) Medical device software – Software life cycle processes
[4] 2017/745 Regulation of the European Parliament on Medical Devices
[5] Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices May 11 2005
[6] EN ISO 14971:2019 Medical devices – Application of risk management to medical devices
[7] Postmarket Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff – Draft Guidance January 22, 2016
[8] IEC TR 62380 Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment
[9] Siemens SN29500 Component Failure Rate data (parts 1 to 14)