25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

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

Presented by
Bob Malins
President, Eagle Summit Technology Associates, Inc.
rjmalins@eaglesummittech.com

About the Authors

Dr. Robert J. Malins

- Founder and Owner, Eagle Summit Technology Associates, Inc.
- Systems engineering, architecture and concept development

Jack Stein

- Director and Systems Engineer, DSI, Inc. (non-profit).
- Co-Chair, INCOSE Risk Management Working Group
- INCOSE Asst. Director, Americas Sector (North-Central Region)

Dr. Ajay Thukral

- Chief Technology Officer, Cientive Group, Indianapolis, IN
- Mathematical analysis and engineering modeling team leader

Christophe Waterplas

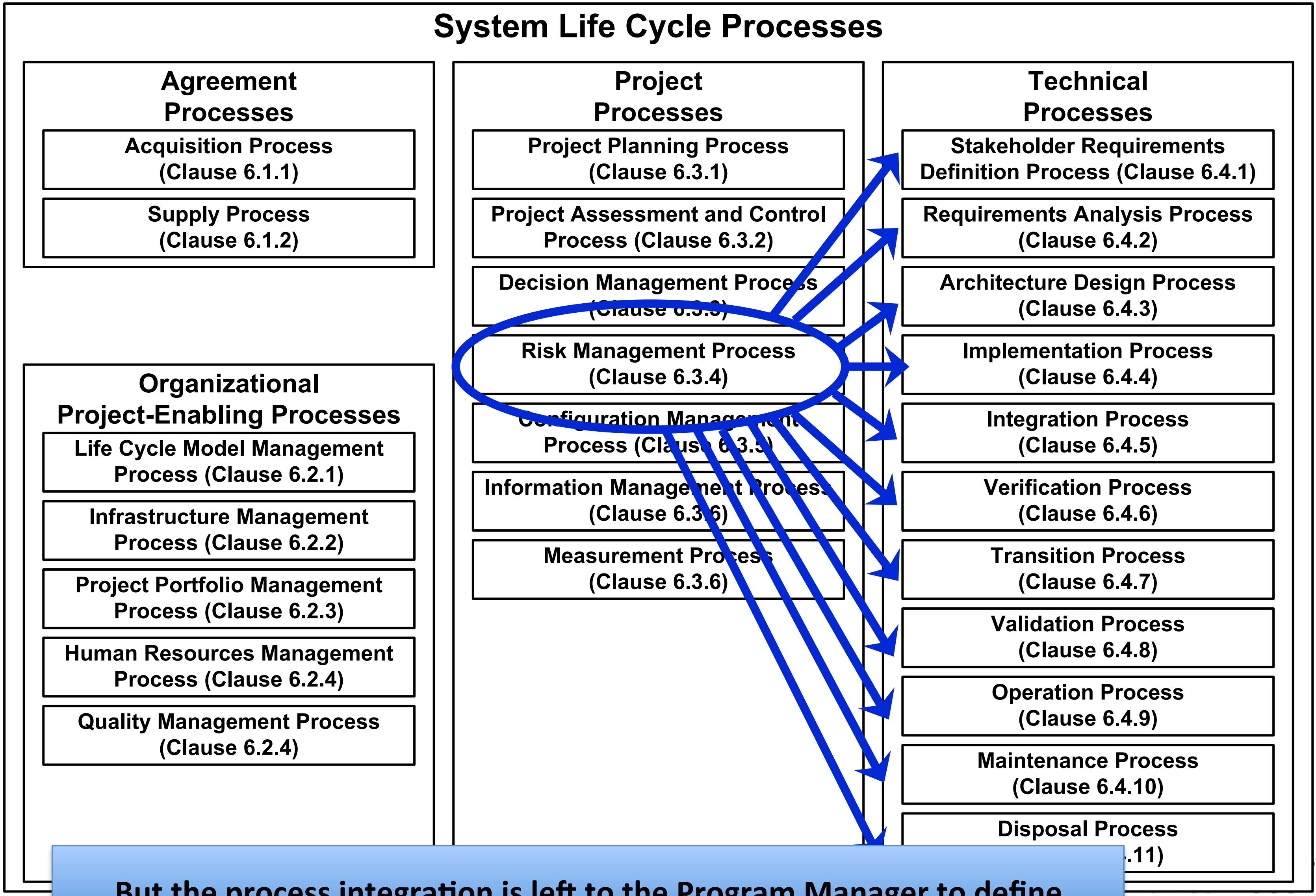
- Lead Systems Engineer, ResMed, Ltd., Australia
- Risk management, usability engineering and alarm systems

Bottom Line Up Front

- ISO 15288 and ISO 14971 can be integrated to form a risk-driven development process for medical devices
- Assurance case development can also be integrated into the process to leverage the risk management activities required by ISO 14971
- SysML modeling techniques can be used to clarify the specific steps in the integrated process

ISO 15288 System and Software Engineering – System Life Cycle Processes
ISO 14971 Medical Device Risk and Safety Management

The Problem (Part 1)



System Life Cycle Processes

Agreement Processes

Acquisition Process (Clause 6.1.1)

Supply Process (Clause 6.1.2)

Organizational Project-Enabling Processes

Life Cycle Model Management Process (Clause 6.2.1)

Infrastructure Management Process (Clause 6.2.2)

Project Portfolio Management Process (Clause 6.2.3)

Human Resources Management Process (Clause 6.2.4)

Quality Management Process (Clause 6.2.4)

Project Processes

Project Planning Process (Clause 6.3.1)

Project Assessment and Control Process (Clause 6.3.2)

Decision Management Process (Clause 6.3.3)

Risk Management Process (Clause 6.3.4)

Configuration Management Process (Clause 6.3.5)

Information Management Process (Clause 6.3.6)

Measurement Process (Clause 6.3.6)

Technical Processes

Stakeholder Requirements Definition Process (Clause 6.4.1)

Requirements Analysis Process (Clause 6.4.2)

Architecture Design Process (Clause 6.4.3)

Implementation Process (Clause 6.4.4)

Integration Process (Clause 6.4.5)

Verification Process (Clause 6.4.6)

Transition Process (Clause 6.4.7)

Validation Process (Clause 6.4.8)

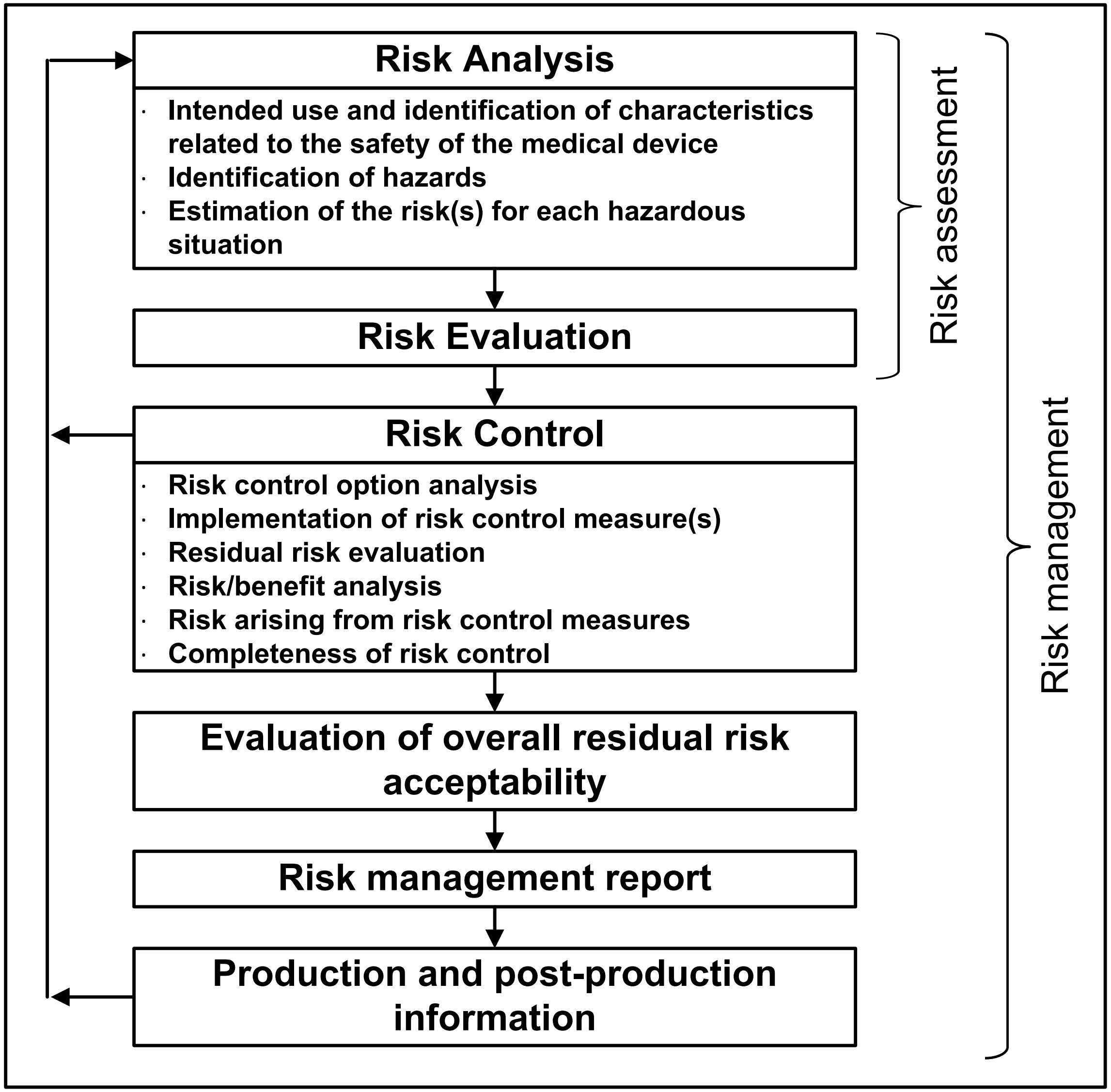
Operation Process (Clause 6.4.9)

Maintenance Process (Clause 6.4.10)

Disposal Process .11)

But the process integration is left to the Program Manager to define

The Problem (Part 2)



Risk Analysis

- Intended use and identification of 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
- Risk arising from risk control measures
- Completeness of risk control

Evaluation of overall residual risk acceptability

Risk management report

Production and post-production information

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

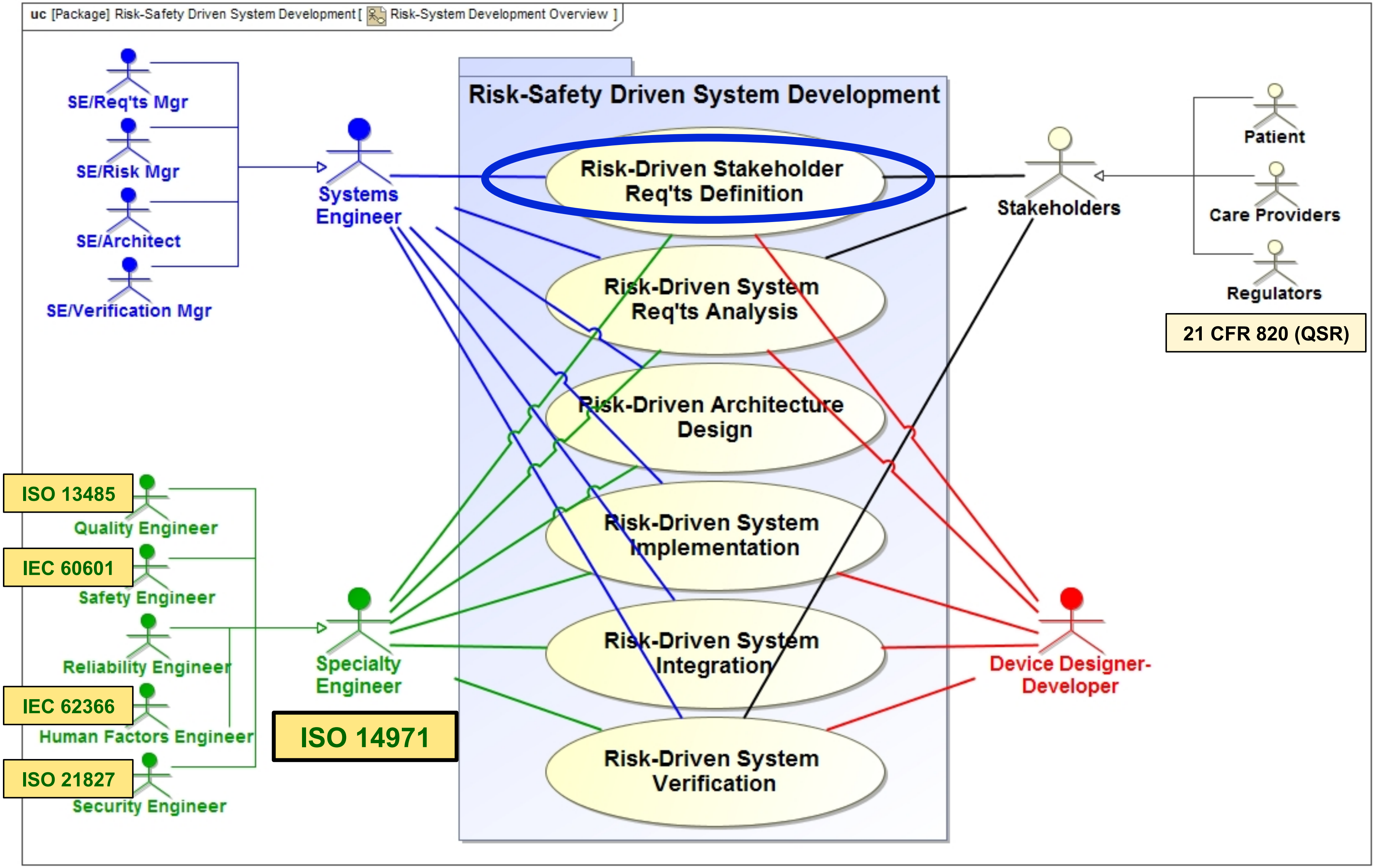
The steps in risk management do not conveniently line up with the steps in device development

Program Managers need a well defined process to integrate these risk management actions into each of the ISO 15288 technical processes

(Summary of our model development process)

SYSML MODELING FOR PROCESS INTEGRATION

MBSE for Process Integration


uc [Package] Risk-Safety Driven System Development [Risk-System Development Overview]
SE/Req'ts Mgr
SE/Risk Mgr
SE/Architect
SE/Verification Mgr
Systems Engineer
Risk-Safety Driven System Development
Risk-Driven Stakeholder Req'ts Definition
Risk-Driven System Req'ts Analysis
Risk-Driven Architecture Design
Risk-Driven System Implementation
Risk-Driven System Integration
Risk-Driven System Verification
Stakeholders
Patient
Care Providers
Regulators
21 CFR 820 (QSR)
ISO 13485
Quality Engineer
IEC 60601
Safety Engineer
Reliability Engineer
IEC 62366
Human Factors Engineer
ISO 21827
Security Engineer
Specialty Engineer
ISO 14971
Device Designer-Developer

Step 1: Understand Process Req’ts

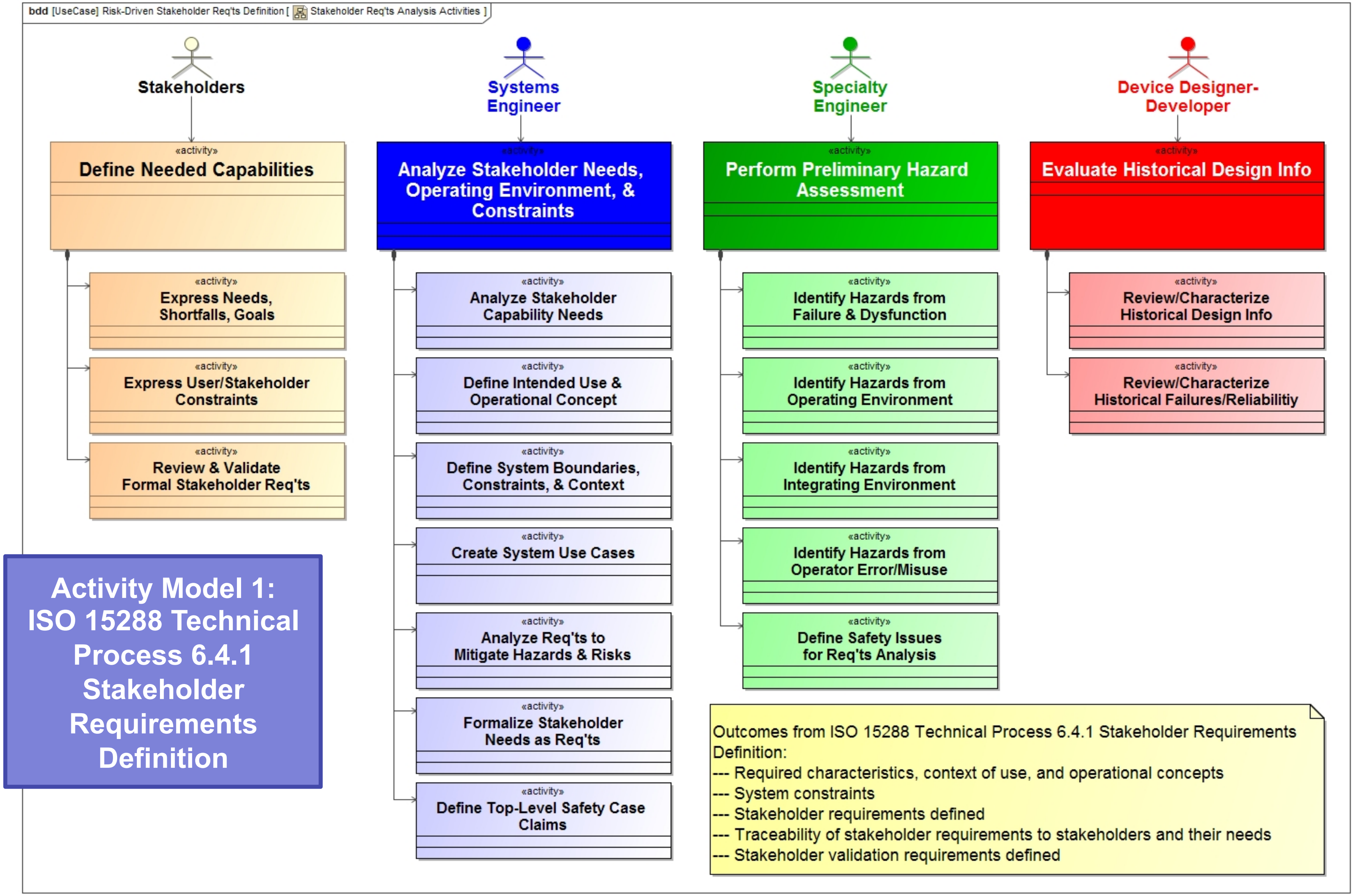
- Analyze the standards using ISO 15288 as the key

Example Analysis for Technical Process 6.4.1

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

Blue font represents output from risk management and/or safety case development that is input to the 15288 technical process. Green font represents the impact on 15288 of risk management and safety case input.

Step 2: Process Activities



bdd [UseCase] Risk-Driven Stakeholder Req'ts Definition [Stakeholder Req'ts Analysis Activities]

Stakeholders

«activity» Define Needed Capabilities

- «activity» Express Needs, Shortfalls, Goals
- «activity» Express User/Stakeholder Constraints
- «activity» Review & Validate Formal Stakeholder Req'ts

Systems Engineer

«activity» Analyze Stakeholder Needs, Operating Environment, & Constraints

- «activity» Analyze Stakeholder Capability Needs
- «activity» Define Intended Use & Operational Concept
- «activity» Define System Boundaries, Constraints, & Context
- «activity» Create System Use Cases
- «activity» Analyze Req'ts to Mitigate Hazards & Risks
- «activity» Formalize Stakeholder Needs as Req'ts
- «activity» Define Top-Level Safety Case Claims

Specialty Engineer

«activity» Perform Preliminary Hazard Assessment

- «activity» Identify Hazards from Failure & Dysfunction
- «activity» Identify Hazards from Operating Environment
- «activity» Identify Hazards from Integrating Environment
- «activity» Identify Hazards from Operator Error/Misuse
- «activity» Define Safety Issues for Req'ts Analysis

Device Designer-Developer

«activity» Evaluate Historical Design Info

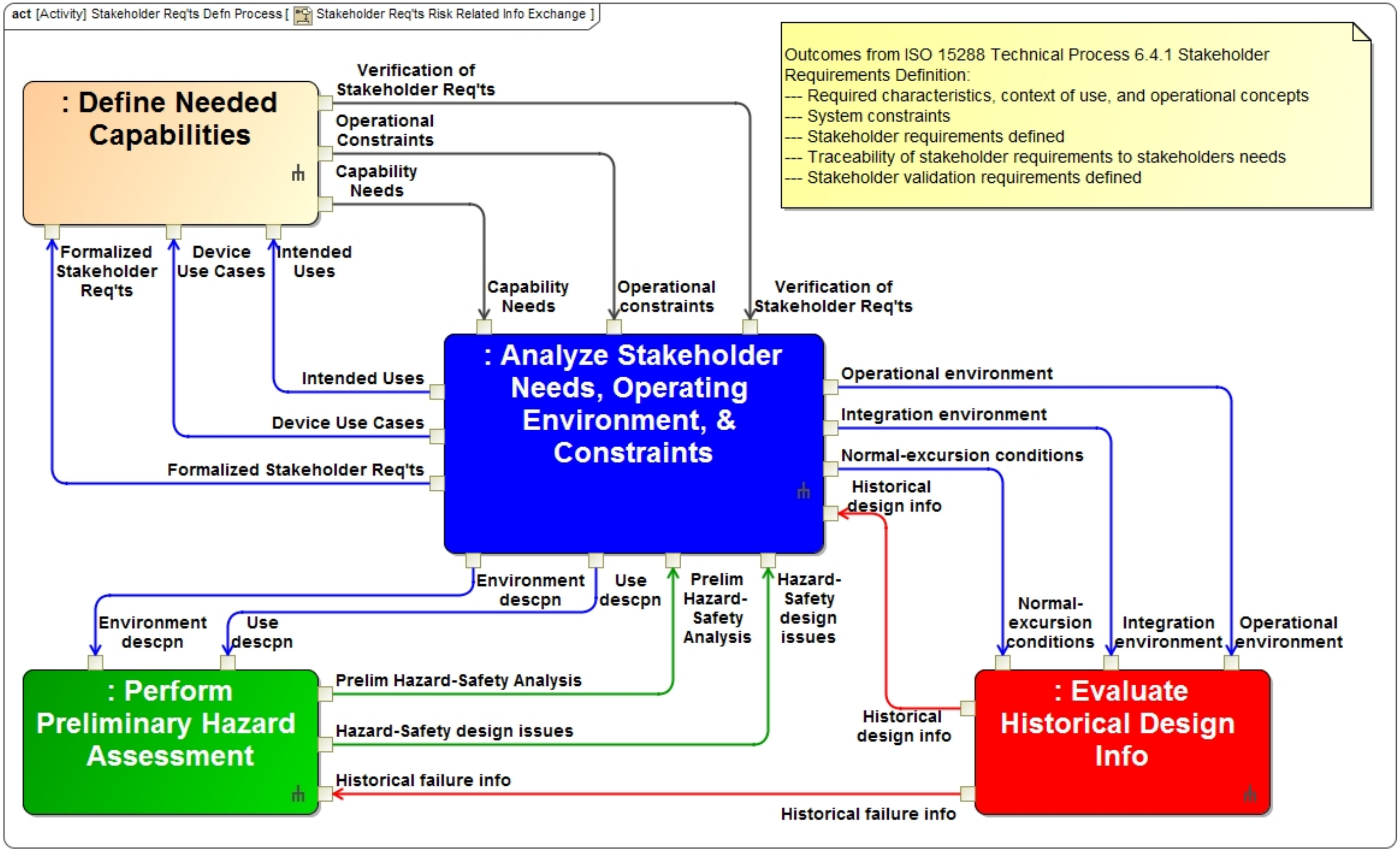
- «activity» Review/Characterize Historical Design Info
- «activity» Review/Characterize Historical Failures/Reliabilitiy

Activity Model 1: ISO 15288 Technical Process 6.4.1 Stakeholder Requirements 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

m

Step 3: Information Flow



act [Activity] Stakeholder Req'ts Defn Process [Stakeholder Req'ts Risk Related Info Exchange]

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 needs
--- Stakeholder validation requirements defined

: Define Needed Capabilities

Verification of Stakeholder Req'ts

Operational Constraints

Capability Needs

Formalized Stakeholder Req'ts

Device Use Cases

Intended Uses

Capability Needs

Operational constraints

Verification of Stakeholder Req'ts

: Analyze Stakeholder Needs, Operating Environment, & Constraints

Intended Uses

Device Use Cases

Formalized Stakeholder Req'ts

Operational environment

Integration environment

Normal-excursion conditions

Historical design info

Environment descpn

Use descpn

Prelim Hazard-Safety Analysis

Hazard-Safety design issues

Environment descpn

Use descpn

Normal-excursion conditions

Integration environment

Operational environment

: Perform Preliminary Hazard Assessment

Prelim Hazard-Safety Analysis

Hazard-Safety design issues

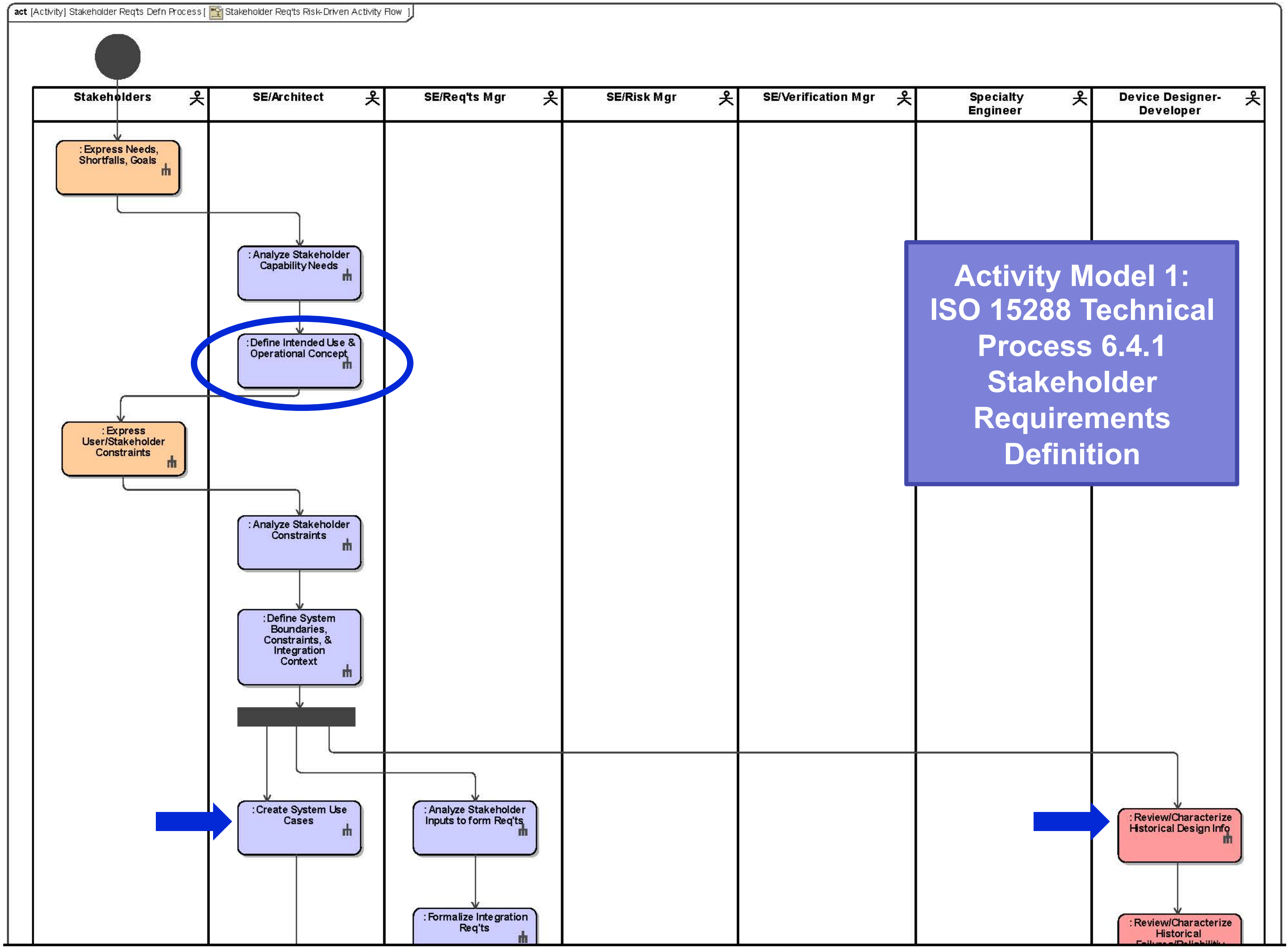
Historical failure info

Historical design info

: Evaluate Historical Design Info

Historical failure info

Step 4: Model Activity Flow



act [Activity] Stakeholder Req'ts Defn Process [Stakeholder Req'ts Risk-Driven Activity Flow]

Stakeholders

SE/Architect

SE/Req'ts Mgr

SE/Risk Mgr

SE/Verification Mgr

Specialty Engineer

Device Designer-Developer

: 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

: Review/Characterize Historical Design Info

: Review/Characterize Historical Failures/Reliability

Activity Model 1: ISO 15288 Technical Process 6.4.1 Stakeholder Requirements Definition

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_(

(A brief diversion)

SAFETY ASSURANCE CASES

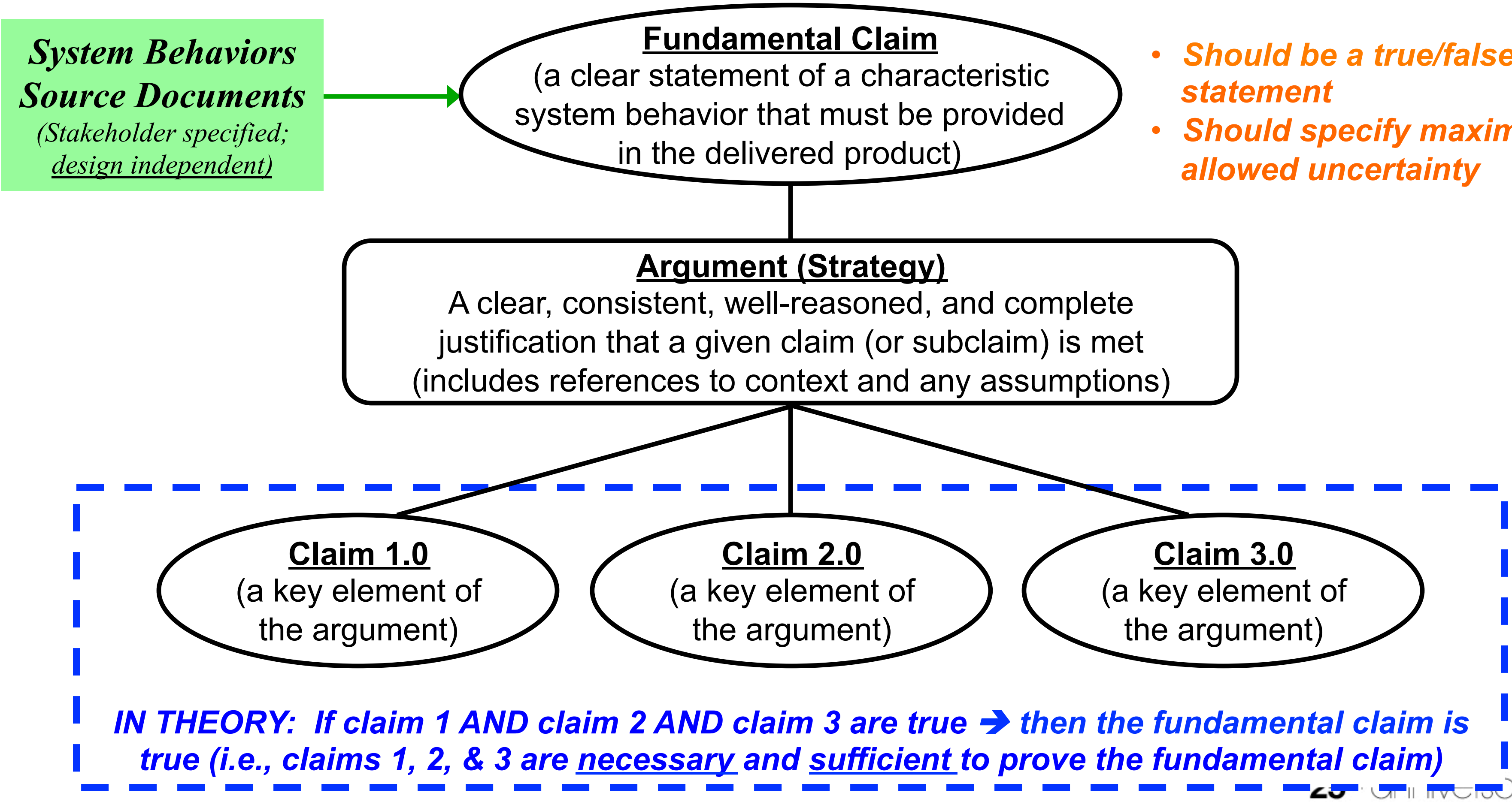
The Assurance Case Concept

- Definition
  - The Safety (*Assurance*) Case shall consist of a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for (*will demonstrate desired behavior in*) a given application in a given environment.
    - UK MOD Defense Standard 00-56 Part 1
- A Safety Assurance Case maps out ***the reasoning*** behind system safety verification
  - Structures the discussion of requirements-argument-evidence
  - Ties specific verification data to specific safety claims
  - Creates a framework for evaluating confidence in the claims

A safety case structures design, analysis, and testing information to enable evaluation of confidence that the system will behave safely in operational environment

How Assurance Cases Work

- An assurance case is a structured argument



System Behaviors Source Documents
(Stakeholder specified; <u>design independent)</u>

<u>Fundamental Claim</u>
(a clear statement of a characteristic system behavior that must be provided in the delivered product)

- ***Should be a true/false statement***
- ***Should specify maximum allowed uncertainty***

<u>Argument (Strategy)</u>
A clear, consistent, well-reasoned, and complete justification that a given claim (or subclaim) is met (includes references to context and any assumptions)

<u>Claim 1.0</u>
(a key element of the argument)

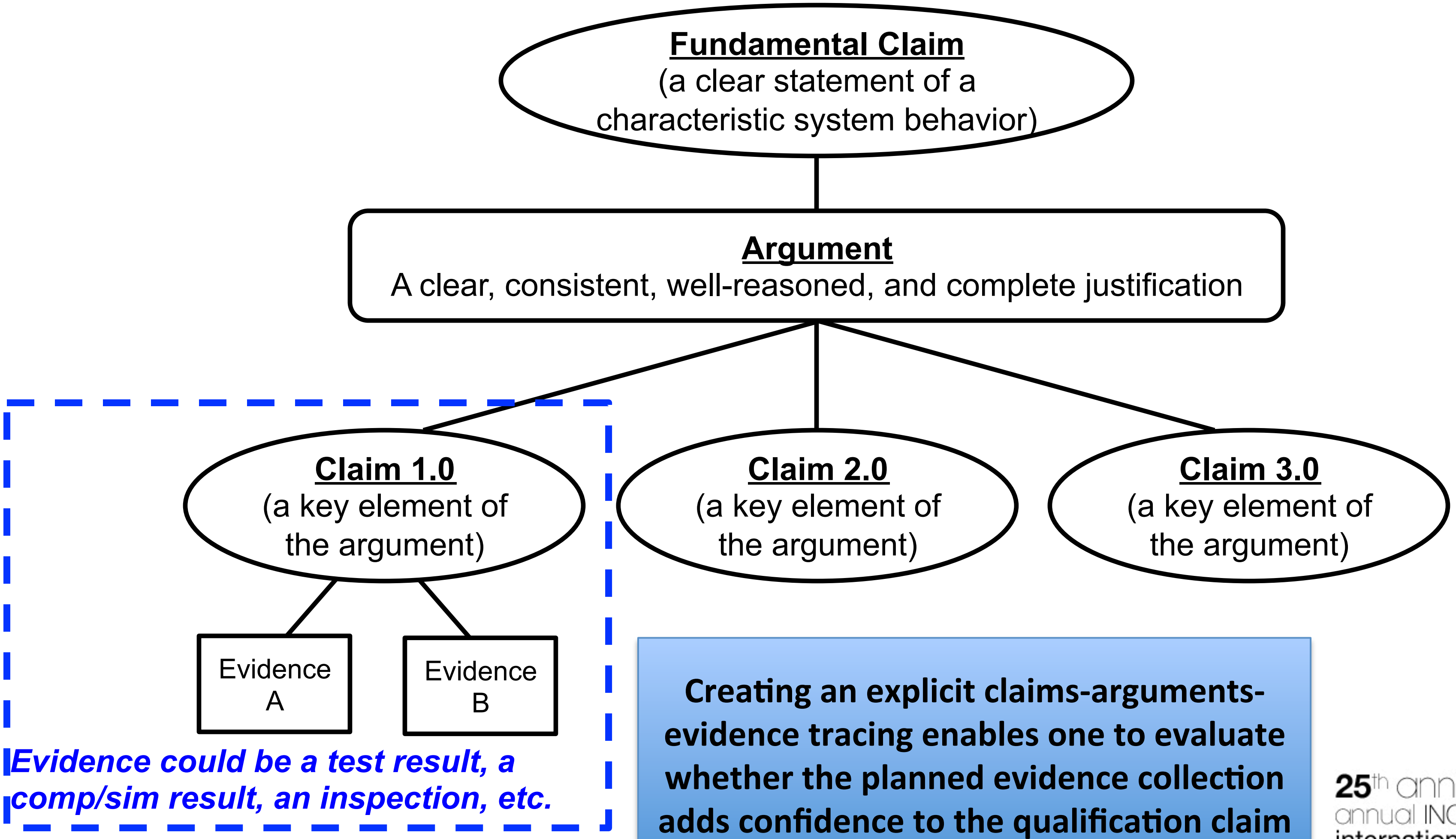
<u>Claim 2.0</u>
(a key element of the argument)

<u>Claim 3.0</u>
(a key element of the argument)

IN THEORY: If claim 1 AND claim 2 AND claim 3 are true → then the fundamental claim is true (i.e., claims 1, 2, & 3 are <u>necessary</u> and <u>sufficient</u> to prove the fundamental claim)

Assurance Cases and Evidence

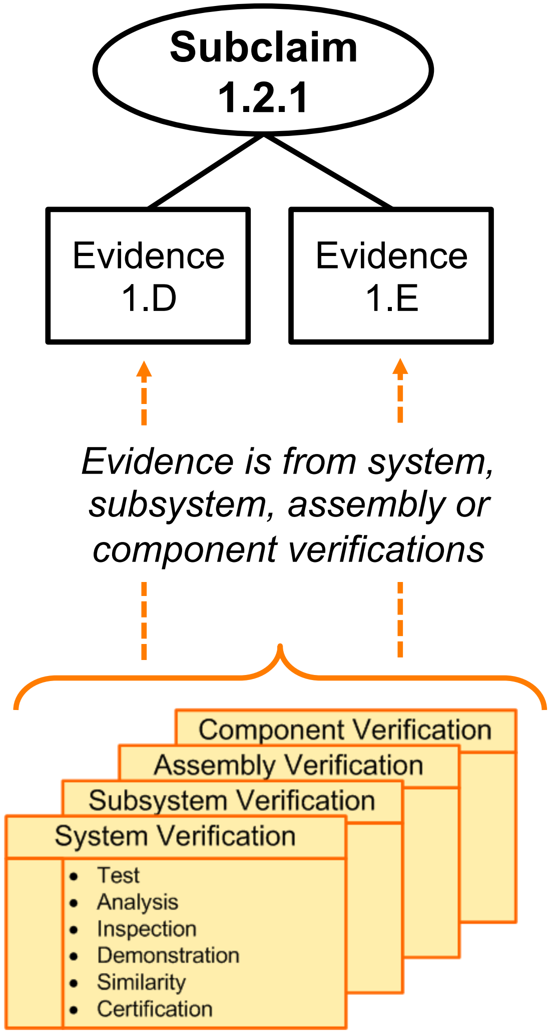
- Evidence is the final step in the assurance case


Fundamental Claim
(a clear statement of a characteristic system behavior)
Argument
A clear, consistent, well-reasoned, and complete justification
Claim 1.0
(a key element of the argument)
Claim 2.0
(a key element of the argument)
Claim 3.0
(a key element of the argument)
Evidence A
Evidence B

Evidence could be a test result, a comp/sim result, an inspection, etc.

Creating an explicit claims-arguments-evidence tracing enables one to evaluate whether the planned evidence collection adds confidence to the qualification claim

Residual Risk and Confidence



Subclaim 1.2.1

Evidence 1.D

Evidence 1.E

Evidence is from system, subsystem, assembly or component verifications

Component Verification

Assembly Verification

Subsystem Verification

System Verification

- Test
- Analysis
- Inspection
- Demonstration
- Similarity
- Certification

- Confidence assessment methodology:
  - Is there a situation or set of conditions under which Evidence is true, but Claim is false?
  - What is the probability that such conditions occur, given what we know?
  - What is the consequence to the system if Claim becomes false?

Consequence					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	M	M	M
1	L	L	L	L	L
	1	2	3	4	5

Likelihood

Residual Risk

  - Will additional testing or analyses provide new evidence lowering the probability estimate?
  - Are there mitigations (design or procedural) that would limit the consequences?

(What we learned from building the model)

IMPLEMENTING SAFETY CASES

Safety Case Implementation (1 of 6)

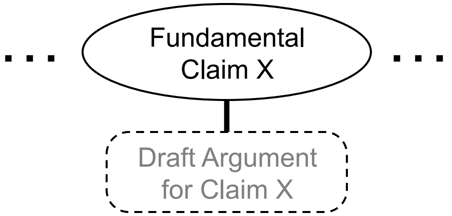
Activity Model 1: ISO 15288 Technical Process 6.4.1 Stakeholder Requirements Definition

Key Development Actions

- Define intended use & use cases
- Define operating & integrating environments
- Define normal & excursion conditions
- Validate above with user review

Key Risk Actions

- Preliminary risk-hazard analyses
- Review historical risk-failure data
- Verify risks-hazards with stakeholders
- Risk control input to req'ts development



- Assurance Case Actions
  - Using preliminary risk-hazard analysis, group hazards into major categories for evaluation
  - Define fundamental claim for each hazard category (i.e., top-level claim structure
  - Draft arguments (strategies) for each fundamental claim
  - Provide input on above to user validation review

Safety Case Implementation (2 of 6)

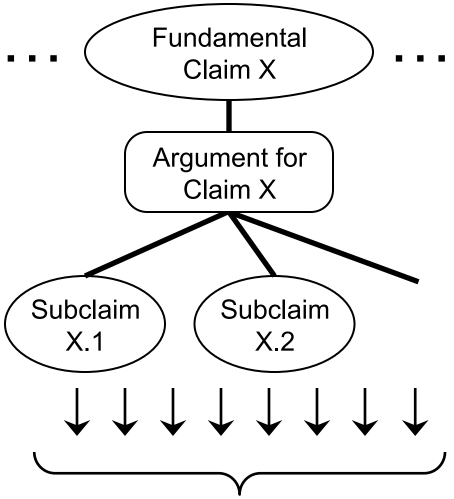
Activity Model 2: ISO 15288 Technical Process 6.4.2 Requirements Analysis Process

Key Development Actions

- Define system boundaries & functions
- Allocate stakeholder needs to functions-define system req'ts
- Define TPMs, quality measures
- Verify system req'ts with user

Key Risk Actions

- Perform functional-FMEA to identify key failure-risk modes
- Identify operator induced risks
- Perform functional FTA/ETA
- Provide Risk control input to TPMs & quality measures



Input to measures and verification planning

- Assurance Case Actions
  - Employ function-based risk analysis results to update arguments (strategies) for each fundamental claim
  - Analyze function-based risk analyses to define second level claims
  - Evaluate function req'ts, TPMs, quality measures
    - Provide input to update TPMs, quality measures
    - Identify new functions needed to implement second level claims
    - Review draft safety assurance case at user review

Safety Case Implementation (3 of 6)

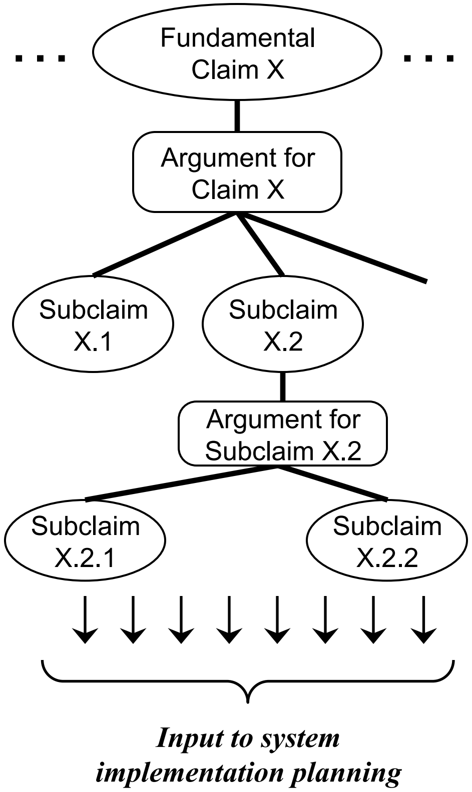
Activity Model 3: ISO 15288 Technical Process 6.4.3 Architectural Design Process

Key Development Actions

- Define logical system architecture
- Evaluate architecture options
- Define internal-external interfaces
- Flow system req’ts to LSA
- Identify human operator roles & usability req’ts

Key Risk Actions

- Update FMEA, FTA, ETA based on LSA elements & details
- Evaluate human-system risks
- Catalog risks (probability, consequence)
- Identify risk control options
- Provide risk control input to LSA



- Assurance Case Actions
  - Evaluate detailed FMEA, FTA, ETA analyses & risk control options to define arguments (strategies) for second level claims
  - Decompose second level claims based on LSA and risk control options – define evidence needs
  - Evaluate risk catalog to assess sufficiency of evidence needs (prepare for residual risk analyses)
  - Provide evidence needs input to system implementation planning

Safety Case Implementation (4 of 6)

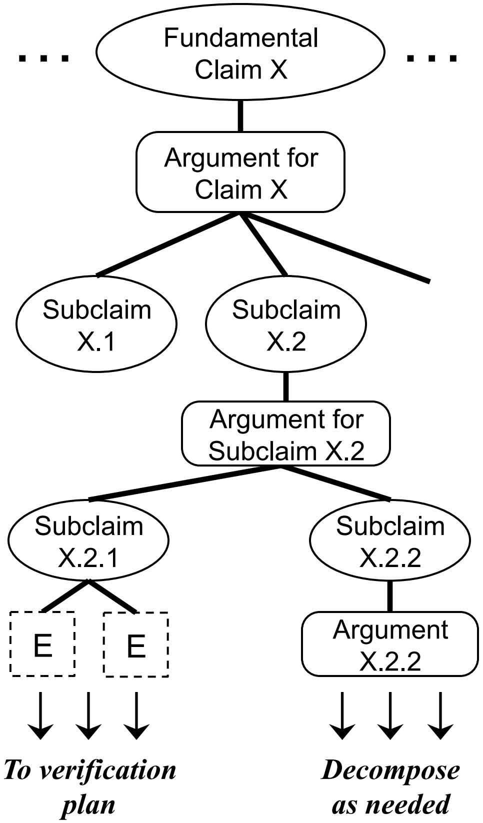
Activity Model 4: ISO 15288 Technical Process 6.4.4 Implementation Process

Key Development Actions

- Define implementation strategy & constraints each LSA element
- Evaluate implementation options
- Select realization LSA elements (H/W, S/W, operator training)
- Define verification each realization

Key Risk Actions

- Evaluate risk control each option
- Incorporate risk control into selected realizations
- Evaluate for new risks
- Evaluate verification data for sufficiency of risk-hazard control



- Assurance Case Actions
  - Evaluate selected realization for sufficiency against second level claims – define third level claims as needed
  - Evaluate risk control options against second/third level claims
  - Evaluate verification data plan against evidence needs
  - Perform initial residual risk analysis against claims – provide updates as need to verification plan

Safety Case Implementation (5 of 6)

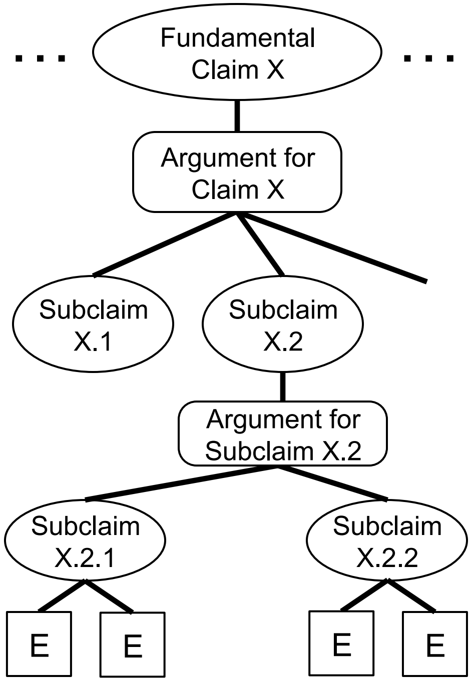
Activity Model 5: ISO 15288 Technical Process 6.4.5 Integration Process

Key Development Actions

- Define integration strategy and constraints
- Obtain elements – assure conformance to req'ts
- Integrate elements – verify conformance/corrective actions

Key Risk Actions

- Update all risk-hazard analyses against achieved performance
- Update residual risk analyses
- Perform risk-benefit analyses
- Evaluate risk control completeness



Consequence					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	M	M	M
1	L	L	L	L	L
	1	2	3	4	5

Likelihood

Integrated Residual Risk

Consequence					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	M	M	M
1	L	L	L	L	L
	1	2	3	4	5

Likelihood

- Assurance Case Actions
  - Evaluate all claims using real data – recommend corrective actions and/or additional verification actions
  - Perform residual risk for each claim – recommend corrective actions and/or additional verification actions
  - Support residual risk and risk-benefit analyses
  - Integrate third ➔ second ➔ fundamental claims and evaluate completeness of risk control

Safety Case Implementation (6 of 6)

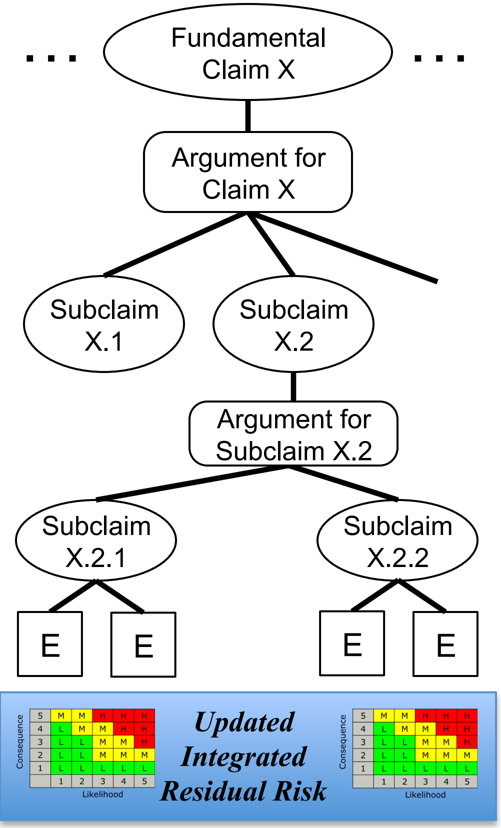
Activity Model 6: ISO 15288 Technical Process 6.4.6 Verification Process

Key Development Actions

- Define verification strategy across the entire life cycle
- Define verification plan
- Conduct verification demos
- Compile/analyze data – record corrective actions

Key Risk Actions

- Employ risk-hazard analyses to create input to verification plan
- Analyze verification data for risk-hazard control
- Update residual risk & risk-benefit analyses – document acceptability
- Finalize risk management files


…

Fundamental Claim X

…

Argument for Claim X

Subclaim X.1

Subclaim X.2

Argument for Subclaim X.2

Subclaim X.2.1

Subclaim X.2.2

E

E

E

E

Consequence					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	M	M	M
1	L	L	L	L	L
	1	2	3	4	5

Likelihood

Updated Integrated Residual Risk

Consequence					
5	M	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	M	M	M
1	L	L	L	L	L
	1	2	3	4	5

Likelihood

- Assurance Case Actions
  - Analyze verification plan against all claims/evidence needs – recommend updates as needed
  - Analyze verification data against all claims
  - Update residual risk for all claims – recommend corrective actions as needed
  - Integrate all analyses and data to document safety assurance case

Process Integration Conclusions

- Risk management across the life cycle
  - Risk analyses begin with stakeholder definition of needs
  - Risk mitigation and control drive system req'ts and architecture
  - Risk control TPMs considered at each step of design
  - Device verification shows performance and safety
- Risk management and safety cases
  - Safety case is hierarchical decomposition of top-level, overarching claims driven by intended use and operational environment
  - Increasing detail of risk analyses drives claims decomposition
  - Strategies to support claims with evidence drives TPMs and verification
  - Very little "new" work beyond risk-hazard analyses of ISO 14971

Questions?

For more information about the SysML model, contact …

Bob Malins

rjmalins@eaglesummittech.com