24th Annual INCOSE International Symposium (IS2015)
Las Vegas, NV, June 30 – July 3, 2015

SysML Activity Models for Applying ISO 14971 Medical Device Risk and Safety Management Across the System Lifecycle

Robert J. Malins
Eagle Summit Technology Associates, Inc.
rjmalins@eaglesummittech.com

Jack Stein
Dynamic Solutions Institute, Inc.
jack.stein@me.com

Ajay Thukral
Cientive Group, Inc.
ajay.thukral@cientivegroup.com

Christophe Waterplas
ResMed Ltd.
Christophe.Waterplas@resmed.com.au

Copyright © 2013 by Robert J. Malins. Published and used by INCOSE with permission.

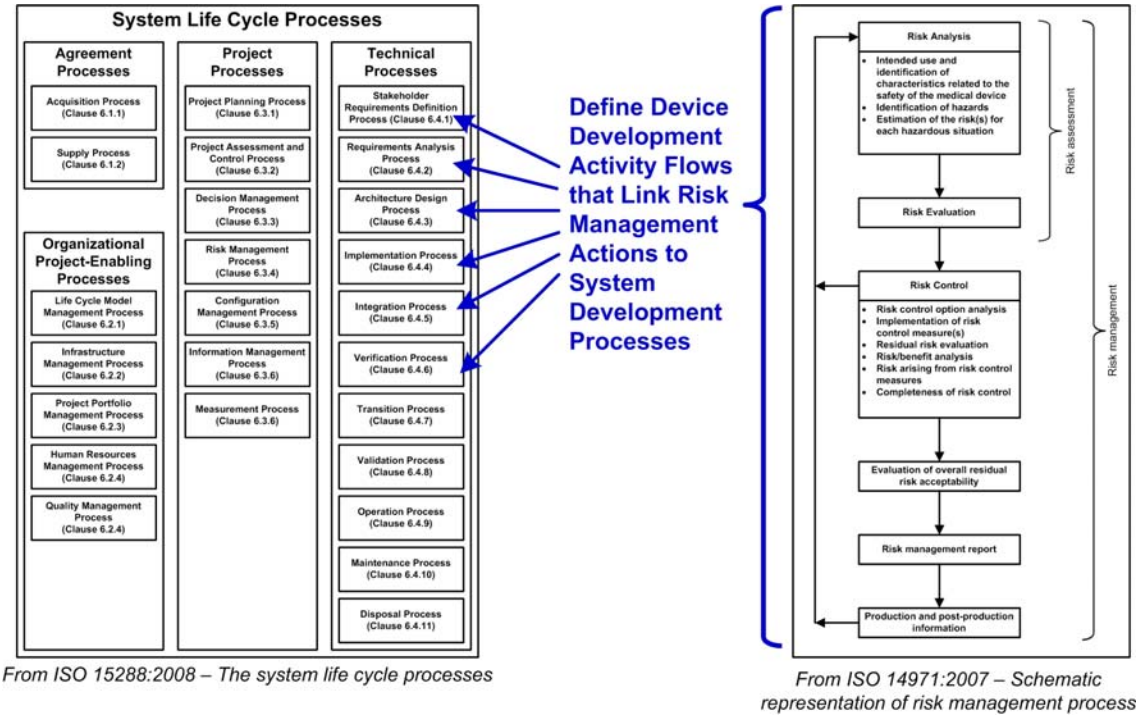
Abstract. The INCOSE Biomedical-Healthcare Model-Based Systems Engineering (MBSE) Challenge Team has been exploring applications of MBSE techniques to medical device development. Because patient and user safety is paramount in medical devices, the team has focused on using MBSE techniques to address safety topics. This paper uses MBSE methods to address the processes of analyzing safety and incorporating risk control at each step of the development portion of the system life cycle in order to achieve "built in" safety. SysML activity models are presented that link the steps of ISO 14971 to the system development technical processes of ISO 15288. In addition, the models show how the analysis results of ISO 14971 can be used to develop a system safety assurance case. The activity models explicitly show the iterative and recursive approach to applying risk management at each stage of system development and address the ISO 13485 requirement for process integration.

Introduction

The most important outcome of medical device risk management is patient and user safety. However, with the advent of medical device interoperability, technological advancement, and globalization, the medical device industry is increasingly challenged to characterize medical devices in a system context considering numerous use cases spanning the full spectrum of application characteristics. Since 2000, ISO 14971 Medical Device Risk and Safety Management has been the recognized

standard for medical device risk management. While ISO 14971 is elegant in its comprehensiveness, precision, and simplicity, its integration with the development process is an exercise left to individual device manufacturers. This has contributed to significant variation in safety outcomes which has, at least in part, led the FDA to issue a draft guidance requiring safety assurance cases for 510(k) submissions for infusion pumps. Many in the industry expect that safety assurance cases will be soon be mandated for many types of devices.

The present work, completed by members of the INCOSE Biomedical-Healthcare Model-Based Systems Engineering (MBSE) Challenge Team, describes a process for applying ISO 14971 across the system lifecycle stages defined in ISO 15288 System and Software Engineering – System Life Cycle Processes. The integration of the two standards incorporates risk analysis directly into the requirements development and design development processes in order to "build in" safety from the beginning. The integrated process recursively generates a safety assurance case using ISO 14971 outcomes from each ISO 15288 lifecycle stage. As illustrated in Figure 1, this work addresses the first six ISO 15288 Technical Processes (TPs), corresponding to the system development portion of the life cycle. The MBSE Challenge Team hopes to address the remaining five processes – corresponding to system deployment, operations/sustainment, and retirement/disposal – in future efforts.



From ISO 15288:2008 – The system life cycle processes

From ISO 14971:2007 – Schematic representation of risk management process

Figure 1. Linking of ISO 14971 Risk Management Steps to System Development Technical Processes in ISO 15288

Background

This paper continues work by previous authors that has shown that risk management in medical device development must begin at the very inception of the device development process (Herring 2007, Jensen 2013, Feng 2013). Previous authors have

shown clearly that achieving effective risk mitigation and control requires that risk definition and hazard analysis begin prior to starting design development. In this way, the control of risk and prevention of safety hazards is incorporated directly in the requirements definition process. Since risk and hazard issues are included in the requirements, risk mitigation and control are addressed at every step of the design, resulting in "built in" safety.

The unique aspect of this work is the use of systems engineering tools for formal integration of risk management actions into each system development technical process. This work uses the Technical Processes of ISO 15288 as the definition of the steps in system development and uses ISO 14971 to define the steps in risk management in order to address the specific requirements for medical device safety. The two processes are linked by means of SysML activity models in order to synchronize the steps for maximum benefit.

This work also continues previous work for linking safety case development to the MBSE process. Safety cases, and assurance cases in general, have been shown to be an effective method for evaluating the outcomes of risk management programs (Bishop 1998, Hawkins 2011). The nature of safety cases, as a hierarchical decomposition of top-level system characteristics supported by verification measurements, creates a structure of safety evidence that can be aligned with the requirements taxonomy, system functional taxonomy, and other hierarchical structures in MBSE (Feng 2012, Mhenni 2013, Ayoub 2012). A range of case studies have been published showing the integration of generalized assurance cases into MBSE (Cressent 2011) and the integration of safety cases into MBSE development for medical devices (Jee 2010).

The referenced work addressed incorporation of safety case elements into the MBSE model of the system. This work uses MBSE tools to link safety case development to the steps in the risk management process. The activity models developed for this paper show how hazard and risk control analyses of 14971 directly feed the safety case development resulting in concurrent risk management and safety case development. In addition, the activity models demonstrate how the design verification work defined in 15288 directly supports safety case evidence requirements. The intent in developing this integrated process is to provide a reference point for all organizations to use in defining what works for them.

Technical Approach

Our approach to integrating ISO 14971 and ISO 15288 actions consisted of two steps. The first step comprised a simple textual alignment between the two standards. This "alignment" consisted of matching specific paragraphs in ISO 14971 with specific activities defined in the ISO 15288 Technical Process descriptions. Once this alignment was achieved, the resulting table of actions was reviewed from the perspective of creating a safety case. A general safety case structure of three hierarchical levels of claims-arguments-subclaims/evidence was assumed. The synchronized development-risk management process was then reviewed to determine the points in the process when the proper information was generated to define each level of the safety case. The result was a concurrent process wherein the safety case

influences the design to improve safety and leverages risk management analysis outcomes to reduce duplication of work.

The second step in our process was to construct an activity model for each ISO 15288 Technical Process such that the requirements of ISO 15288 and ISO 14971 were satisfied and the requisite information for each level of the safety case was produced. Each ISO 15288 Technical Process was treated as a use case as shown in Figure 2. As shown in the figure, four actors were used in the SysML model: the stakeholder, the systems engineer, the specialty engineer, and the design engineer. For the purposes of addressing risk management, the primary emphasis in the modeling was on the actions of the systems engineer, the specialty engineer, and the stakeholders. Figure 2 shows that each of these actors represents a class of actors whose perspective and program role must be considered. The activity modeling defined actions for all four actors and explicitly considered the four systems engineering roles shown in the figure.

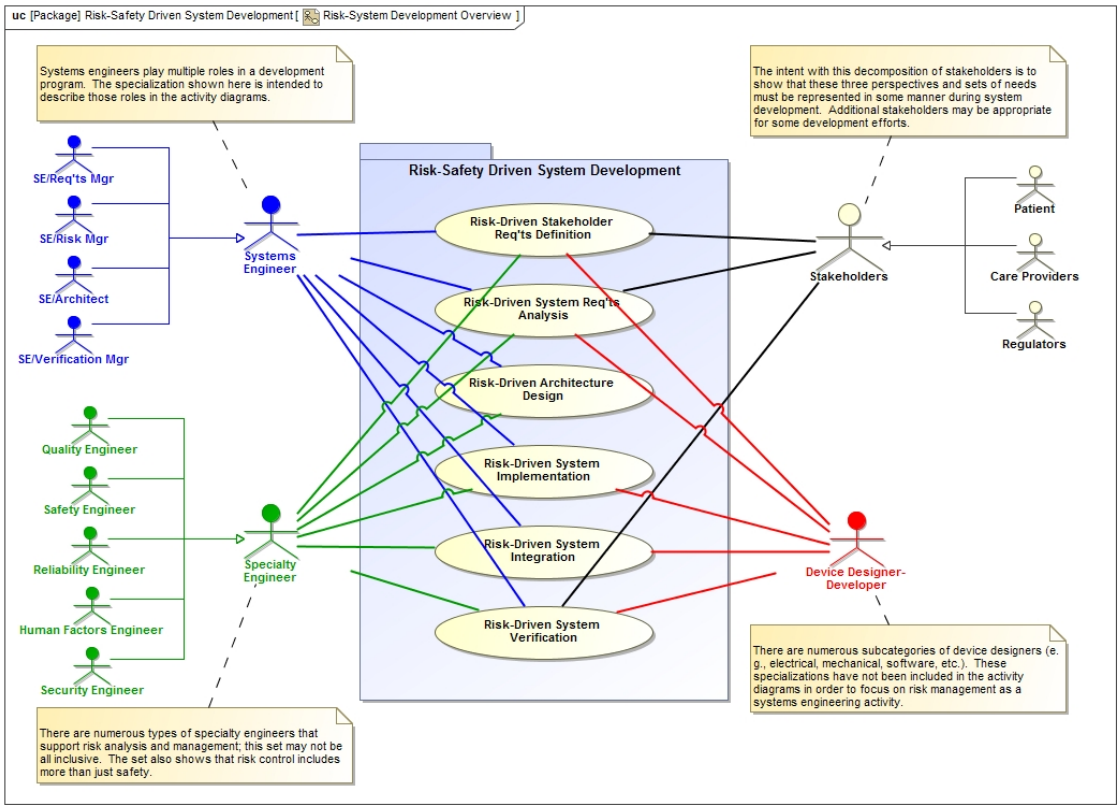


Figure 2. Outline of the use cases developed for integrating ISO 14971 with ISO 15288 (The color code assigned to each actor is continued in the remaining figures to identify the activities performed by each actor.)

It is important to note that the specialty engineer actor shown in Figure 2 represents a broad range of specialties including general safety, quality, reliability, human factors, and security. The process model described in the following sections focuses on safety, but also could be used to address any of these other specialty areas. Specialty areas like human factors and security are addressed in specific ISO standards; these standards have not been addressed in this work, but are being considered for future work by the MBSE Challenge Team.

Three SysML modeling artifacts were developed for each of the six use cases:

1) An activity functional decomposition was developed for each of the four primary actors. The major activities were extracted directly from the two ISO standards. These were then decomposed an additional level in order to make explicit the connections between development, risk management, and safety case activities that were identified during the alignment process in step one.
2) An information exchange model between the four roles was developed and captured as a SysML activity diagram. This activity diagram highlighted the products of the activities and how the four different actors interacted with each other.
3) An activity flow model was constructed using the activities from the activity functional decomposition. The activity flow diagram specified the sequence of activities necessary to achieve the information products shown in the information exchange model. The activity flow diagrams also showed what process activities could be performed concurrently and which ones necessarily were sequential due to dependence.

Results

The activity models for the six use cases produced a rather extensive page count of artifacts, far more pages than could be included in the page limitation for this paper. As a result, this paper only presents extracts from the model. The material presented below focuses on the information exchange model for each use case, since the information exchanges represent the continuous feedback between design and risk management that is critical to reducing hazards and safety issues at each stage of design development. A PDF format printout of all of the artifacts in the model can be obtained from the authors.

Activity Modeling for Risk-Driven Stakeholder Requirements Definition

The objectives of ISO 15288 TP 6.4.1 Stakeholder Requirements Definition is to elicit and formalize the capabilities the stakeholder needs and the system constraints resulting from the stakeholder's operational concept and operating environment. The most important outcomes from TP 6.4.1 is a formal list of stakeholder requirements, validated through stakeholder review, along with the verification approaches to be used to show that the system meets these requirements. The information flow for TP 6.4.1 is shown in Figure 3. The process begins with stakeholder provided capability needs and operating constraints elicited by the systems engineer. The systems engineer then analyzes these to form an operational concept, intended use, and system use cases that are validated with the stakeholder. Once validated they are used to provide design engineers with operational information that can be used to evaluate historical design experience to identify promising approaches for meeting the requirements. The operational information is also provided to the specialty engineers who use it to perform an early hazard assessment to identify safety needs based on knowledge of the operational environment and on review of data about similar devices. The systems engineer integrates the input from the designers and specialty engineers to form a complete package, including safety issues that must be controlled, that is validated by the stakeholders.

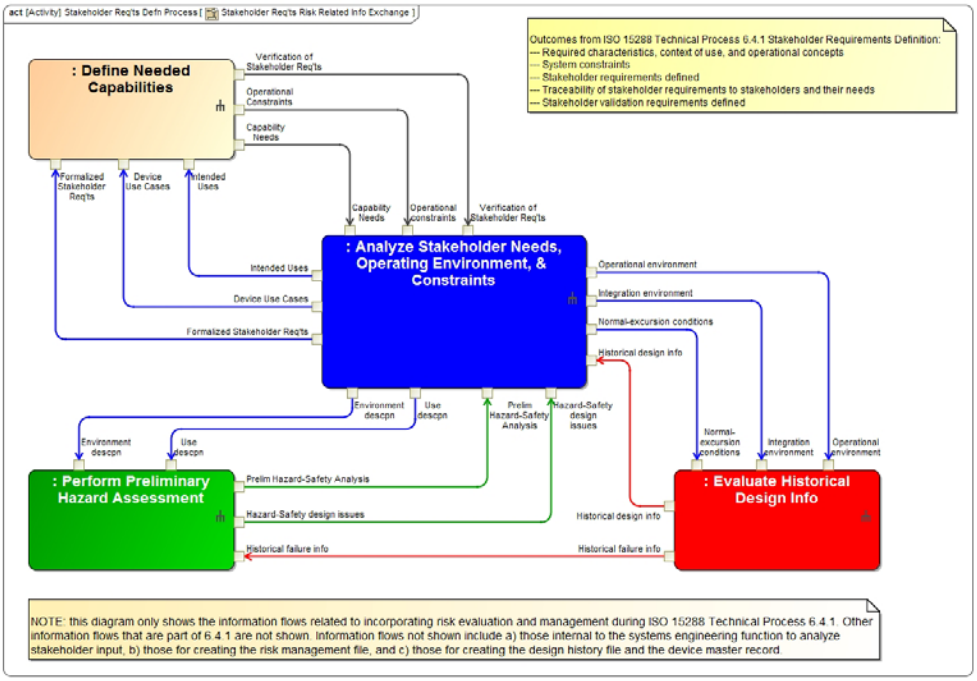


Figure 3. Key information exchanges for Risk-Driven Stakeholder Requirements Definition

From the perspective of risk control-mitigation and safety case development, three key actions are accomplished during TP 6.4.1. The first action is executing a preliminary risk-hazard analysis based on the device intended use and its associated use cases; this is performed by the specialty engineers. The second action is the review of historical risk and safety information for the intended use and operating environment performed by the design team. Both of these products are used to verify with the stakeholders the key elements of risk and safety control required of the system and to ensure that these elements are represented in the stakeholder requirements package. The third key action in TP 6.4.1 is to use the results of the preliminary hazard analyses and historical review to create the top-level safety claims for the system. As a result of these three actions the system risks and hazards are identified and verified with the stakeholders, the control-mitigation requirements for these hazards are included into the stakeholder requirements package in order to drive system design, and the basic structure of the safety case for proving safe operation is defined in order to drive the system verification planning process.

Activity Modeling for Risk-Driven System Requirements Analysis

The primary objective of ISO 15288 TP 6.4.2 is to convert stakeholder input into a formal requirements package that will drive the system design. The primary outcomes from the process are the requirements package itself and the allocation of the requirements to system functions, both of which are validated with the stakeholders. The key information exchanges in the process are shown in Figure 4. The process begins with the systems engineers analyzing the stakeholder input from TP 6.4.1 and creating the system functional boundaries, system functions, and stakeholder requirements allocations. These are then used by the specialty engineers

to perform functional risk, safety, reliability, security, and other assessments, to include functional Failure Modes and Effects Analyses (FMEA) and functional Fault Tree Analyses. The outcomes of these analyses are used to incorporate risk mitigation and safety requirements into the system requirements package. The system functional descriptions and risk analyses are then evaluated by the design engineers to assess design and technology feasibility for each of the systems functions and to create technical performance measures (TPMs) and technical quality measures (TQMs) for system. The systems engineers then integrate all of this information in to a complete requirements package, analyze requirements traceability to needs and constraints, and then review the complete process with the stakeholders for validation.

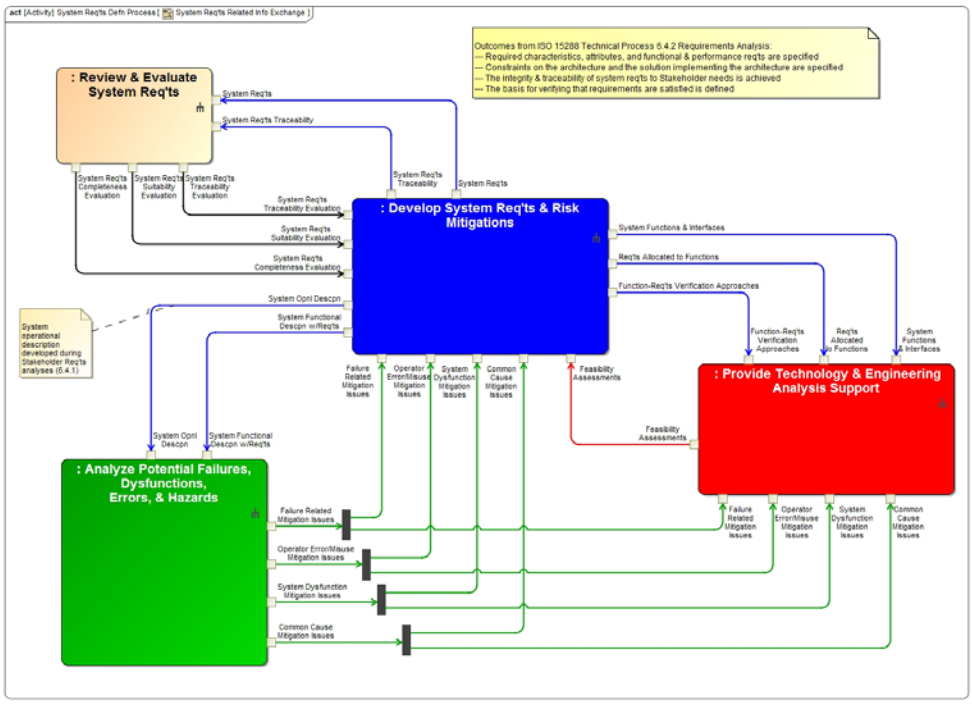


Figure 4. Key information exchanges for Risk-Driven System Requirements Analysis

TP 6.4.2 includes a number of critical risk control and safety implementation actions. The detailed risk analyses using the system functions provide additional detail beyond the preliminary hazard analyses of TP 6.4.1 and develop the quantitative values for requirements that must be included in the design. In addition, these analyses and the resulting requirements feed directly into establishing the arguments to be applied to each claim in the safety case. Moreover, the development of the TQMs and TPMs not only supports the design process, but also supports the safety case by being tailored and/or augmented to satisfy the evidence needs of the safety case claims and arguments. By including risk control needs and safety case evidence needs directly into the definition of the system requirements package, safety is "built in" to the system from the beginning. It should be noted that the role of the design engineers at this point is to assess the feasibility of meeting each requirement. And the implied iteration between requirements (system engineering function) and design and technology feasibility (design engineering function) ensures that the overall package not only satisfies the stakeholder capability needs, but also is practical to achieve.

Activity Modeling for Risk-Driven Architecture Design

ISO 15288 TP 6.4.3 has the objectives of creating the system architecture and defining the roles of humans in operating and controlling the system. TP 6.4.3 produces a logical system architecture, a feasible and effective physical system architecture, a human-system design, and a safety-risk control design approach. The information exchange model for TP 6.4.3 is shown in Figure 5. The process begins with the systems engineers defining a logical system architecture (LSA) from the system functions and analyzing the human-system integration and interface approach. These are then analyzed by the specialty engineers to define risk control needs and usability concepts that will prevent or minimize human errors, misuse, and dysfunctions. These are then provided to the designers who develop design alternatives for each LSA element; the alternatives are evaluated against the requirements by the systems engineers and approaches are selected for the physical architecture. The design engineers then develop the physical design approaches for each element of the physical architecture along with the designs for risk control and safety included in each element. The design engineers also define the verification approaches that will be used to evaluate system hardware. The specialty engineers evaluate these approaches and make recommendations for updates. All of this information is integrated by the systems engineers for review and validation by the stakeholders.

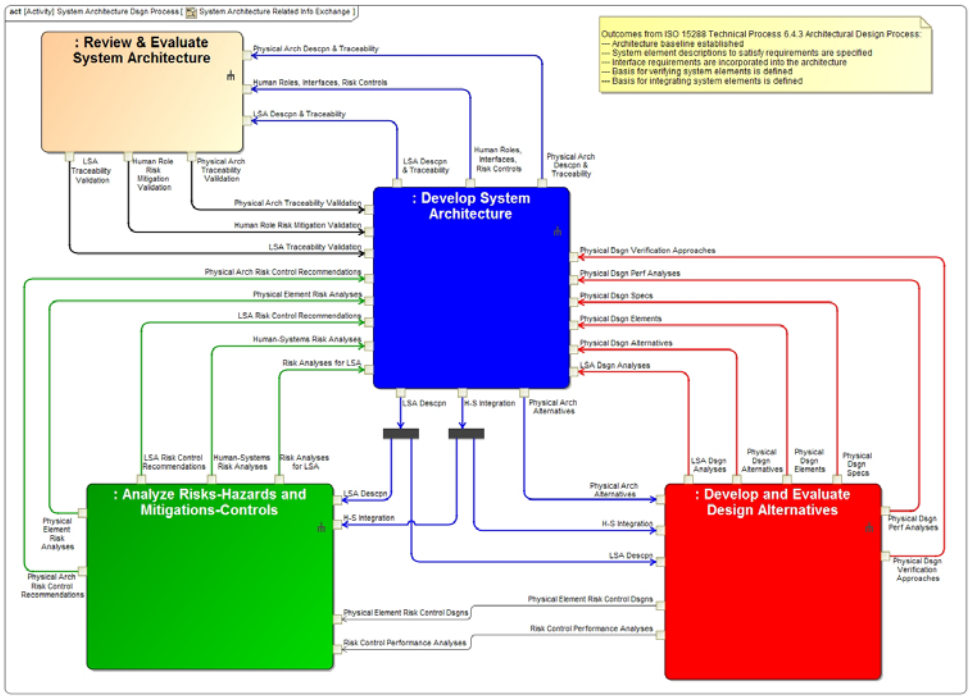


Figure 5. Key information exchanges for Risk-Driven System Architecture Design

TP 6.4.3 is the part of the life cycle where the upfront risk and safety analyses outcomes are embedded directly in the system design. The focus on human-system integration ensures that the architecture provides for adequate control of human-system failures, misuse, dysfunctions. The evaluation of design alternatives

by the systems engineers and specialty engineers directly considers risk control to ensure that the selected design approaches meet safety needs. The iteration between the systems engineers defining the architecture and the specialty engineers evaluating that architecture creates the information necessary for the second level claims of the safety case. In addition, the risk control designs are driven by the arguments for substantiating the second level claims and the definition of evidence needs for the second level claims becomes a critical part of defining the verification approaches.

Activity Modeling for Risk-Driven System Implementation

ISO 15288 TP 6.4.4 realizes each individual element of the system design and develops verification data demonstrating that the realized elements meet requirements. The primary outcomes from TP 6.4.4 are fully realized hardware, software, and operating training elements of the system along with the verification data developed for each element. TP 6.4.4 primarily consists of the design engineers creating or acquiring the elements of the system. As indicated in Figure 6, the primary role for the systems engineering and specialty engineering functions are to review and evaluate the implementation strategies and verification data to determine if system requirements and risk control goals have been met. The review and evaluation process is iterative with both systems engineers and specialty engineers providing recommended updates to the implementation based on their evaluations.

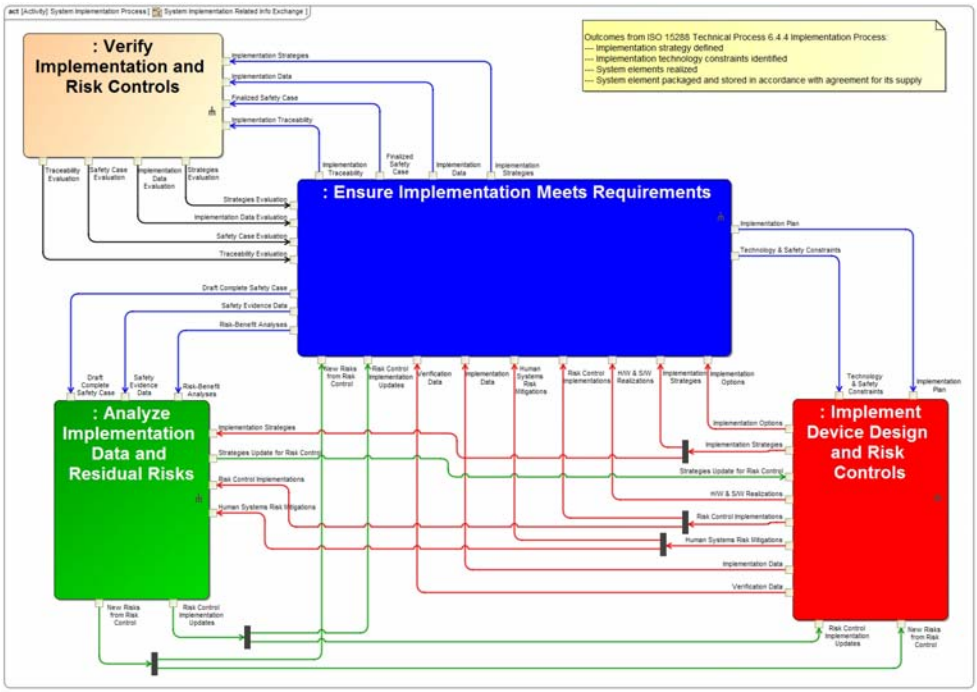


Figure 6. Key information exchanges for Risk-Driven System Implementation

During TP 6.4.4, risk control goals constrain implementation strategies to ensure that the strategies are tailored to meet risk goals. Much of this tailoring has already been achieved prior to TP 6.4.4 by means of the incorporation of risk control into the requirements set and the embedding of risk controls into the system architecture. The iteration between design engineering and specialty engineering during TP 6.4.4 ensures the implementation approaches meet the safety goals and provides the

mechanism for specialty engineers to recommend implementation updates to improve system safety. TP 6.4.4 also develops the first verification data that are used to show that actual hardware, software, and human-systems integration performance meets the requirements set in earlier Technical Processes. These verification data, because they were defined in part by the evolving safety case, are also used directly to provide the evidence for the third level safety case claims. In this way, the concurrent accomplishment of the safety case not only produces a superior design, it requires very little additional work beyond that which is necessary to meet ISO 14971 risk control requirements and to execute the planned verification testing. From the perspective of reporting to regulatory organizations, the safety case structures the risk management data in order to facilitate evaluation of the risk control outcomes.

Activity Modeling for Risk-Driven System Integration

The objective of ISO 15288 TP 6.4.5 is to integrate the system elements into a complete system that can be verified against requirements and stakeholder needs. The products of TP 6.4.5 are the integrated system, the data documenting conformance to requirements, and the design history records for system changes where necessary to achieve conformance. In theory, both capabilities and risk control-safety were fully considered during the architecting and designing of the system and integration should be a matter of assembling the elements realized in TP 6.4.4 and verifying that they meet requirements. However, real life is rarely that simple. As a result, TP 6.4.5 continues the iteration between design engineers executing integration in hardware, software, and human-systems interfaces while the systems engineering and specialty engineering functions continue to perform more detailed analyses of system operations based on actual verification data to ensure requirements and safety goals are met and to define system updates when the initial realization and/or integration does not meet requirements.

It should be noted that parts of TP 6.4.5 are actually performed well before the initiation of TP 6.4.4. Key steps in TP 6.4.5, specifically those related to creating and evaluating the integration strategy, should be performed in parallel with TP 6.4.3 in order to influence the system architecture so that integration is practical and facile.

TP 6.4.5 is a critical point for both device risk management and safety case development. During TP 6.4.5 the system becomes sufficiently mature that residual risk can be evaluated using real measurements on the hardware-software-human system integrated assembly. The residual risk evaluation is followed by a risk-benefit analysis and, if necessary, the recommendation of additional risk control-risk mitigation actions that update the system design, implementation, and integration. If changes are made, then the residual risk and risk-benefit analyses are repeated on the updated implementation to ensure that no new risks have been introduced. TP 6.4.5 is also the first point in the system development life cycle when all evidence needs can be met for all levels of claims in the safety case. Therefore, TP 6.4.5 is the point when the complete safety case is assembled and evaluated for quality, completeness, and ability to provide compelling proof of safety. The assembly of the safety case and the analyses of residual risk and risk-benefit are complementary works and should be compared to each other for consistency.

Activity Modeling for Risk-Driven System Verification

ISO 15288 TP 6.4.6 performs the final verification of the complete device and the outcome is a fully functioning system with a data package verifying that requirements and safety goals have been met. As with TP 6.4.5, the early elements of TP 6.4.6 – defining the verification strategies and plan – are actually performed in parallel with TP 6.4.3, 6.4.4, and 6.4.5. Beginning verification planning early ensures that the requirements, TPM and TQM, and design feasibility assessments fully consider the issues and difficulties inherent in system integration. Also like TP 6.4.5, TP 6.4.6 should be a simple process because all issues associated with performance and risk control were considered early and "built in" to the requirements, system design, system implementation, and system integration. Therefore, TP 6.4.6 continues the iterative process of testing the system, evaluating the test data to determine conformance/non-conformance, recommending updates where necessary, and then verifying that the updates do not introduce new risks.

From the perspective of risk management and safety case development, TP 6.4.6 continues the analyses of TP 6.4.5 using the data generated in the more realistic operating environment of system verification. TP 6.4.6 continues the work to assemble hard evidence showing that all safety case claims have been met and that the residual risk and risk-benefit is acceptable when the device is operated in a realistic environment.

Alignment With FDA Guidance for Design Control

The goal of the methodology in this paper is to address the full life cycle of the device development process. The intent of the Biomedical-Healthcare MBSE Challenge Team is to provide development organizations with a reference process which can be tailored to a given organizations specific business needs. The life cycle process for device development is addressed in the Food and Drug Administration's (FDA's) design control guidance document (FDA 1997). The FDA's design control process is summarized in Figure 7. In the figure, the blue outline shows the portion of the design control process addressed by the process model for ISO 15288 TP 6.4.1 to TP 6.4.6. The final portion of the process, namely production and validation, is addressed by ISO 15288 TP 6.4.7 to TP 6.4.11 and is the subject of potential future work by the MBSE Challenge Team.

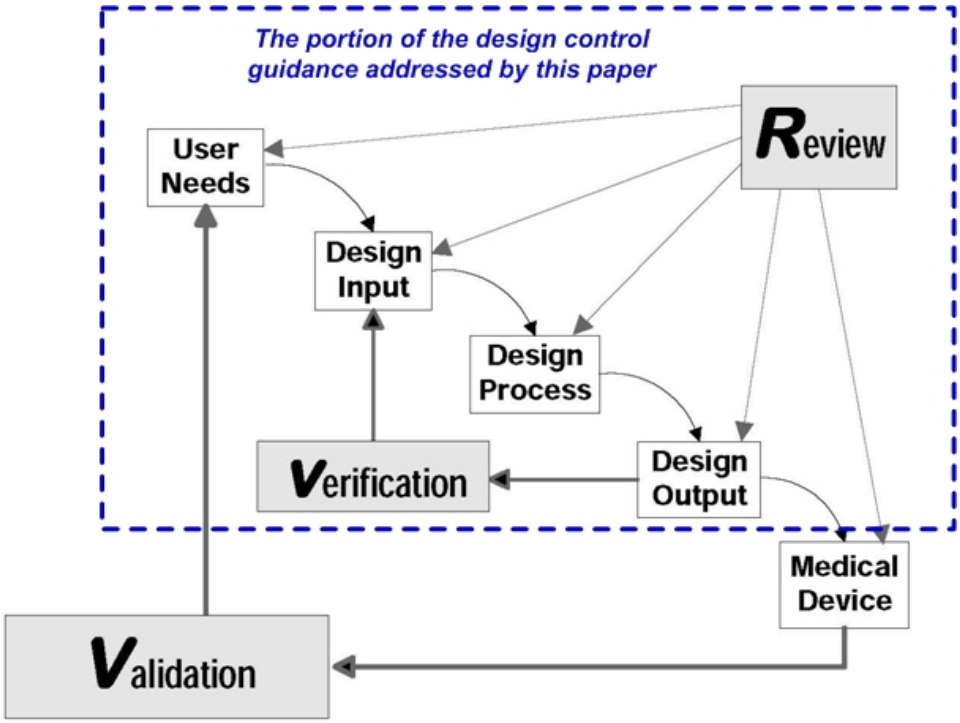


Figure 7. Design control process summary from FDA guidance paper with annotations showing relationship to the activity model described in this paper

The process described in the preceding sections of this paper can be mapped directly to the FDA design control process. Many of the details of the mapping are contained in the detailed activity flow diagrams that support the information exchanges shown in Figures 3 to 6. The key connections between the process model herein and the FDA process can be summarized as follows:

Design control general requirements. The key overarching design control requirements are for integrating quality and risk management throughout the development process beginning with the elicitation of user needs; this requirement is addressed in our model for TP 6.4.1 wherein risk analysis and requirements development are initiated as part of creating the user-driven description of intended use, operational concept, and device use cases.

Design and development planning. The key requirements for the development plan are to define the tasks and associated reviews as well as the interfaces between the tasks. The work summarized in this paper defined the requisite tasks in the activity functional decompositions and defined the interfaces in the activity flow diagrams; thus the model itself can be used to support design and development planning.

Design input. for design control, the key aspects of design input are clearly specifying the intended use, patient and user needs, and the operational concept for the device and translating these into engineering requirements and assessing them for adequacy. The information exchanges for TP 6.4.1 and TP 6.4.2 clearly show how these requirements are met in the process model.

Design output. FDA guidance for design output focuses on documenting the outcomes of each step in the development process and showing that the products directly reflect the user needs and device requirements. The process descriptions for TP 6.4.3 to TP 6.4.6 show that at each stage of development, the design is traced to the original requirements and any gaps or shortfalls from the traceability analyses are addressed as design updates.

Design reviews. The process model includes two types of design reviews. The primary reviews are shown in the information exchange descriptions (Figures 3 to 6) as the information exchanges to the Stakeholder actor and the review feedback from the Stakeholders to the systems engineers. TP 6.4.4, 6.4.5, and 6.4.6 include a second type of review in the information exchange to the Specialty Engineering actors who review the design from the perspective of adequacy of design to mitigate and/or control risks (see example exchanges in Figure 6).

Design verification. Design verification is addressed throughout the process model beginning with the definition of verification approaches in TP 6.4.3 and continuing through the actual measurement and evaluation of verification data at the component level in TP 6.4.5 and at the system level in TP 6.4.6.

Conclusions

This paper has provided an overview of the activity model developed by the Biomedical-Healthcare MBSE Challenge Team to show how risk management is integrated into the system life cycle during system development. The activity model begins the risk analyses during the elicitation of stakeholder needs and leverages stakeholder experience with the operational environment and system intended use to ensure a complete understanding of risk control and safety needs. The early risk and hazard analyses are then incorporated into the requirements analysis and definition process to ensure that system design directly considers risk control from the beginning of its development. The consideration of risk is continued during system architecture development where risk control designs are evaluated for effectiveness and TPMs and TQMs are defined so that the efficacy of risk control implementation, integration, and verification can be measured. In theory, if risk control is fully considered during requirements and design development, system implementation and integration and verification should be a simple process of showing that the realized system meets requirements. However, that is an unrealistic expectation. Hence the activity model includes iterative processes wherein the system is realized and tested and then the test data are evaluated to ensure requirements and safety goals are met and to define system updates when the initial realization and/or integration does not meet requirements. The evaluation of residual risk and risk-benefit are part of each iteration to ensure that design changes to address one issue do not add new risk or safety issues.

The activity model presented integrates the creation of a safety assurance case with the conventional risk management process of ISO 14971. The safety case is a hierarchical decomposition of top-level, overarching claims driven by intended use and operational environment. The top level claims are developed during the preliminary hazard analyses performed during stakeholder capability needs elicitation

and the arguments for meeting these claims are developed in parallel with, and in iteration with, the definition of system requirements. The top-level claims are decomposed in parallel with the functional and architectural decomposition of the system. The evidence needs for these claims and subclaims is directly part of the development of TPMs and TQMs and the creation of system verification plans and approaches. As the system matures through implementation, integration, and verification, the verification data becomes the leaf level evidence inserted into the safety case. As a result, creating the safety case requires very little additional effort beyond that already performed for risk management and system verification.

The activity model developed by the Biomedical-Healthcare MBSE Challenge Team directly addresses the process integration mandate levied by ISO 13485 Medical devices—Quality management systems—Requirements for regulatory purposes. The need for process integration is specified in ISO 13485 Section 4.0 General Requirements. The model presented provides that process integration. In addition, the model also addresses ISO 13485 Section 7.0 Product Realization requirements concerning customer input, requirements development, and design and development addressing the control of risks and safety.

The process integration achieved with the MBSE Challenge Team's activity model focused on general risks and overall safety. As was shown in the model definition (see figure 2), the integration process applies equally well to safety, security, reliability, usability, and other sources of system risk and safety concerns. Therefore, it is expected that the process used to integrate ISO 14971 across the life cycle could be easily generalized to address other medical device relevant standards such as ISO 60601 Medical Electrical Equipment Safety, IEC 62366 Application of Usability Engineering to Medical Devices, ISO 21827 System Security Engineering, and IEC 80001 Risk Management for Medical Devices on IT Networks.

References

M. S. Herring, B. D. Owens, N. Leveson, M. Ingham, and K. Ann Weiss, “A Safety-Driven, Model-Based System Engineering Methodology, Part I”, MIT Technical Report, 2007, http://sunnyday.mit.edu/JPL-Part-1.pdf).

D. C. Jensen and I. Y. Tumer, "Modeling and Analysis of Safety in Early Design", Conference on Systems Engineering Research (CSER'13), Atlanta, GA, March 19-22, 2013.

D. Feng and C. Eyster, "Risk-Based Requirements Management Framework with Applications to Assurance Cases", IEEE Aerospace Conference, March 2-9, 2013

P. Bishop and R. Bloomfield, “A Methodology for Safety Case Development”, Proceedings of the Sixth Safety-critical System Symposium, Birmingham, UK, 1998; http://www.adelard.com/papers/sss98web.pdf

R. Hawkins, T. Kelly, J. Knight and P. Graydon, "A New Approach to Creating Clear Safety Arguments", Safety-critical Systems Symposium, Southampton, UK, February 2011

D. Feng and C. Eyster, “Towards Integrating Assurance Cases into Risk-Based Requirement Management”, 22nd Annual INCOSE International Symposium, Rome, Italy, 2012

F. Mhenni, N. Nguyeny, H. Kadimay and J-Y Choley, "Safety Analysis Integration in a SysML-Based Complex System Design Process", 2013 IEEE International Systems Conference (SysCon), April 15-18, 2013

A. Ayoub, B. Kim, I. Lee and O, Sokolsky, "A Safety Case Pattern for Model-Based Development Approach", NASA Formal Methods Symposium (NFM), Norfolk, VA, April 2012 (This paper is posted at Scholarly Commons. http://repository.upenn.edu/cis_papers/485)

R. Cressent, P. David, V. Idasiak and F. Kratz, "Dependability analysis activities merged with system engineering, a real case study feedback", Christophe Berenguer, Antoine Grall, Carlos Guedes Soares. ESREL 2011, Sep 2011, France. CRC Press

E. Jee, I. Lee and O. Sokolsky, "Assurance Cases in Model-Driven Development of the Pacemaker Software", Proceedings of the 4th International Symposium On Leveraging Application of Formal Methods, Verification and Validation (ISoLA), Part II, LNCS 6416, pp. 343-356, Amirandes, Heraclion, Crete, October 18-20, 2010

Food and Drug Administration, "Design Control Guidance for Medical Device Manufacturers", March 11, 1997

Biographies

Dr. Robert J. Malins is the founder and owner of Eagle Summit Technology Associates, Inc. and has over 35 years of experience in R&D and system development in defense, aerospace, energy, and security fields as well as in commercial product development. Dr. Malins is a senior systems engineer skilled in both the technical and management functions of systems engineering. In addition, he has a strong background in numerous technologies and has been the concept integrator for many multi-disciplinary teams. For the past ten years Dr. Malins has provided systems engineering, architecture development, and concept development support to Army programs in unmanned systems development, tactical network integration, and force basing architectures and to DOE National Laboratory programs to transfer DOE technologies to military systems. Prior to forming Eagle Summit, Dr. Malins worked in the aerospace industry supporting a broad range of advanced technology programs in directed energy, kinetic energy interceptors, command and control systems, and novel optical and RF sensors. Dr. Malins received his BS in chemistry in 1974 from the University of Houston and his Ph.D. in physical chemistry in 1978 from the University of Iowa.

Jack Stein is a Systems Engineer, Co-Chair of the INCOSE Risk Management Working Group (WG), member of the INCOSE- Project Management Institute (PMI) Strategic Alliance WG, and member of the INCOSE Biomedical-Healthcare WG and Model-Based Systems Engineering (MBSE) Challenge Team. He also serves as Assistant Director of the INCOSE Americas Sector North-Central Region. Mr. Stein has 28 years of experience in the Automotive and Medical Device industries, and more than 20 years of experience as a U.S. national technical expert in the development of a variety of industry standards (ISO, IEC, SAE, ZVEI). Recently, he led the effort to complete the revision of the Risk Management section of the INCOSE Systems Engineering. Handbook Version 4.0. He is currently leading a collaborative effort between the INCOSE Risk Management WG and the PMI Risk Management Community of Practice (CoP) in support of the INCOSE-PMI Strategic Alliance. Mr. Stein studied Systems, Reliability and Quality Engineering at the University of Arizona, Tucson, Arizona under the Ford Motor Company Fellowship Award, and has BSEE and Bachelor of Commerce Degrees from the University of Windsor, Ontario, Canada.

Dr. Ajay Thukral is co-founder of Cientive Group, Inc. and serves as the company's Chief Technology Officer, in addition to sitting on the Board of Directors. Dr. Thukral has a background in aerospace engineering. He has been an integral part of the team that developed some of the core tools for Cientive's proprietary transcription services. He leads the mathematical analysis, modeling of engineering and biomedical teams at Cientive. He is a former R&D mathematical and modeling specialist and continues to serve as a consultant for Roche Diagnostics. Dr. Thukral received his BS degree from the Indian Institute of Technology and his MS and Ph.D. from Auburn University.

Christophe Waterplas is a lead systems engineer at Resmed Ltd. with over 10 years of experience in the medical device industry. Mr. Waterplas graduated with a master

degree in electromechanical engineering and telecommunication in 1998 from Université libre de Bruxelles in Brussels, Belgium. He began his professional career as a software engineer in the telecommunication industry. In 2003 he changed fields, developing embedded software for mechanical ventilators at Resmed before becoming a systems engineer in 2005. He has worked on several projects providing his expertise in risk management, usability engineering and alarm systems.

.