Reference Architectures and Medical Device Development and Evaluation

Applying Risk-Hazard-Safety Management Across the System Lifecycle

Model working file
October 2014

Bob Malins
Eagle Summit Technology Associates, Inc.
505-238-9227
rjmalins@eaglesummittech.com
Model Version 2_0 2014-10-01
Outline & Status of the Work

• Overview
  – This package provides the model artifacts for the technical process descriptions developed for the INCOSE Biomedical-Healthcare MBSE Challenge Team
    • INCOSE GLRC8 paper “Applying ISO 14971 Medical Device Risk and Safety Management Across the System Lifecycle: A SysML Use Case Linking ISO 14971 and ISO 15288”

• Outline of Analysis Products
  – Tables documenting initial synchronization of ISO 14971 with ISO 15288 and safety case development
  – SysML model structure and overview of technical process use cases
  – Integrated ISO 15288/ISO 14971 technical process descriptions
    • Process Model 1 -- Technical Process 6.4.1 Stakeholder Req’ts Definition
    • Process Model 2 -- Technical Process 6.4.2 System Req’ts Analysis
    • Process Model 3 -- Technical Process 6.4.3 Architecture Design
    • Process Model 4 -- Technical Process 6.4.4 System Implementation
**Project Scope**

- Current project begins ISO 14971-ISO 15288 integration by examining device development

<table>
<thead>
<tr>
<th>Agreement Processes</th>
<th>Technical Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition Process (Clause 6.1.1)</td>
<td>Stakeholder Requirements Definition Process (Clause 6.4.1)</td>
</tr>
<tr>
<td>Supply Process (Clause 6.1.2)</td>
<td>Requirements Analysis Process (Clause 6.4.2)</td>
</tr>
<tr>
<td></td>
<td>Architectural Design Process (Clause 6.4.3)</td>
</tr>
<tr>
<td></td>
<td>Implementation Process (Clause 6.4.4)</td>
</tr>
<tr>
<td></td>
<td>Integration Process (Clause 6.4.5)</td>
</tr>
<tr>
<td>Organizational Project-Enabling Processes</td>
<td>Verification Process (Clause 6.4.6)</td>
</tr>
<tr>
<td>Life Cycle Model Management Process (Clause 6.2.1)</td>
<td>Transition Process (Clause 6.4.7)</td>
</tr>
<tr>
<td>Infrastructure Management Process (Clause 6.2.2)</td>
<td>Validation Process (Clause 6.4.8)</td>
</tr>
<tr>
<td>Project Portfolio Management Process (Clause 6.2.3)</td>
<td>Operation Process (Clause 6.4.9)</td>
</tr>
<tr>
<td>Human Resource Management Process (Clause 6.2.4)</td>
<td>Maintenance Process (Clause 6.4.10)</td>
</tr>
<tr>
<td>Quality Management Process (Clause 6.2.5)</td>
<td>Disposal Process (Clause 6.4.11)</td>
</tr>
</tbody>
</table>

**Device development portion of the life cycle**

- Near-term objective for INCOSE Biomedical MBSE Challenge Team
- Addressed in the current project and this presentation

**Device operations, sustainment, and disposal portion of the life cycle**

- Includes operations, sustainment, and maintenance within care provider organization
- Includes ultimate device disposal by care provider organization or others
- Possible future work by INCOSE Challenge Team
Project Approach

- Develop a SysML model that integrates ISO 14971 with ISO 15288 and builds an safety case

---

**System Life Cycle Processes**

<table>
<thead>
<tr>
<th>Agreement Processes</th>
<th>Project Processes</th>
<th>Technical Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition Process (Clause 6.1.1)</td>
<td>Project Planning Process (Clause 6.3.1)</td>
<td>Stakeholder Requirements Definition Process (Clause 6.4.1)</td>
</tr>
<tr>
<td>Supply Process (Clause 6.1.2)</td>
<td>Project Assessment and Control Process (Clause 6.3.2)</td>
<td>Requirements Analysis Process (Clause 6.4.2)</td>
</tr>
<tr>
<td></td>
<td>Decision Management Process (Clause 6.3.3)</td>
<td>Architectural Design Process (Clause 6.4.3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implementation Process (Clause 6.4.4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integration Process (Clause 6.4.5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verification Process (Clause 6.4.6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transition Process (Clause 6.4.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validation Process (Clause 6.4.8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operation Process (Clause 6.4.9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance Process (Clause 6.4.10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disposal Process (Clause 6.4.11)</td>
</tr>
</tbody>
</table>

From ISO 15288:2008 – The System Lifecycle Processes

---

Define Device Development Activity Flows that Link Risk Management Actions to System Development Processes

---

From ISO 14971:2007 – Schematic representation of risk management process
Applying Risk-Hazard-Safety Management Across the System Lifecycle

### TABLE: Proposed Activity Laydown – ISO 14971 Actions Against ISO 15288 Technical Development Processes

<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder Req'ts Definition Process (6.4.1)</td>
<td>• Define all intended uses of the system or device</td>
<td>Initial/Preliminary Hazard Analysis</td>
<td>Identified hazards are grouped based on similarity in phenomenology. The groups are used to develop the top-level claims of the assurance case</td>
</tr>
<tr>
<td>• Req'd characteristics, context of use, operational concepts</td>
<td>• Define use cases for all intended uses of the device or system</td>
<td>• Identify hazards from failure, dysfunction, and misuse [4.2]</td>
<td>• &quot;The device will be safe from group x hazards&quot;</td>
</tr>
<tr>
<td>• System constraints</td>
<td>• Define system operating environment and expectation on user/operator roles</td>
<td>• Identify hazards from operating environment [4.3]</td>
<td>Employ the top-level claims to evaluate the completeness of the req'ts set for risk and safety issues.</td>
</tr>
<tr>
<td>• Traceability of stakeholder req'ts to stakeholders &amp; their needs</td>
<td>• Define system integrating environment and stakeholder integration expectations</td>
<td>• Identify hazards from integrating environment [4.3]</td>
<td></td>
</tr>
<tr>
<td>• Stakeholder req'ts defined</td>
<td>• Define normal and excursion operating conditions</td>
<td>• Identify hazards from operator actions or errors/usability [4.3]</td>
<td></td>
</tr>
<tr>
<td>• Stakeholder validation req'ts defined</td>
<td></td>
<td>Identify any additional stakeholder req'ts necessary to mitigate hazards</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Additional User Needs:**
- Verifying additional user needs for safety/risk control with stakeholders and establish traceability to stakeholder req'ts

**Note:**
- *Blue bold face font* indicates a feedback from risk management/assurance case to the Technical Process.
- *Green bold face font* indicates feedback into Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Analysis Process (6.4.2)</td>
<td><strong>Define system functional boundaries</strong></td>
<td><strong>Perform functional FMEA based on system functional taxonomy</strong></td>
<td><strong>Use results of functional FMEA, FTA, and ETA to define the overall strategy (or set of strategies) for each of the top-level assurance case claims</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Define system functions/functional taxonomy</strong></td>
<td><strong>Identify conventional failure modes and their probability and consequence [4.4]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Allocate stakeholder req'ts to system functions and develop system req'ts</strong></td>
<td><strong>Identify failures due to operator actions (usability) and their probability and consequences [4.4]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Define technical/quality measures for each function to achieve req'ts</strong></td>
<td><strong>Define additional technical/quality measures based on failure analysis</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Define functions and req'ts related to mitigating risk, safety, and usability issues</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Define functions and req'ts related to mitigating risk, safety, and usability issues</strong></td>
<td></td>
<td>Map second level claims to system functions</td>
</tr>
<tr>
<td></td>
<td><strong>Perform functional FMEA based on system functional taxonomy</strong></td>
<td><strong>Identify common cause dysfunctions and their probability and consequence [4.4]</strong></td>
<td><strong>Perform initial assessment of technical/quality measures for sufficiency in meeting claims</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Perform FTA/ETA based on intended use and operating/integrating environment</strong></td>
<td><strong>Identify event-based dysfunctions and their probability and consequences [4.4]</strong></td>
<td><strong>Identify new system functions needed to ensure that second level claims can be met.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Define additional technical/quality measures based on failure analysis</strong></td>
<td><strong>Identify new/revised technical/quality measures to ensure second level claims can be met.</strong></td>
</tr>
</tbody>
</table>

Note: *Blue bold face font* indicates a feedback *from* risk management/assurance case to the Technical Process.

Note: *Green bold face font* indicates feedback *into* Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Design Process (6.4.3)</td>
<td>- Define logical system architecture</td>
<td>- Map functional FMEA, FTA, ETA outcomes to logical system architecture elements</td>
<td>Develop strategy for each second level claim based on logical system architecture elements.</td>
</tr>
<tr>
<td>- Architecture baseline established</td>
<td>- Allocate functions to logical system architecture elements</td>
<td>- Re-evaluate probability and consequences based on architecture elements [5.0]</td>
<td>Decompose second level claims into third level claims based on risk analysis and selected risk control measures.</td>
</tr>
<tr>
<td>- System element descriptions to satisfy req'ts specified</td>
<td>- Define system interfaces (internal &amp; external)</td>
<td>- Determine if risk control measures are needed for each architecture element [6.1]</td>
<td>Develop evidence needs for each third level claim based on technical and quality control measures applied to each architecture element.</td>
</tr>
<tr>
<td>- Interface req'ts incorporated</td>
<td>- Allocate system requirements to architecture elements</td>
<td>Assess risk control options [6.2]</td>
<td>Evaluate overall set of safety case claims for completeness.</td>
</tr>
<tr>
<td>- Traceability of architecture to req'ts established</td>
<td>- Identify human operator roles and associated usability req'ts</td>
<td>- Identify new constraints on architecture to &quot;build in&quot; safety</td>
<td>Identify updates to logical system architecture based on what is needed for complete safety assurance case.</td>
</tr>
<tr>
<td>- Basis for verifying system elements defined</td>
<td>- Identify and evaluate design alternatives</td>
<td>- Identify new architecture elements needed to &quot;build in&quot; safety or control/mitigate risk</td>
<td></td>
</tr>
<tr>
<td>- Basis for integrating system elements defined</td>
<td>Update logical system architecture to incorporate built in safety and risk control/mitigation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: *Blue bold face font* indicates a feedback from risk management/assurance case to the Technical Process. Note: *Green bold face font* indicates feedback into Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Process (6.4.4)</td>
<td>• Define implementation strategy for each architecture element</td>
<td>Implement the selected risk control measures into the implementation strategy for each architecture element [6.3]</td>
<td>Evaluate component implementation strategies to assure that they will meet third level claim evidence needs</td>
</tr>
<tr>
<td>• Implementation strategy defined</td>
<td>• Define implementation constraints for each architecture element</td>
<td>Implement the selected risk control measures into the of each architecture element [6.3]</td>
<td><em>Revise implementation strategies to support the assurance case</em></td>
</tr>
<tr>
<td>• Implementation technology constraints identified</td>
<td>• Realize each architecture element (hardware, software, operator training)</td>
<td>Evaluate verification data on each realization to determine if risk goals have been achieved at component level [6.4]</td>
<td>Evaluate verification data to assure that it is sufficient to justify all third level claims</td>
</tr>
<tr>
<td>• System elements realized</td>
<td>• Record data verifying that each realization meets the constraints applied</td>
<td>Evaluate verification data on each realization to determine if risk control measures have introduced new risks [6.6]</td>
<td><em>Develop input to update component realization in order to achieve satisfaction of each third level claim</em></td>
</tr>
<tr>
<td>• System element packaged &amp; stored in accordance with agreement for its supply</td>
<td></td>
<td><em>Update implementation strategy and/or realization if needed</em></td>
<td></td>
</tr>
</tbody>
</table>

Note:  *Blue bold face font* indicates a feedback *from* risk management/assurance case to the Technical Process.
Note:  *Green bold face font* indicates feedback *into* Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
</table>
| **Integration Process (6.4.5)**  
- System integration strategy defined  
- Unavoidable integration constraints impacting req'ts defined  
- System capable of being verified is assembled and integrated  
- Non-conformances due to integration are recorded | - Define system constraints based on integration strategy  
**Update constraints based on needs to provide evidence to assurance case**  
- Obtain system elements  
- Assure system elements conform to req'ts/record non-conformances/corrective actions  
**Update assurance req'ts/obtain new system elements based on residual risk evaluation & evaluation of assurance case evidence**  
- Integrate elements according to interface controls and assembly procedures/record non-conformances/corrective actions  
**Update integration process/revise integration based on residual risk evaluation & evaluation of assurance case evidence** | - Update FMEA, FTA, ETA hazard estimation based on actual system element performances [4.4]  
**Provide input to revise system element req'ts & assurance measurements to meet goals from hazard estimation**  
- Update risk analysis based on actual/revised system element performances and integration constraints [5.0]  
**Provide input to revise integration procedures, constraints & measurements to reduce system risk**  
- Perform risk/benefit analysis based on actual/revised system element performances and integration results [6.4]  
**Incorporate results of assurance case evaluation into risk evaluation**  
- Evaluate completeness of risk control [6.7]  
**Provide input to revise integration procedures, constraints & measurements to improve risk control**  
- Update risk/benefit analysis [6.5] | - Compare actual system element assurance data to evidence needs for third level claims  
**Provided input to revise system element performances and assurance measurements to satisfy evidence needs**  
- Integrate evidence to evaluate satisfaction of third level claims  
**Provide input for additional req'ts and verification tests for system elements and additional integration constraints**  
- Integrate evidence + third level claims to evaluate second level claims  
**Provide input for additional req'ts and verification tests for system elements and additional integration constraints**  
- Integrate evidence + second level claims + third level claims to evaluate first level claims  
**Provide input to evaluation of overall effectiveness of risk control** |

Note: *Blue bold face font* indicates a feedback from risk management/assurance case to the Technical Process.  
Note: *Green bold face font* indicates feedback into Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
<table>
<thead>
<tr>
<th>ISO 15288 Technical Processes (outcomes shown in bullets)</th>
<th>15288 Actions/Products Connected to Risk Analysis (see model for complete list of 15288)</th>
<th>ISO 14971 Analyses, Iterations and Recursions [clause references to ISO 14971]</th>
<th>Relationship to Recursive Development of Safety Assurance Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Process (6.4.6)</td>
<td>• Define verification strategy throughout the system lifecycle</td>
<td>Employ Preliminary Hazard Analysis and Functional Risk Estimates to determine risk control verification approaches [4.3, 4.4]</td>
<td>Analyze strategies for first-level claims to determine assurance verification approaches</td>
</tr>
<tr>
<td></td>
<td>• Define verification plan</td>
<td>Provide input to verification strategy</td>
<td>Provide input to verification strategy</td>
</tr>
<tr>
<td></td>
<td>• Conduct verification data available</td>
<td>Provide input to verification plan</td>
<td>Provide input to verification plan</td>
</tr>
<tr>
<td></td>
<td>• Make verification results including discrepancies</td>
<td>Anayze verification data to update evaluation of completeness of risk control [6.7]</td>
<td>Analyze strategies and evidence needs for second and third-level claims to determine assurance verification req'ts</td>
</tr>
<tr>
<td></td>
<td>• Analyze/record/report corrective actions</td>
<td>Analyze verification data to update evaluation of residual risk [6.4]</td>
<td>Provide input to corrective actions (corrective actions could cause revision to any one of the technical processes 6.4.1-6.4.6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analyze verification data to update evaluate of risk/benefit [6.5]</td>
<td>Provide input to corrective actions (corrective actions could cause revision to any one of the technical processes 6.4.1-6.4.6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analyze results of assurance case evaluation as input to risk management</td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analyze verification data to determine overall acceptability of residual risk</td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td><strong>Revise verification strategy based on hazard estimation and strategies for first level claims</strong></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td><strong>Revise verification strategy based on</strong></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td><strong>Update any element of system design, integration, verification based on results of risk analyses and assurance case evaluations</strong></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provide input to corrective actions</td>
</tr>
</tbody>
</table>

Note: **Blue bold face font** indicates a feedback from risk management/assurance case to the Technical Process.
Note: **Green bold face font** indicates feedback into Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)
Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Model Structure
This package of use cases forms a precursor to the use cases for MBSE models that are shown in the "Reference Architecture Definitions and Applications" model. This package of use cases provides the raw material of process integration that will then be used in the Reference Architecture model's use cases. This package is being modeled separately for convenience in exploring options and getting review of the integration of the ISO 14971 process with the ISO 15288 system life cycle.

The use cases in this package address the elements of the life cycle relate to system development (i.e., ISO 15288 Technical Processes 6.4.1 to 6.4.6).

The use cases in this package address the elements of the life cycle after the system has transitioned to the field (i.e., ISO 15288 Technical Processes 6.4.7 to 6.4.11).

This package contains use cases for processes that included at multiple points in the ISO 15288 Technical Processes and that are not necessarily specified by ISO 15288.
NOTE: this diagram is just a placeholder for now. Eventually these use cases will get elaborated and the requirements that drive their execution (e.g., ISO 14971 for the risk management file and the FDA guidance documents for DHF & DMR) will be referenced.
NOTE: These six use cases step through the ISO 15288 Technical Processes 6.4.1 to 6.4.6 with one use case for each technical process showing how ISO 14971 risk management actions impact the activities within the technical process. Clearly there is a flow of activity from first (top) use case to the last (bottom) use case. This flow will be captured by linking the activity diagrams that elaborate the use cases.

The decomposition of stakeholders is an initial cut; there may be more added later. The intent with this specialization is to show that these three perspectives and sets of needs must be represented in some manner during system development.

There are numerous subcategories of device designers (e.g., electrical, mechanical, software, etc.). These specializations have not been included in the activity diagrams in order to focus on risk management as a systems engineering activity.

There are numerous types of specialty engineers that support risk analysis and management; this set may not be all inclusive. The set also shows that risk control includes more than just safety.

Systems engineers play multiple roles in a development program. The specialization shown here is intended to describe those roles in the activity diagrams.

The decomposition of stakeholders is an initial cut; there may be more added later. The intent with this specialization is to show that these three perspectives and sets of needs must be represented in some manner during system development.
Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Process Model 1 – 6.4.1 Stakeholder Req’ts Definition
Outcomes from ISO 15288 Technical Process 6.4.1 Stakeholder Requirements Definition:

- Required characteristics, context of use, and operational concepts
- System constraints
- Stakeholder requirements defined
- Traceability of stakeholder requirements to stakeholders and their needs
- Stakeholder validation requirements defined

Stakeholders perform these actions as part of the elicitation of req's by the Systems Engineers. See ISO 15288 6.4.1.3 actions (separate bdd).

Specialty engineers perform these actions to address key parts of ISO 15288 6.4.1.3 b) 3) and 6.4.1.3 b) 4).

Design engineers perform these actions in support of systems engineers and specialty engineers.
Outcomes from ISO 15288 Technical Process 6.4.1 Stakeholder Requirements Definition:
--- Required characteristics, context of use, and operational concepts
--- System constraints
--- Stakeholder requirements defined
--- Traceability of stakeholder requirements to stakeholders and their needs
--- Stakeholder validation requirements defined

NOTE: this diagram only shows the information flows related to incorporating risk evaluation and management during ISO 15288 Technical Process 6.4.1. Other information flows that are part of 6.4.1 are not shown. Information flows not shown include a) those internal to the systems engineering function to analyze stakeholder input, b) those for creating the risk management file, and c) those for creating the design history file and the device master record.
Stakeholders

- Express Needs, Shortfalls, Goals
  - Analyze Stakeholder Capability Needs
  - Define Intended Use & Operational Concept
  - Express User/Stakeholder Constraints
  - Analyze Stakeholder Constraints
  - Define System Boundaries, Constraints, & Integration Context
- Create System Use Cases
  - Analyze Stakeholder Inputs to form Req'ts
  - Formalize Integration Req'ts

SE/Architect

SE/Req'ts Mgr

SE/Risk Mgr

SE/Verification Mgr

Specialty Engineer

Device Designer-Developer

- Review/Characterize Historical Design Info
- Review/Characterize Historical Reliability, Safety
Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Process Model 2 – 6.4.2 Requirements Analysis Process
Outcomes from ISO 15288 Technical Process 6.4.2 Requirements Analysis:
— Required characteristics, attributes, and functional & performance req'ts are specified
— Constraints on the architecture and the solution implementing the architecture are specified
— The integrity & traceability of system req'ts to Stakeholder needs is achieved
— The basis for verifying that requirements are satisfied is defined

Stakeholders review req'ts analysis & management products under the leadership of systems engineers as per ISO 15288 6.4.2.3.

Systems Engineer

Review & Evaluate System Req'ts

Evaluate Traceability of System Req'ts to Stakeholder Needs
Evaluate Suitability of System Req'ts to Satisfy Stakeholder Needs
Assess Completeness of System Req'ts Relative to Stakeholder Needs

Develop System Req'ts & Risk Mitigations

Critical Activities:
— Define System Functional Boundaries
— Define System Functions
— Define Implementation Constraints for Each Function
— Specify System Req'ts for Each Function
— Define Technical & Quality Measures
— Apply Verification Approaches to Functions
— Develop Second-Level Assurance Case Elements
— Formalize, Review, & Publish System Req'ts

Analyze Potential Failures, Dysfunctions, Errors, & Hazards

Critical Activities:
— Allocate Hazards & Risks to System Functions
— Perform Functional FMEA
— Analyze Reliability-Based Failures
— Analyze User/Operator Induced Failures
— Determine Req'd Failure Mitigations
— Perform FTA/ETA on System & Operating Environment
— Identify & Analyze Event-Based Dysfunctions
— Identify & Analyze Common Cause Events
— Determine Req'd Event & Common Cause Mitigations
— Recommend Risk-Safety-Hazard Based Req'ts Updates

Provide Technology & Engineering Analysis Support

Critical Activities:
— Analyze System Functions for Implementation Feasibility
— Analyze System Req'ts for Feasibility
— Analyze Req'ts Verification Approaches for Feasibility

Specialty Engineer

Specialty engineers perform these actions in sync with SE actions in order to satisfy the req'ts of ISO 14971 paragraph 4.4.

Stakeholders review req'ts analysis & management products under the leadership of systems engineers as per ISO 15288 6.4.2.3.

Device Designer/Developer

Design engineers perform these actions for the assessment and analysis of req'ts feasibility.
Outcomes from ISO 15288 Technical Process 6.4.2 Requirements Analysis:
--- Required characteristics, attributes, and functional & performance req'ts are specified
--- Constraints on the architecture and the solution implementing the architecture are specified
--- The integrity & traceability of system req'ts to Stakeholder needs is achieved
--- The basis for verifying that requirements are satisfied is defined
System Req'ts Risk-Driven Activity Flow

1. Define System Functional Boundaries
2. Define System Functions
3. Define Stakeholder Constraints
4. Allocate Stakeholder Req'ts to Functions
5. Analyze Allocated Stakeholder Req'ts
6. Define Technology Feasibility Constraints
7. Define Design Feasibility Constraints
8. Allocate Hazards & Risks to System Functions
9. Analyze Reliability-Based Failures
10. Analyze User/Operator Induced Failures
11. Analyze System Functions for Implementation Feasibility
- Establish Req'ts Traceability to Stakeholder Needs
- Evaluate Traceability of System Req'ts to Stakeholder Needs
- Evaluate Suitability of System Req'ts to Satisfy Stakeholder Needs
- Assess Completeness of System Req'ts Relative to Stakeholder Needs
- Resolve Req'ts Conflicts
- Resolve Stakeholder Comments & Revisions
- Publish System Req'ts

E stablish Req'ts Traceability to Stakeholder Needs
R esolve Req'ts Conflicts
R esolve Stakeholder Comments & Revisions
P ublish System Req'ts
Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Process Model 3 – 6.4.3 Architecture Development Process
Outcomes from ISO 15288 Technical Process 6.4.3 Architectural Design Process:
- Architecture baseline established
- System element descriptions to satisfy requirements are specified
- Interface requirements are incorporated into the architecture
- Basis for verifying system elements is defined
- Basis for integrating system elements is defined

Stakeholders review the architecture and the allocation of requirements to architecture elements to ensure that traceability to stakeholder needs and constraints is fully satisfactory.

Specialty engineers perform these actions in sync with SE and Design actions in order to satisfy the requirements of ISO 14971 paragraphs 5.0, 6.2, and 6.2.

Design engineers perform these actions to support LSA development and to fulfill key requirements of ISO 15288 paragraph 6.4.3.

Stakeholders review the architecture and the allocation of requirements to architecture elements to ensure that traceability to stakeholder needs and constraints is fully satisfactory.

See separate, more detailed elaboration of systems engineering actions that shows how all requirements of ISO 15288 6.4.3 are satisfied.

Specialty engineers perform these actions in sync with SE and Design actions in order to satisfy the requirements of ISO 14971 paragraphs 5.0, 6.2, and 6.2.

Design engineers perform these actions to support LSA development and to fulfill key requirements of ISO 15288 paragraph 6.4.3.

Specialty engineers perform these actions in sync with SE and Design actions in order to satisfy the requirements of ISO 14971 paragraphs 5.0, 6.2, and 6.2.
Develop System Architecture

- Define Logical System Architecture (LSA)
  - Analyze Use Cases to Define Human Roles
  - Allocate System Functions to Allocate Human vs System
  - Analyze Req'ts to Derive LSA Element Req'ts
  - Define and Analyze LSA Internal & External Interfaces
  - Analyze Req'ts Input and Traceability
  - Document LSA & LSA Req'ts

- Analyze Human-Systems Integration
  - Analyze System Functions to Allocate Human vs System
  - Analyze LSA to Identify Human-System Interactions & Interfaces
  - Analyze LSA Req'ts to Define Req'ts for Human Actions

- Develop System Physical Architecture
  - Define Physical Architecture Options
  - Analyze Physical Element Specs Against Req'ts
  - Analyze Physical Interface Specs Against Req'ts
  - Analyze Physical Element Verification Methods
  - Update Physical Element Req'ts to Improve Risk Control

- Develop Third Level Assurance Case Elements
  - Analyze LSA to Develop Second Level Claim Strategies
  - Decompose Second Level Claims to Third Level LSA-based Claims
  - Evaluate Risk Analyses to Define Third Level Evidence Needs
  - Update LSA Req'ts to Improve Risk Control
  - Align Third Level Claims/Evidence to Physical Arch
  - Evaluate Physical Element Specs Against Evidence Needs
  - Update Specs & Verification Approaches
  - Update Physical Element Req'ts to Improve Risk Control

- Document Architecture & System Specifications
  - Integrate Quality Measures & Verification Methods
  - Integrate Logical & Physical Architecture Descriptions
  - Document Traceability of LSA Req'ts & Physical Element Specs
  - Analyze Human-Systems Integration
  - Group Functions into Logical Design Elements
  - Define Logical System Architecture (LSA)

MBSE Details for System Architecture Development

- Develop Third Level Assurance Case Elements
  - Analyze LSA to Develop Second Level Claim Strategies
  - Decompose Second Level Claims to Third Level LSA-based Claims
  - Evaluate Risk Analyses to Define Third Level Evidence Needs
  - Update LSA Req'ts to Improve Risk Control
  - Align Third Level Claims/Evidence to Physical Arch
  - Evaluate Physical Element Specs Against Evidence Needs
  - Update Specs & Verification Approaches
  - Update Physical Element Req'ts to Improve Risk Control

- Document Architecture & System Specifications
  - Integrate Quality Measures & Verification Methods
  - Integrate Logical & Physical Architecture Descriptions
  - Document Traceability of LSA Req'ts & Physical Element Specs

- Analyze Human-Systems Integration
  - Analyze System Functions to Allocate Human vs System
  - Analyze LSA to Identify Human-System Interactions & Interfaces
  - Analyze LSA Req'ts to Define Req'ts for Human Actions

- Develop System Physical Architecture
  - Define Physical Architecture Options
  - Analyze Physical Element Specs Against Req'ts
  - Analyze Physical Interface Specs Against Req'ts
  - Analyze Physical Element Verification Methods
  - Update Physical Element Req'ts to Improve Risk Control

- Develop Third Level Assurance Case Elements
  - Analyze LSA to Develop Second Level Claim Strategies
  - Decompose Second Level Claims to Third Level LSA-based Claims
  - Evaluate Risk Analyses to Define Third Level Evidence Needs
  - Update LSA Req'ts to Improve Risk Control
  - Align Third Level Claims/Evidence to Physical Arch
  - Evaluate Physical Element Specs Against Evidence Needs
  - Update Specs & Verification Approaches
  - Update Physical Element Req'ts to Improve Risk Control

- Document Architecture & System Specifications
  - Integrate Quality Measures & Verification Methods
  - Integrate Logical & Physical Architecture Descriptions
  - Document Traceability of LSA Req'ts & Physical Element Specs

- Analyze Human-Systems Integration
  - Analyze System Functions to Allocate Human vs System
  - Analyze LSA to Identify Human-System Interactions & Interfaces
  - Analyze LSA Req'ts to Define Req'ts for Human Actions

- Develop System Physical Architecture
  - Define Physical Architecture Options
  - Analyze Physical Element Specs Against Req'ts
  - Analyze Physical Interface Specs Against Req'ts
  - Analyze Physical Element Verification Methods
  - Update Physical Element Req'ts to Improve Risk Control

- Develop Third Level Assurance Case Elements
  - Analyze LSA to Develop Second Level Claim Strategies
  - Decompose Second Level Claims to Third Level LSA-based Claims
  - Evaluate Risk Analyses to Define Third Level Evidence Needs
  - Update LSA Req'ts to Improve Risk Control
  - Align Third Level Claims/Evidence to Physical Arch
  - Evaluate Physical Element Specs Against Evidence Needs
  - Update Specs & Verification Approaches
  - Update Physical Element Req'ts to Improve Risk Control

- Document Architecture & System Specifications
  - Integrate Quality Measures & Verification Methods
  - Integrate Logical & Physical Architecture Descriptions
  - Document Traceability of LSA Req'ts & Physical Element Specs

- Analyze Human-Systems Integration
  - Analyze System Functions to Allocate Human vs System
  - Analyze LSA to Identify Human-System Interactions & Interfaces
  - Analyze LSA Req'ts to Define Req'ts for Human Actions

- Develop System Physical Architecture
  - Define Physical Architecture Options
  - Analyze Physical Element Specs Against Req'ts
  - Analyze Physical Interface Specs Against Req'ts
  - Analyze Physical Element Verification Methods
  - Update Physical Element Req'ts to Improve Risk Control

- Develop Third Level Assurance Case Elements
  - Analyze LSA to Develop Second Level Claim Strategies
  - Decompose Second Level Claims to Third Level LSA-based Claims
  - Evaluate Risk Analyses to Define Third Level Evidence Needs
  - Update LSA Req'ts to Improve Risk Control
  - Align Third Level Claims/Evidence to Physical Arch
  - Evaluate Physical Element Specs Against Evidence Needs
  - Update Specs & Verification Approaches
  - Update Physical Element Req'ts to Improve Risk Control

- Document Architecture & System Specifications
  - Integrate Quality Measures & Verification Methods
  - Integrate Logical & Physical Architecture Descriptions
  - Document Traceability of LSA Req'ts & Physical Element Specs
Outcomes from ISO 15288 Technical Process 6.4.3 Architectural Design Process:
- Architecture baseline established
- System element descriptions to satisfy requirements are specified
- Interface requirements are incorporated into the architecture
- Basis for verifying system elements is defined
- Basis for integrating system elements is defined

MagicDraw, 1-1 C:\AA05-Holdin\INCOSE Biomed MBSE Challenge\AA03-Use cases for MBSE model\02-MBSE & Haz-Safety U_C\Risk-Safety-Life_Cycle (v2_}
- Develop & Analyze Risk Control Implementation Designs
- Analyze & Model Physical Architecture Performance
- Select & Recommend Physical Element Designs

- Analyze LSA Reqts to Derive Physical Element Specs
- Evaluate Risk Analyses to Define Third Level Evidence Needs

- Analyze Physical Element Specs Against Reqts
- Analyze Physical Interface Specs Against Reqts

- Analyze Physical Element Verification Methods
- Integrate Quality Measures & Verification Methods

- Evaluate Physical Element Specs Against Risk Control Needs
- Map LSA Risks-Hazards to Physical Elements
- Re-evaluate Probability Consequence Analyses

- Evaluate Risk Controls Within Each Physical Element
- Recommend Physical Design Risk Control Updates
Integrate Logical & Physical Architecture Designs

Evaluate Physical Architecture Against Needs & Constraints

Document Traceability of LSA Reqts & Physical Element Specs

Align Third Level Claims/Evidence to Physical Arch

Evaluate Physical Element Specs Against Evidence Needs

Update Physical Element Reqts to Improve Risk Control

Update Specs & Verification Approaches

Evaluate Physical Architecture Against Needs & Constraints
Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Process Model 4 – 6.4.4 System Implementation Process
Outcomes from ISO 15288 Technical Process 6.4.4 Implementation Process:
- Implementation strategy defined
- Implementation technology constraints identified
- System elements realized
- System element packaged and stored in accordance with agreement for its supply
Implement Device Design and Risk Controls

- Define & Analyze Implementation Options
  - Evaluate Make, Buy, Reuse System Elements
  - Define Procedures, Processes, Tools, Equipment
  - Define Risk Control Implementations
  - Define Verification Values and Processes
  - Analyze Strategies Against Req'ts Verification

- Select Implementation Strategies
  - Define Procedures, Processes, Tools, Equipment
  - Define Risk Control Implementations
  - Define Verification Values and Processes
  - Analyze Strategies Against Req'ts Verification

- Realize Hardware and Software
  - Implement Risk Control Designs
  - Develop Risk Control Verification Data
  - Compare Implementation to Req'ts

- Realize Risk Control Implementations
  - Implement Human Systems Risk Mitigations
  - Define and Create Operator Training
  - Deploy Operator Training
  - Confirm Operator Training Effectiveness

- Realize Human Systems Risk Mitigations & Controls
  - Define Procedures, Processes, Tools, Equipment
  - Define Verification Values and Processes
  - Analyze Strategies Against Req'ts Verification

- Update Elements to Achieve Risk Control Goals
- Compile Implementation Data
- Compile Verification Data
Outcomes from ISO 15288 Technical Process 6.4.4 Implementation Process:
--- Implementation strategy defined
--- Implementation technology constraints identified
--- System elements realized
--- System element packaged and stored in accordance with agreement for its supply

MagicDraw, 1-1 C:\AA05-Holding\INCOSE Biomed MBSE Challenge\AA03-Use cases for MBSE model\02-MBSE & Haz-Safety U_C\Risk-Safety-Life_Cycle (v2_0