Functional Safety Certification from Automotive to Medical

Abstract

The medical device sector has many international standards and guidance documents; it is also a very wide ranging product sector. This paper aims to suggest a strategy for assessing systems including either or both electronic hardware and software, that utilises some of the techniques introduced in the ISO 26262: 2011[1] automotive functional safety standard. The reason for suggesting this approach is to recommend processes that will help improve and simplify the risk assessment and development activities of safety relevant medical devices.

The approach here is very much systems focussed on and relates to medical devices that would come under the remit of IEC 60601-1[2] and hence are defined as ME EQUIPMENT or ME SYSTEMS (devices transferring energy to or measuring energy from the patient). Here there are strong parallels with the functional safety strategy used in the automotive sector.

Not all products are deemed to be ME EQUIPMENT or ME SYSTEMS nor is IEC 60601-1 relevant for all medical devices, others may be e.g. in-vitro or implantable devices. Not all software that falls under the remit of the software life-cycle standard IEC 62304[3 is relevant to IEC 60601-1 e.g. standalone software can be a medical device. [4], [5]

Keywords

Functional safety, ME SYSTEM, ME EQUIPMENT, risk analysis, HARM.

Introduction

One weakness in the medical device standards at present is they tend to focus on items such as software in isolation. Ultimately many medical devices are systems supporting electronic hardware, mechanical components, software and firmware, hence a systems approach is required, both to generate the optimal design solution and minimise the risk of HARM[6]. Note all text in capitals represent the terms utilised in the relevant standard.

Many engineering teams are tasked with developing medical devices that could in the worst case scenario kill a patient[7], with at present not the most comprehensive set of guidance documents. Providing detailed guidance on how to assess and mitigate risks in ME SYSTEMS/ME EQUIPMENT enables development teams to implement lower risk solutions. Tapping into the information sources in other industries can greatly assist in improving the processes in a given sector. In this case many 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[8] 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. Examples include architectural definitions for diversity, redundancy and common cause failures listed in IEC 60601-1, or how teams relate the requirements of section 14 in IEC 60601-1 to the guidance in IEC 62304. The decomposition of software class in IEC 62304 is assessed at a software rather that at an architectural level

Medical device standards are constantly improving and updates to ISO 14971 and IEC 60601-1 in particular have helped to clarify the processes required, however 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.

This paper aims to introduce certain aspects of ISO 26262 into the development of ME EQUIPMENT/ME SYSTEMS and hence provide clearer guidelines for developing systems, hardware and software to meet the functional safety requirements placed upon them.

The main limitation in this strategy is that it cannot address all products across the industry sector, but is relevant to a group that tend to be more complex in design.

ME SYSTEM/ME EQUIPMENT Functional Safety Considerations – System Level

The proposal would be 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 Figure 1.

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	

Figure 1 ME SYSTEM/ME EQUIPMENT Classification

At present ISO 14971 introduces different types of technique to risk assess products (predominantly in appendices), but does not give specific guidance or guidelines on when or how to use them.

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. e.g. for Class C deductive analysis, using a fault tree analysis could be strongly recommended.

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 need not be dissimilar to the exercise in 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 Class applied. ISO 14971 requires the assessment and management of risk[8] as shown in Figure 2, the process of following this flowchart is not defined in as much detail as necessary for safety relevant ME SYSTEM/ME EQUIPMENT development

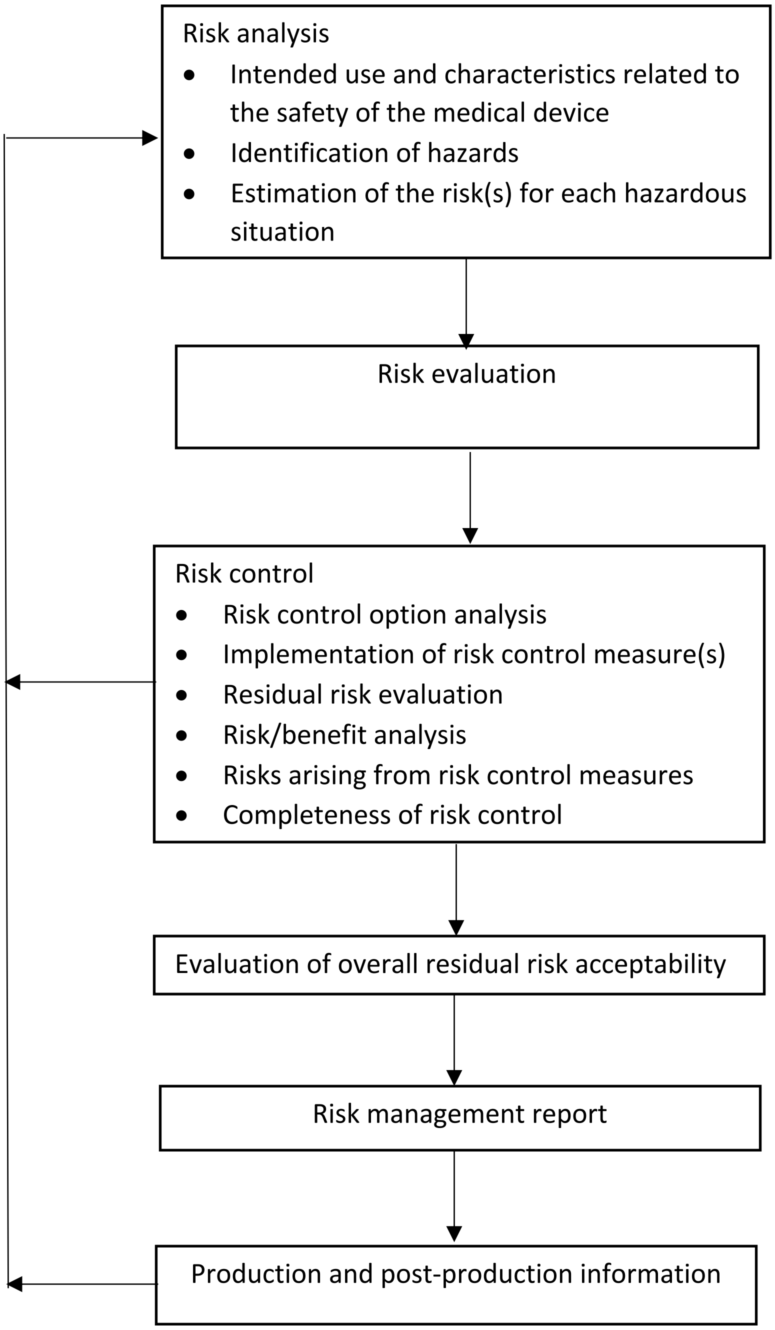
Risk analysis
• Intended use and characteristics related to the safety of the medical device
• Identification of hazards
• Estimation of the risk(s) for each hazardous situation
Risk evaluation
Risk control
• Risk control option analysis
• Implementation of risk control measure(s)
• Residual risk evaluation
• Risk/benefit analysis
• Risks arising from risk control measures
• Completeness of risk control
Evaluation of overall residual risk acceptability
Risk management report
Production and post-production information

Figure 2 ISO 14971 Risk Management Process

The first two stages 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 shall complement one another. Findings from a design FMEA feeding back to the system FMEA and vice-versa.

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). Figure 3 illustrates a typical table for acceptability where risks on the bottom left are acceptable, top right are unacceptable, requiring significant change and area in between can be more easily risk reduced 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.

	Negligible	Minor	Serious	Critical	Catastrophic
Frequent	🟩		🟥	🟥	🟥
Probable	🟩 R1	R2		🟥	🟥
Occasional	🟩	R4		🟥 R5	🟥 R6
Remote	🟩	🟩			🟥
Improbable	🟩	🟩	🟩 R3		

Figure 3 ISO 14971 Risk Assessment Process

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

For ME SYSTEM/ME EQUIPMENT classification, the process in Figure 3 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 Figure 4). In the example in Figure 4 the team assessing the risks are also assessing the quality of the mitigation i.e. in this case a second device to monitor the treadmill speed. Controllability as part of the initial risk assessment ensures that teams are focussed on the potential ability to manage the risks of HARM in the ME EQUIPMENT/ME SYSTEM

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

Where Severity, Occurrence and Controllability range from 1 to 10. The highest Severity and Occurrence rates are 10 but the lowest Controllability is rated with 10. The RPN is calculated by multiplying Severity x Occurrence x Controllability

Figure 4 Example FMEA with Controllability for ME EQUIPMENT/ME SYSTEM Risk Assessment

Figure 4 gives an example of an FMEA for an ECG stress test system controlling a treadmill. The initial estimation of the risk priority number (RPN) is then based on all three factors – severity, occurrence and controllability. At a system level the mitigation can be defined, if not at this stage in detail, for the implementation. The evaluation and analysis of the mitigation can then be assessed using e.g. design FMEAs during the development process.

The rating of Controllability should be derived from quantitative rather than qualitative data.

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. In that section of IEC 60601-1 topics such as diversity, redundancy, partitioning of functionality and common cause failures are introduced, but little is defined in terms of how these topics could be tackled or when they should be addressed. The second area where decomposition is referenced in IEC 62304 section 4.3, where the software class can be reduced by one of three methods (hardware, independent SOFTWARE SYSTEM and healthcare procedures). The reduction of the software class through decomposition reduces the safety requirements and development effort of the decomposed software component The decomposition through hardware or an independent SOFTWARE SYSTEM would involve introducing a redundant element that ensures the ME SYSTEM/ME EQUIPMENT remains in a safe state if the decomposed software component failed due to e.g. a systematic fault. The use of healthcare procedures could be additional guidance in the accompanying documentation. This however is at a stage where the architecture will often be either fixed or restricted in terms of change.

The technique defined in ISO 26262-9 section 5.4 to decompose ASIL C down to lower ASIL ratings is indicated in Figure 5.

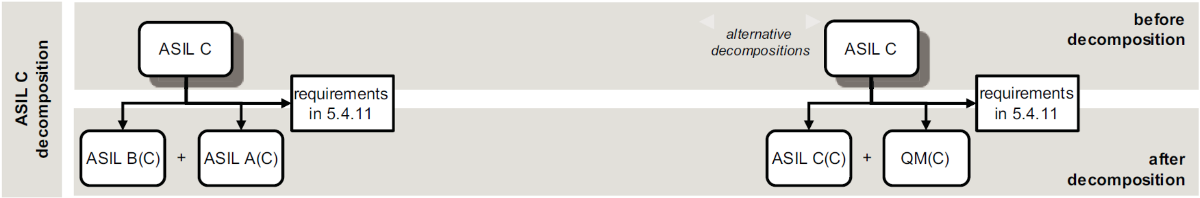

Figure 5 ISO 26262 ASIL C Decomposition

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 (refer to Figure 1). Class A would be treated with a criticality similar to QM/ASIL A in ISO 26262.

As indicated in Figure 5 a key aspect of ISO 26262 decomposition is to show that there is sufficient independence between decomposed ASIL components e.g. the reference to requirements in 5.4.11 in Figure 5. In ISO 26262 sufficient independence is demonstrated, through an analysis of dependent failures, which aims to identify single events or single that could bypass or invalidate the required independence e.g. partitions of functions or software elements. Equally for ME EQUIPMENT/ME SYSTEM decomposition, freedom from interference between elements would be an essential requirement.

Note IEC 60601-1 Annex H uses the term decomposition to describe V-model activities at component level, this should not be confused with the ISO 26262 definition or the definition in this paper.

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 6. This introduces both a V-model for the hardware and software development processes (refer to Figure 8 for software). Both V-models are then derived from the system level requirements. Figure 6 illustrates the relationship between the system level requirements and the hardware and software requirements documents. In ME SYSTEM/ME EQUIPMENT development there is a V model for software see Figure 8, however this is not mirrored in hardware development.

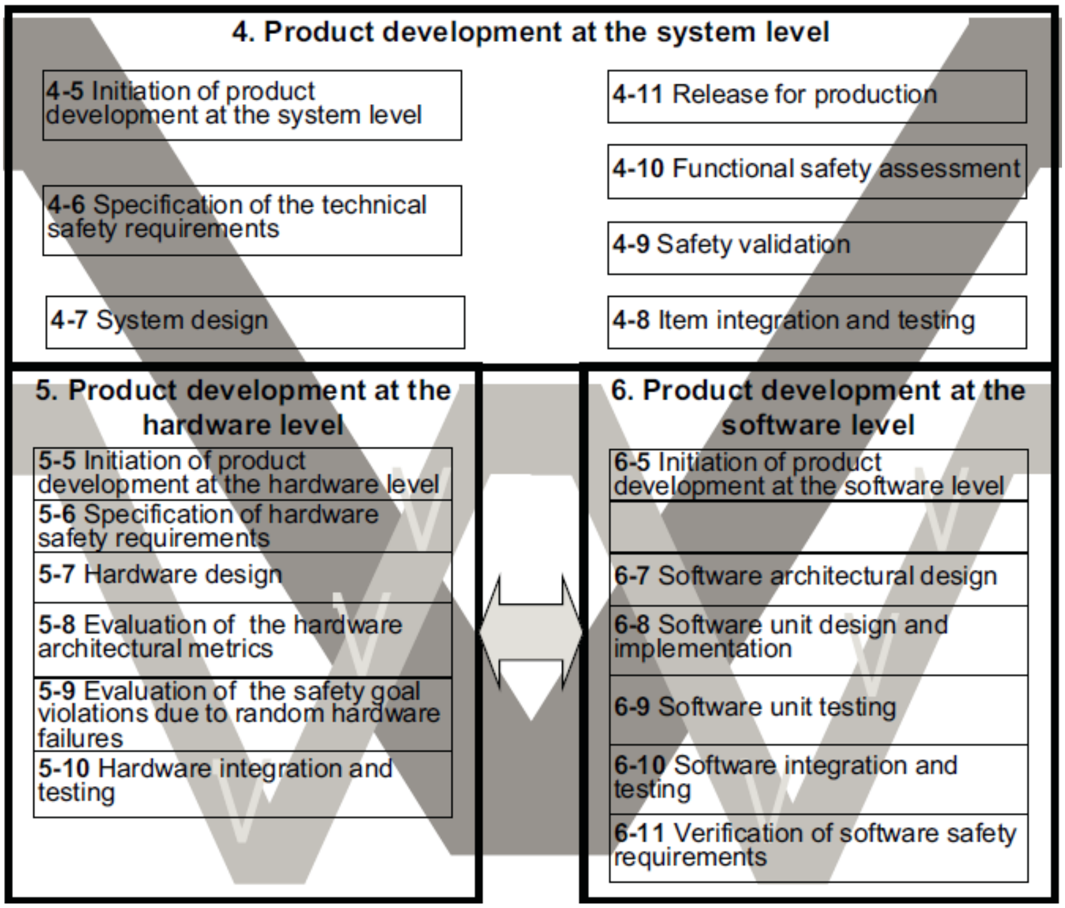
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements

Figure 6 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 8.

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. Ultimatelythe hardware and software 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 e.g. simulation of all Class B and Class C safety related hardware.

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 e.g. a permissible random hardware failure rate[10]

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 Figure 7. Using industry recognised guidance for component reliability e.g. international standards IEC TR 62380[11] or SN 29500[12], the failure rates for the safety relevant circuits can be calculated. The limits in Figure 7 correspond to those for ASIL C and ASIL B in ISO 26262.

In ISO 14971 and IEC 60601-1 there is currently no guidance on hardware metrics thus leaving the assessment of hardware suitability very open. ISO 14971 does suggest the prediction or probabilities in estimating probabilities, but there are no defined quantitative goals.

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

Figure 7 Hardware Metric Target Values

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

Latent Fault Metric = $1 - \Sigma_{SR}\,\lambda_{LP} / \Sigma_{SR}\,(\lambda - \lambda_{SF} - \lambda_{RF})$

Where λ represents the failure in time rate (FIT) taken from the relevant industry source

SR – safety relevant, SF – Single Fault, LP – Latent Fault and 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 Figure 7 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.

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 8.

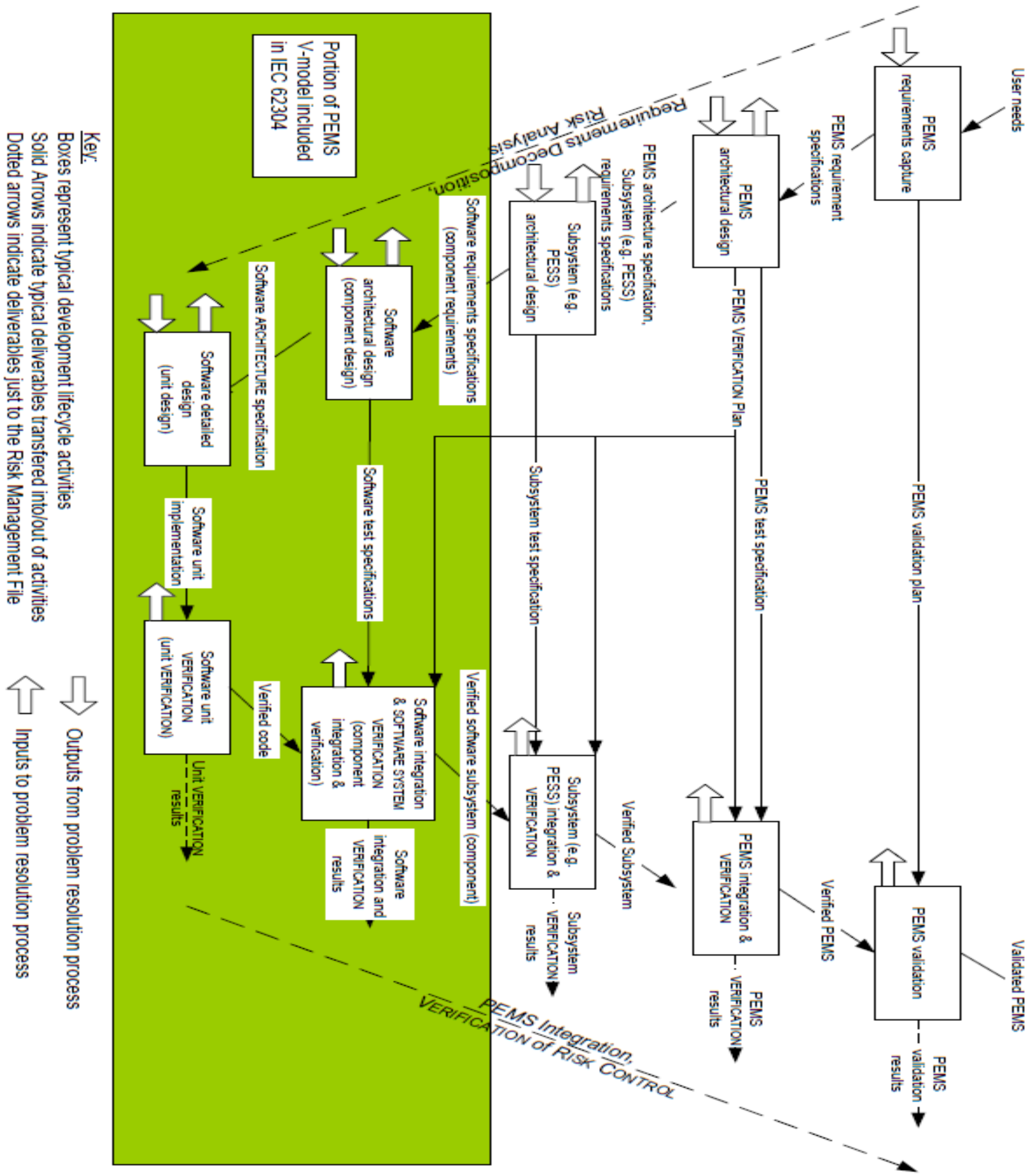
User needs
PEMS requirements capture
PEMS requirement specifications
PEMS architectural design
PEMS architecture specification, Subsystem (e.g. PESS) requirements specifications
Subsystem (e.g. PESS) architectural design
Requirements Decomposition, Risk Analysis
Software requirements specifications (component requirements)
Software architectural design (component design)
Software ARCHITECTURE specification
Software detailed design (unit design)
Software unit implementation
Software unit VERIFICATION (unit VERIFICATION)
Unit VERIFICATION results
Verified code
Software test specifications
Software integration & SOFTWARE SYSTEM VERIFICATION (component integration & verification)
Software integration and VERIFICATION results
Verified software subsystem (component)
Subsystem test specification
Subsystem (e.g. PESS) integration & VERIFICATION
Subsystem VERIFICATION results
Verified Subsystem
PEMS VERIFICATION Plan
PEMS test specification
PEMS integration & VERIFICATION
PEMS VERIFICATION results
Verified PEMS
PEMS validation plan
PEMS validation
PEMS validation results
Validated PEMS
PEMS Integration, VERIFICATION of RISK CONTROL
Portion of PEMS V-model included in IEC 62304
Key:
Boxes represent typical development lifecycle activities
Solid Arrows indicate typical deliverables transfered into/out of activities
Dotted arrows indicate deliverables just to the Risk Management File
Outputs from problem resolution process
Inputs to problem resolution process

Figure 8 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 is currently working on cybersecurity guidelines [7], and these could be used as reference source.

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.

Not all aspects of ISO 26262 are flawless, the interpretation of the hardware metrics leads to confusion in industry and the coverage of cybersecurity risks is currently fairly minimal, however by comparing techniques and methods from other industries such as automotive a

Future Work

Lorit Consultancy in cooperation with partner organisations, is currently preparing training material based on the concepts in this paper. Once available this could be used as a guideline for medical device manufacturers producing ME EQUIPMENT and ME SYSTEMS.

References

[1] – ISO 26262:2011 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] – 2007/47/EC Directive of the European Parliament and of the Council of 5 September 2007

[5] – Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices May 11 2005

[6] - EN ISO 14971:2012 Medical devices – Application of risk management to medical devices

[7] – Robotic surgery linked to 144 deaths in the US - http://www.bbc.co.uk/news/technology-33609495

[8] – Reliability Analysis of Maintenance Data for Medical Devices – Sharareh Taghipour, Dragan Banjevic Andrew K.S. Jardine University of Toronto

[9] – Postmarket Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff – Draft Guidance January 22, 2016

[10] – Meeting international standards for medical device reliability and risk management – PTC.com

[11] – IEC TR 62380 Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment

[12] – Siemens SN29500 Component Failure Rate data (parts 1 to 14)