Reference Architectures and Medical Device Development and Evaluation

Applying Risk-Hazard-Safety Management Across the System Lifecycle

Model working file
October 2014

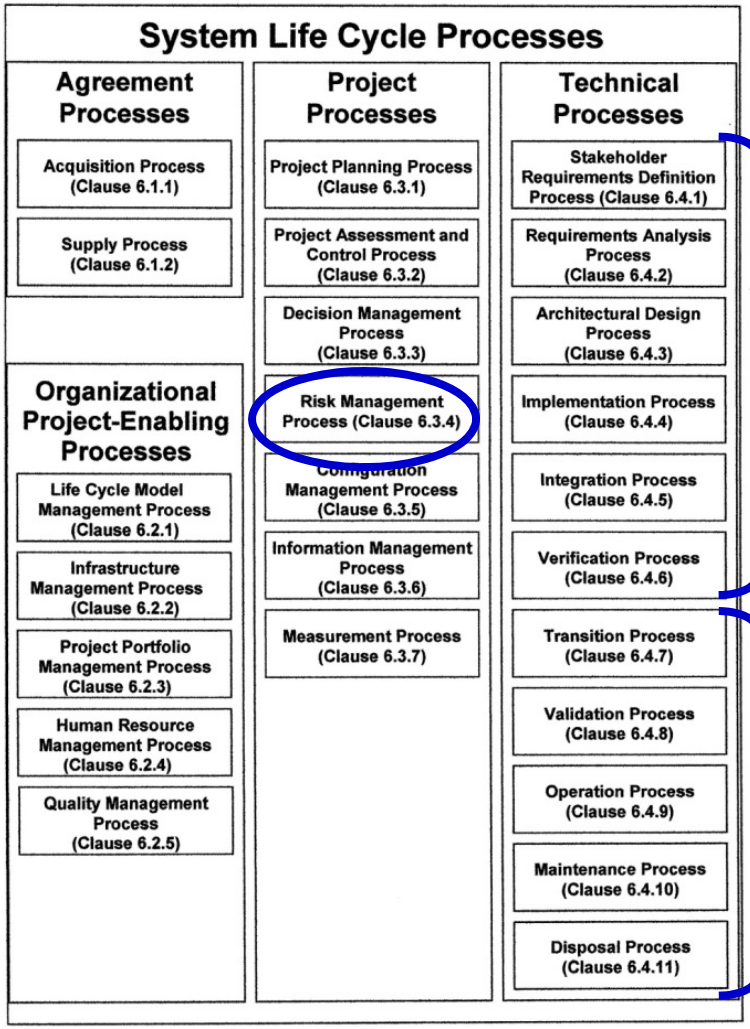
Bob Malins
Eagle Summit Technology Associates, Inc.
505-238-9227
rjmalins@eaglesummittech.com
Model Version 2_0 2014-10-01

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



From ISO 15288:2008 – The System Lifecycle Processes

Device development portion of the life cycle

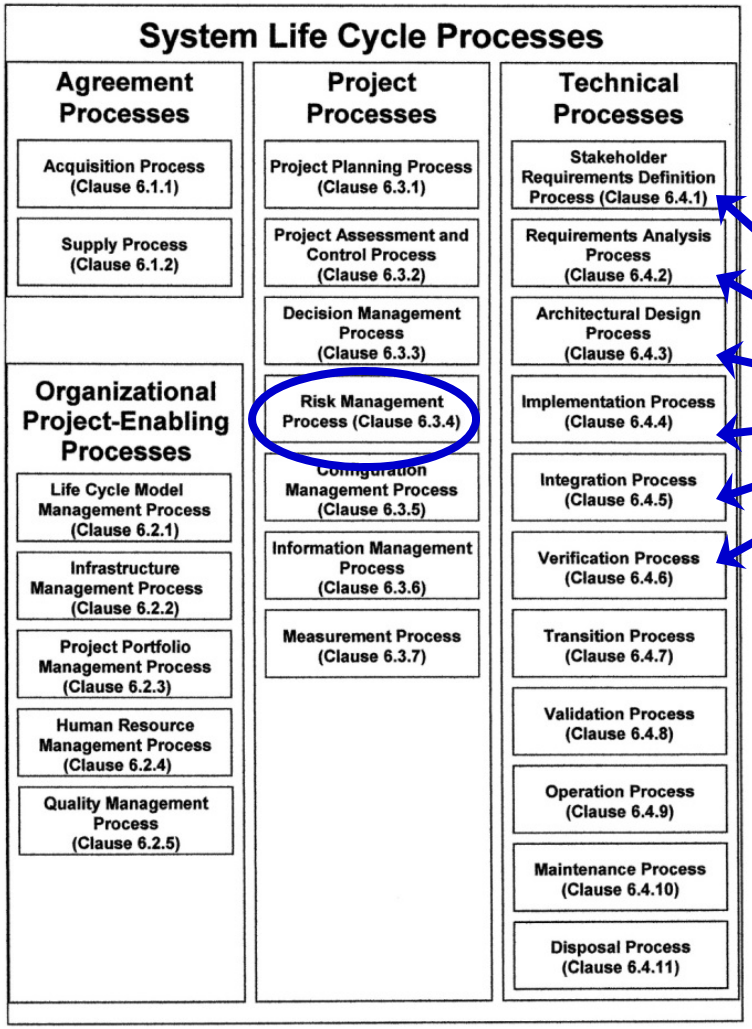
- Near-term objective for INCOSE Biomedical MBSE Challenge Team
- Addressed in the current project and this presentation

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

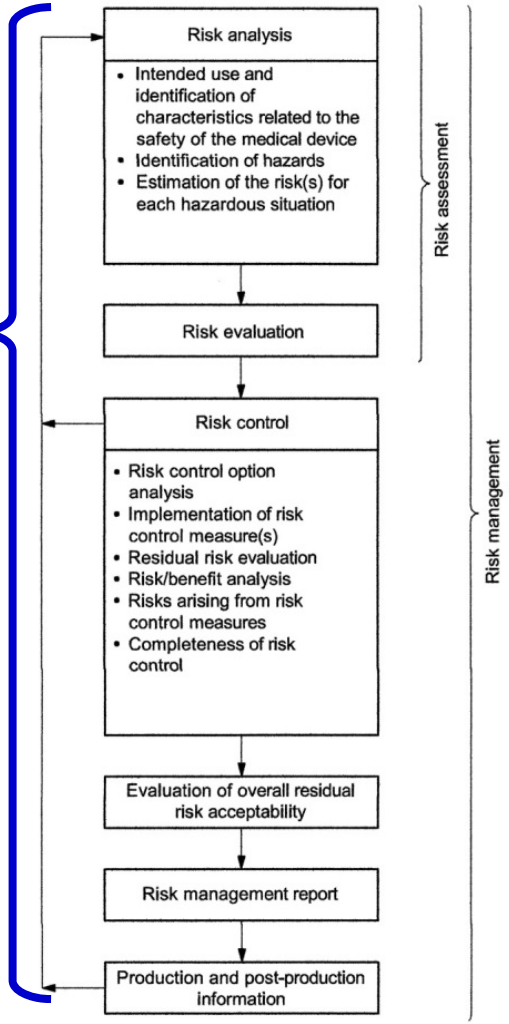
- Includes operations, sustainment, and maintenance within care provider organization
- Includes ultimate device disposal by care provider organization or others
- Possible future work by INCOSE Challenge Team

Project Approach

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



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



From ISO 15288:2008 – The System Lifecycle Processes

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

Applying Risk-Hazard-Safety Management Across the System Lifecycle

Analysis of ISO 15288 Life Cycle Phases in light of ISO 14971 Risk Management Actions and Safety Case Development Process

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

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**
Stakeholder Req'ts Definition Process (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.***

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)

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**
Requirements Analysis Process (6.4.2) • Req'd characteristics, attributes, and functional & performance req'ts specified • Constraints on architecture and system realization defined • Integrity and traceability of system req'ts to stakeholder requirements achieved • Basis for verifying req'ts satisfaction is defined	• Define system functional boundaries • Define system functions/functional taxonomy • Allocate stakeholder req'ts to system functions and develop system req'ts • Define technical/quality measures for each function to achieve req'ts • ***Define functions and req'ts related to mitigating risk, safety, and usability issues***	Perform functional FMEA based on system functional taxonomy • Identify conventional failure modes and their probability and consequence **[4.4]** • Identify failures due to operator actions (usability) and their probability and consequences **[4.4]** ***Define additional technical/quality measures based on failure analysis*** Perform FTA/ETA based on intended use and operating/integrating environment • Identify common cause dysfunctions and their probability and consequence **[4.4]** • Identify event-based dysfunctions and their probability and consequences **[4.4]** ***Define additional technical/quality measures based on failure analysis***	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 Employ specific failure and dysfunction mechanisms to decompose top-level assurance case claims into second level claims Map second level claims to system functions • Perform initial assessment of technical/quality measures for sufficiency in meeting claims ***Identify new system functions needed to ensure that second level claims can be met.*** ***Identify new/revised technical/quality measures to ensure second level claims can be met***

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)

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**
Architectural Design Process (6.4.3) • Architecture baseline established • System element descriptions to satisfy req'ts specified • Interface req'ts incorporated • Traceability of architecture to req'ts established • Basis for verifying system elements defined • Basis for integrating system elements defined	• Define logical system architecture • Allocate functions to logical system architecture elements • Define system interfaces (internal & external) • Allocate system requirements to architecture elements • Identify human operator roles and associated usability req'ts • ***Identify and evaluate design alternatives***	Map functional FMEA, FTA, ETA outcomes to logical system architecture elements • Re-evaluate probability and consequences based on architecture elements **[5.0]** • Determine if risk control measures are needed for each architecture element **[6.1]** Assess risk control options **[6.2]** • Identify new constraints on architecture to "build in" safety • Identify new architecture elements needed to "build in" safety or control/mitigate risk ***Update logical system architecture to incorporate built in safety and risk control/mitigation***	Develop strategy for each second level claim based on logical system architecture elements. Decompose second level claims into third level claims based on risk analysis and selected risk control measures. Develop evidence needs for each third level claim based on technical and quality control measures applied to each architecture element. Evaluate overall set of safety case claims for completeness. ***Identify updates to logical system architecture based on what is needed for complete safety assurance case***.

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)

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>Implementation Process</u> (6.4.4) • Implementation strategy defined • Implementation technology constraints identified • System elements realized • System element packaged & stored in accordance with agreement for its supply	• Define implementation strategy for each architecture element • Define implementation constraints for each architecture element • Realize each architecture element (hardware, software, operator training) • Record data verifying that each realization meets the constraints applied	Implement the selected risk control measures into the implementation strategy for each architecture element **[6.3]** Implement the selected risk control measures into the of each architecture element **[6.3]** Evaluate verification data on each realization to determine if risk goals have been achieved at component level **[6.4]** Evaluate verification data on each realization to determine if risk control measures have introduced new risks **[6.6]** ***Update implementation strategy and/or realization if needed***	Evaluate component implementation strategies to assure that they will meet third level claim evidence needs ***Revise implementation strategies to support the assurance case*** Evaluate verification data to assure that it is sufficient to justify all third level claims ***Develop input to update component realization in order to achieve satisfaction of each third level claim***

Note: ***Blue bold face font*** indicates a feedback ***<u>from</u>*** risk management/assurance case to the Technical Process.
Note: ***Green bold face font*** indicates feedback ***<u>into</u>*** Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)

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**
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*** Update residual risk evaluation based on actual/revised system element performances and integration results [**6.4**] ***Provide input to revise integration procedures, constraints & measurements to reduce residual risk*** Perform risk/benefit analysis based on actual/revised system element performances and integration results [**6.5**] ***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***

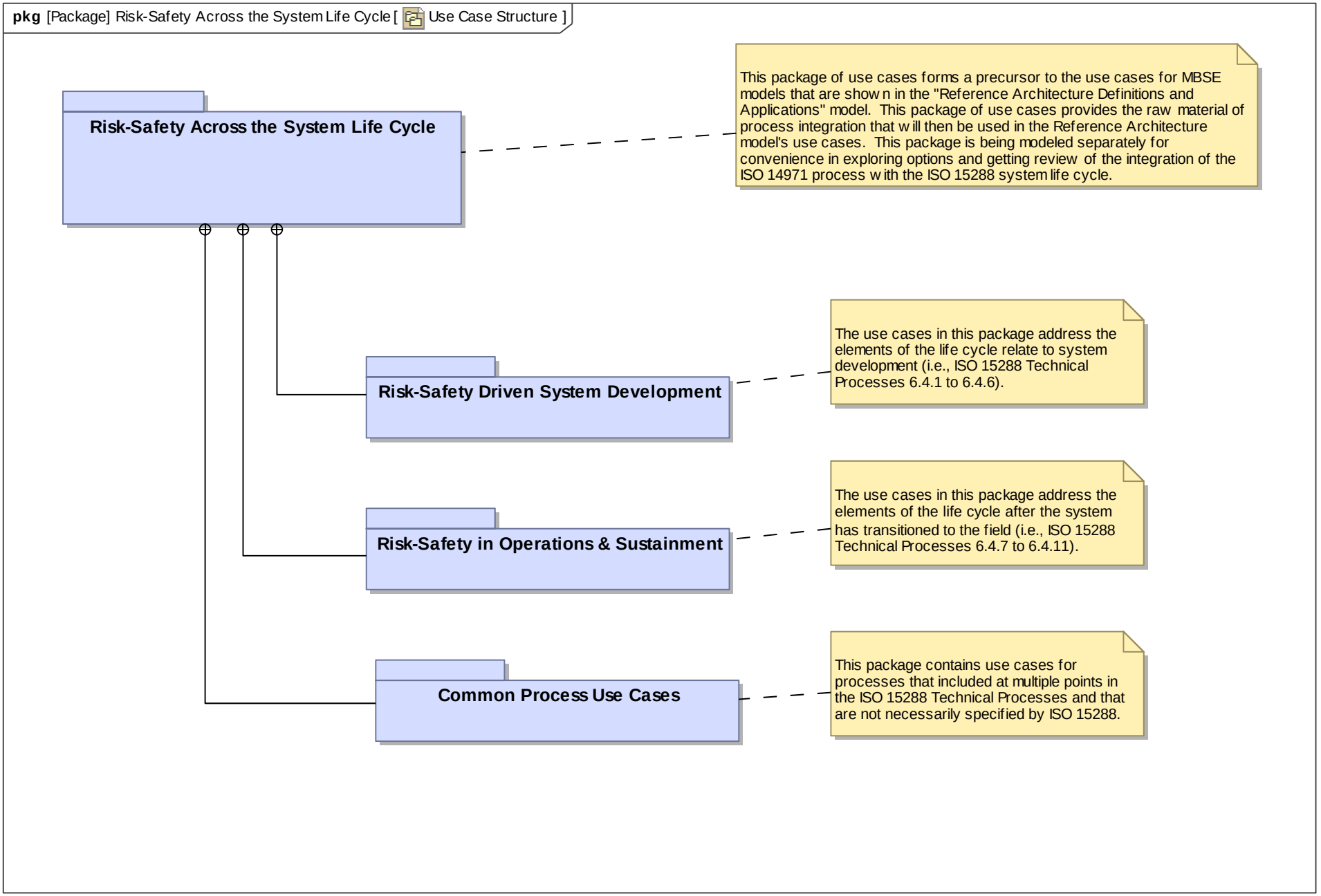
Note: ***Blue bold face font*** indicates a feedback ***from*** risk management/assurance case to the Technical Process.
Note: ***Green bold face font*** indicates feedback ***into*** Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)

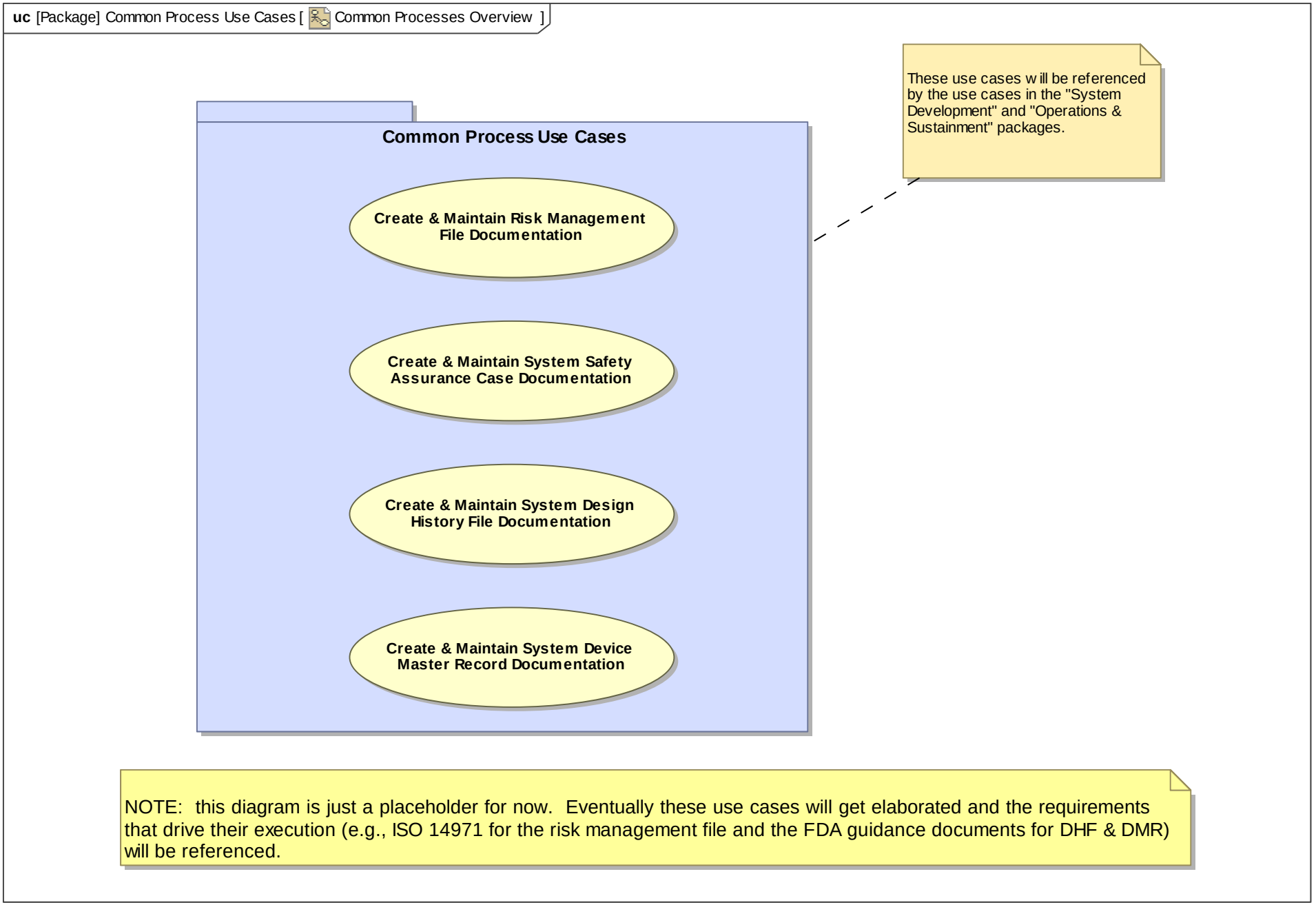
ISO 15288 Technical Processes (outcomes shown in bullets)	**15288 Actions/Products Connected to Risk Analysis** (see model for complete list of 15288)	**ISO 14971 Analyses, Iterations and Recursions** [clause references to ISO 14971]	**Relationship to Recursive Development of Safety Assurance Case**
Verification Process (6.4.6) • Verification strategy defined • Verification constraints provided as input to req'ts • Data providing info for corrective actions are reported • Objective evidence that realized product satisfies req'ts and the architecture is provided	• Define verification strategy throughout the system lifecycle ***Revise verification strategy based on hazard estimation and strategies for first level claims*** • Define verification plan ***Revise verification strategy based on*** • Conduct verification demonstration • Make verification data available • Analyze/record/report verification results including discrepancies ***Update any element of system design, integration, verification based on results of risk analyses and assurance case evaluations*** • Analyze/record/report corrective actions	Employ Preliminary Hazard Analysis and Functional Risk Estimates to determine risk control verification approaches [**4.3, 4.4**] ***Provide input to verification strategy*** Employ risk control evaluations to determine risk control verification req'ts [**5.0, 6.3, 6.4, 6.6**] ***Provide input to verification plan*** Analyze verification data to update evaluation of completeness of risk control [6.7] Analyze verification data to update evaluation of residual risk [6.4] Analyze verification data to update evaluate of risk/benefit [6.5] ***Analyze results of assurance case evaluation as input to risk management*** Analyze verification data to determine overall acceptability of residual risk ***Provide input to corrective actions (corrective actions could cause revision to any one of the technical processes 6.4.1-6.4.6)***	Analyze strategies for first-level claims to determine assurance verification approaches ***Provide input to verification strategy*** Analyze strategies and evidence needs for second and third-level claims to determine assurance verification req'ts ***Provide input to verification plan*** Analyze verification data to update evaluation of evidence + third-level claims + second-level claims + first-level claims Analyze verification data to determine if overall assurance case is satisfied and if assurance case is complet ***Provide input to corrective actions (corrective actions could cause revision to any one of the technical processes 6.4.1-6.4.6)***

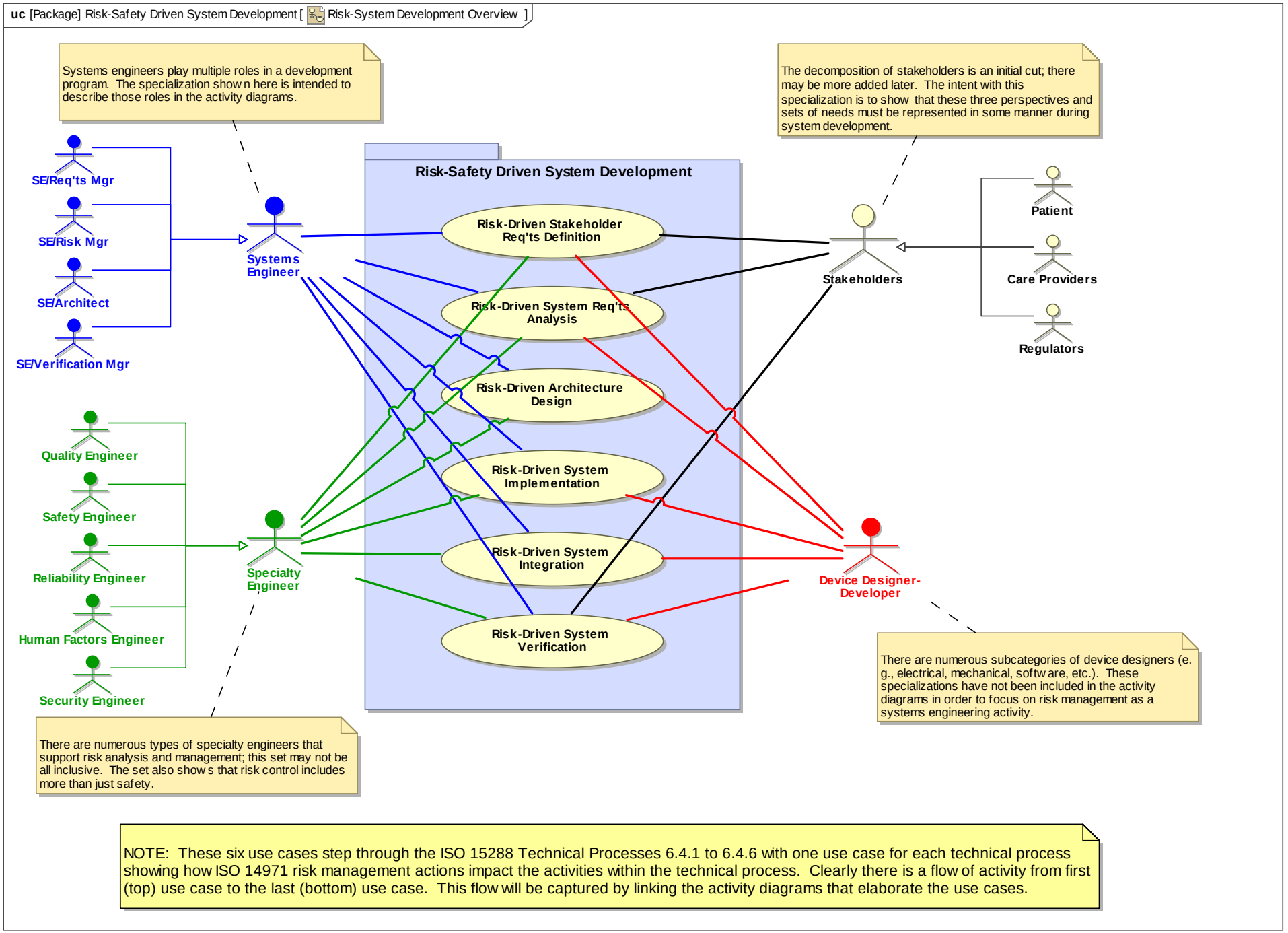
Note: ***Blue bold face font*** indicates a feedback ***from*** risk management/assurance case to the Technical Process.
Note: ***Green bold face font*** indicates feedback ***into*** Tech processes (from risk mgt & assurance) or Risk Mgt (from assurance case)

Applying Risk-Hazard-Safety Management Across the System Lifecycle

Modeling ISO 15288-ISO 14971 Integration: Model Structure

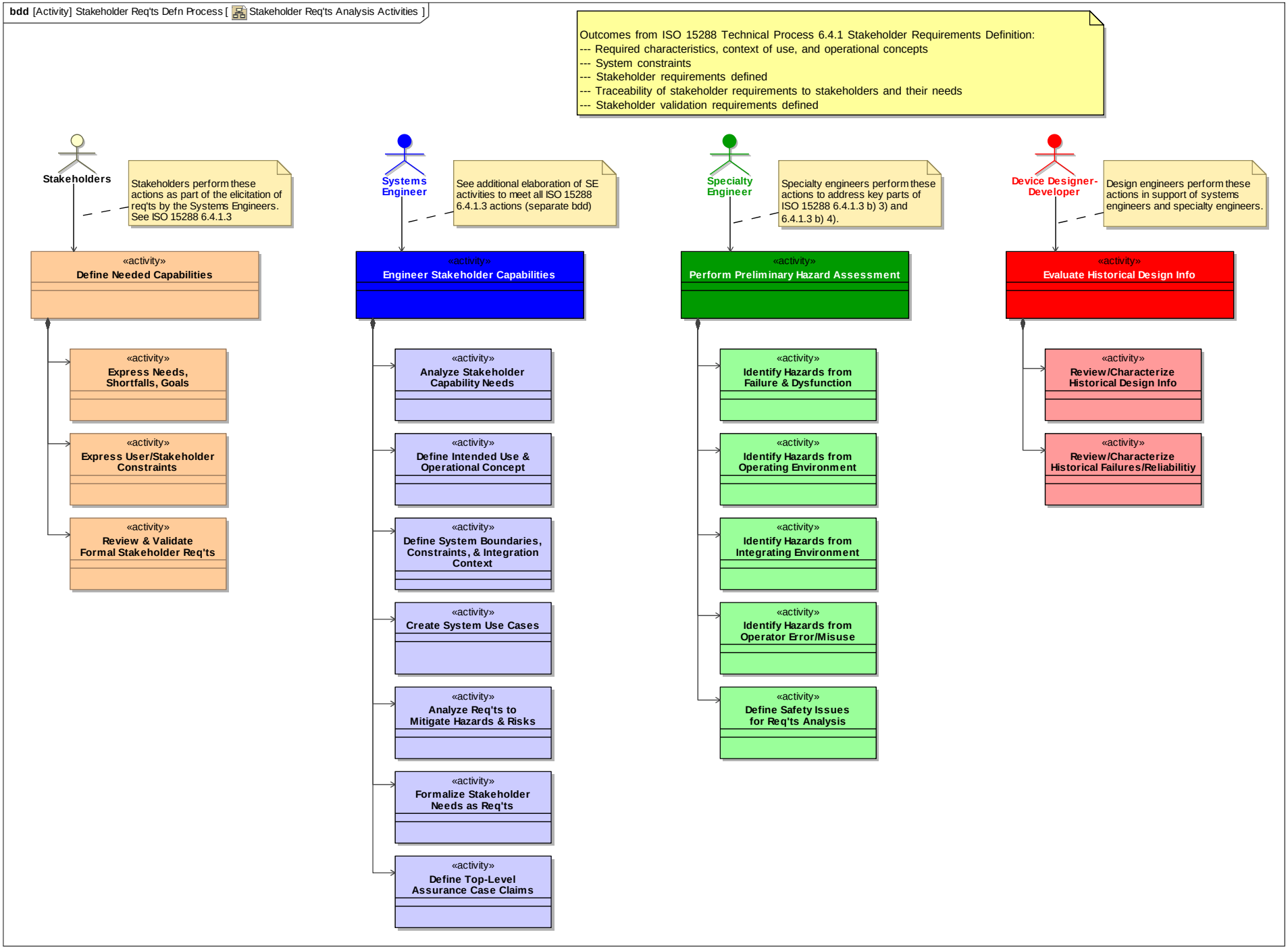

pkg [Package] Risk-Safety Across the System Life Cycle [Use Case Structure]
Risk-Safety Across the System Life Cycle
This package of use cases forms a precursor to the use cases for MBSE models that are shown in the "Reference Architecture Definitions and Applications" model. This package of use cases 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.
Risk-Safety Driven System Development
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).
Risk-Safety in Operations & Sustainment
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).
Common Process Use Cases
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.

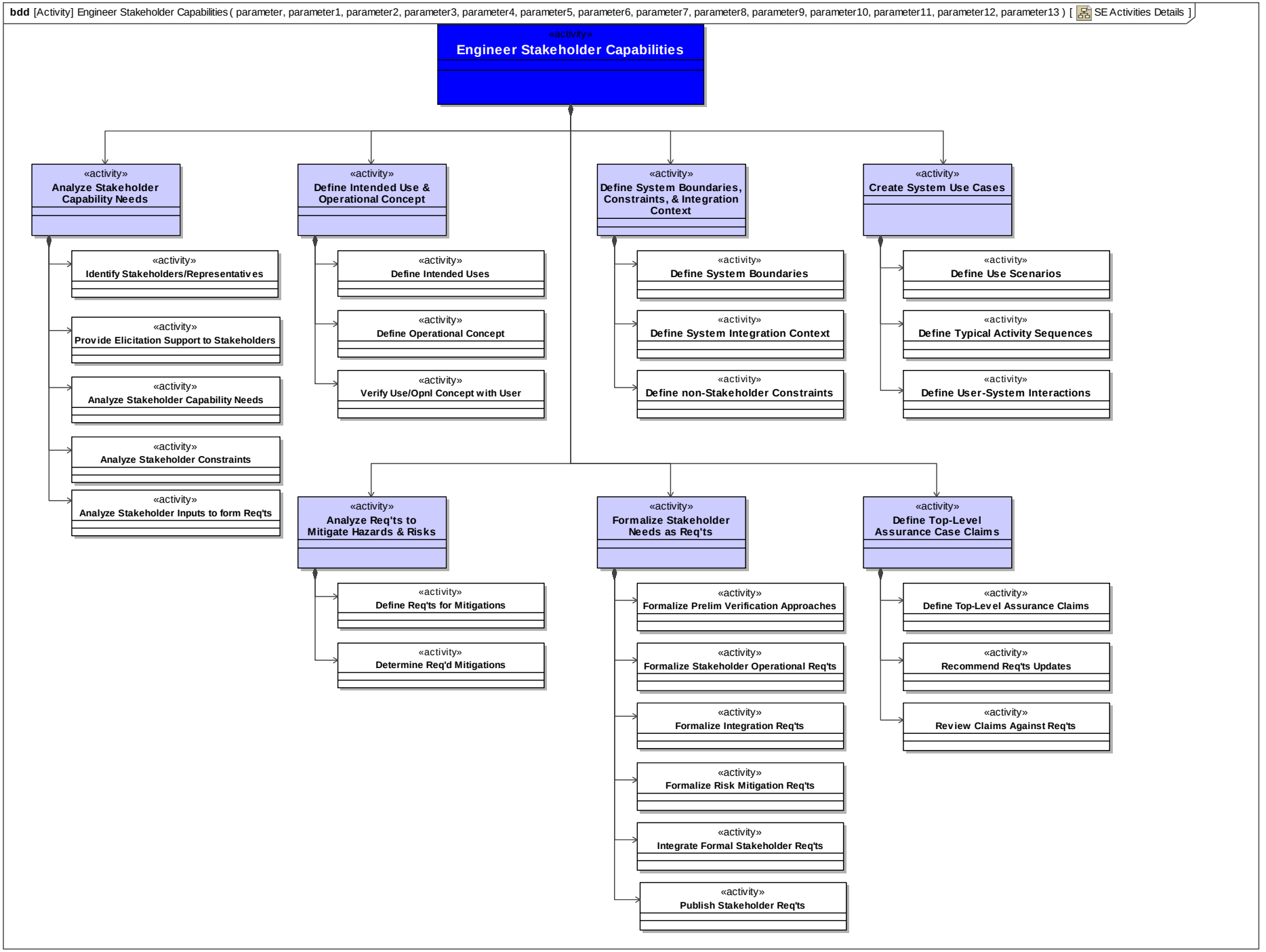

uc [Package] Common Process Use Cases [Common Processes Overview]
Common Process Use Cases
Create & Maintain Risk Management File Documentation
Create & Maintain System Safety Assurance Case Documentation
Create & Maintain System Design History File Documentation
Create & Maintain System Device Master Record Documentation
These use cases w ill be referenced by the use cases in the "System Development" and "Operations & Sustainment" packages.
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.

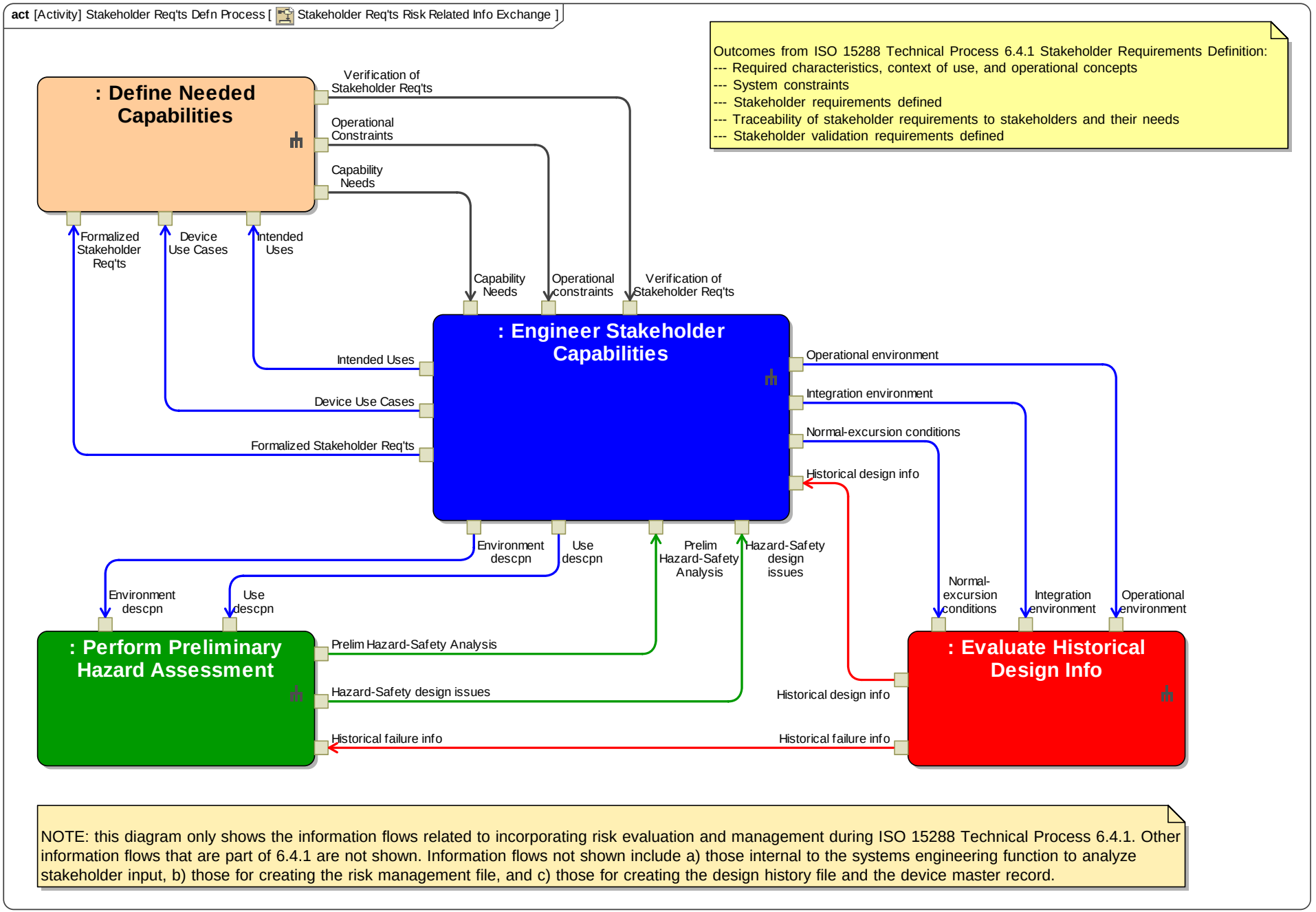

uc [Package] Risk-Safety Driven System Development [Risk-System Development Overview]
Systems engineers play multiple roles in a development program. The specialization shown here is intended to describe those roles in the activity diagrams.
The decomposition of stakeholders is an initial cut; there 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.
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
Quality Engineer
Safety Engineer
Reliability Engineer
Human Factors Engineer
Security Engineer
Specialty Engineer
Device Designer-Developer
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.
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.
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.

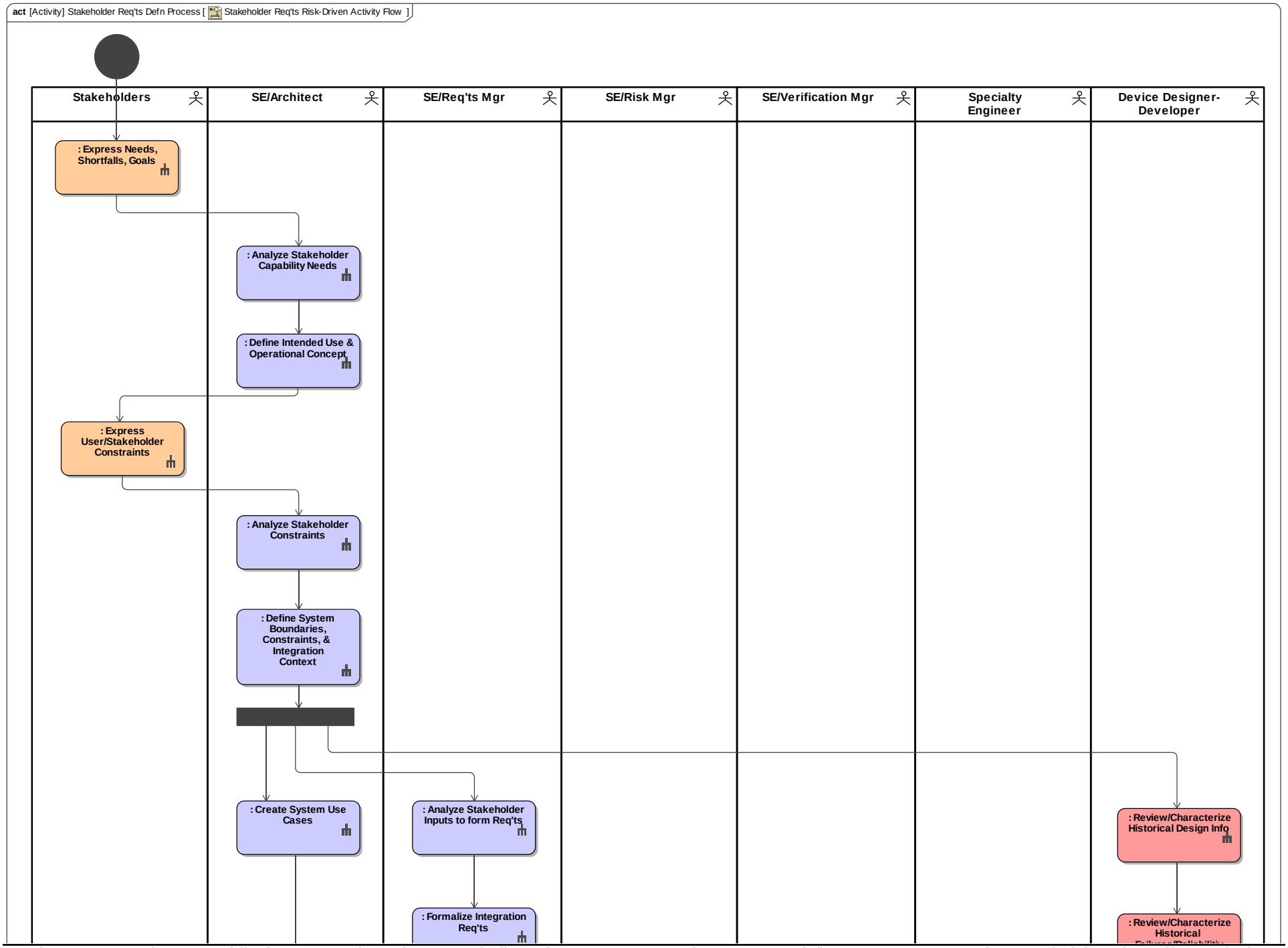
Applying Risk-Hazard-Safety Management Across the System Lifecycle

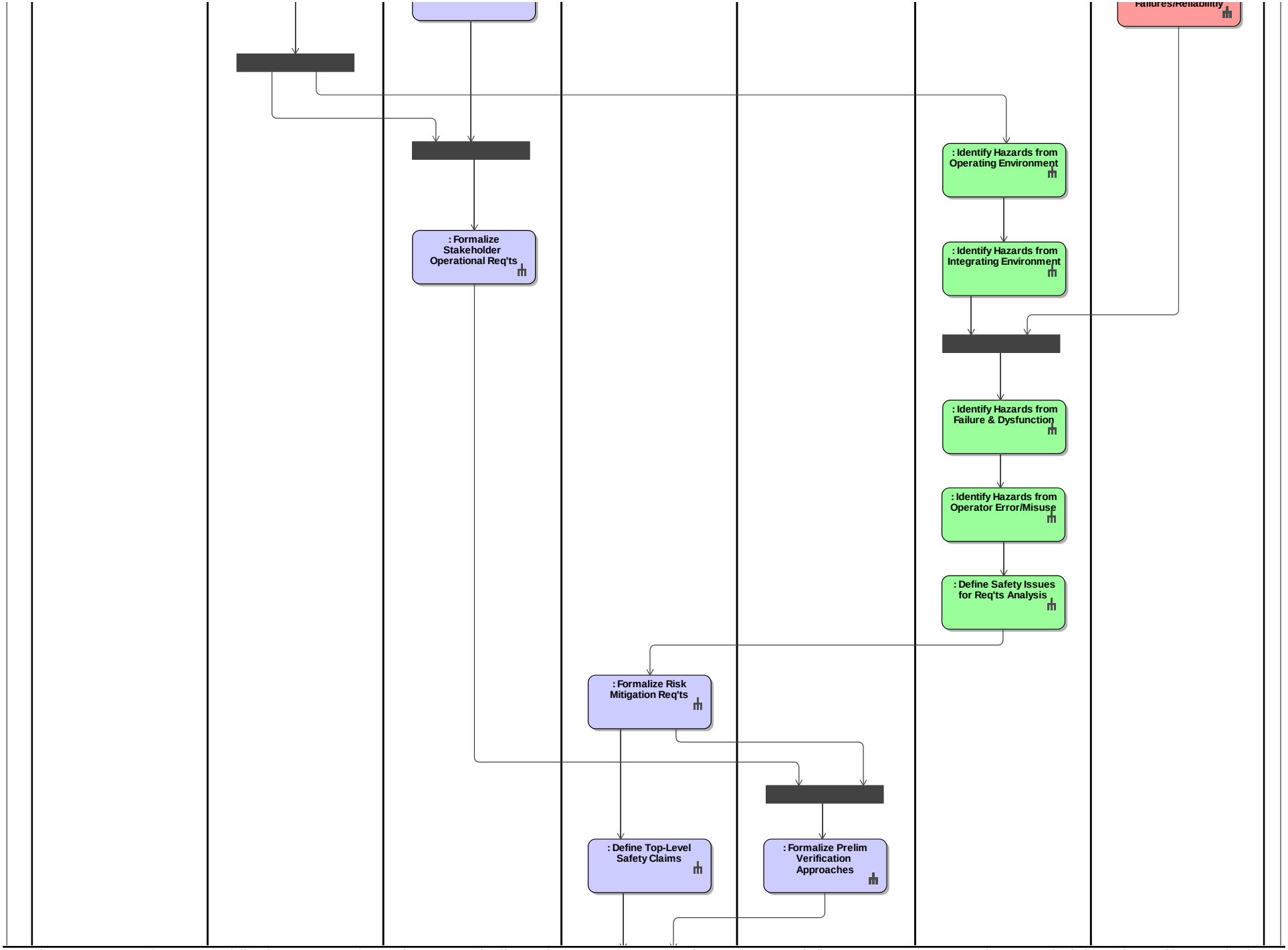
Modeling ISO 15288-ISO 14971 Integration: Process Model 1 – 6.4.1 Stakeholder Req’ts Definition

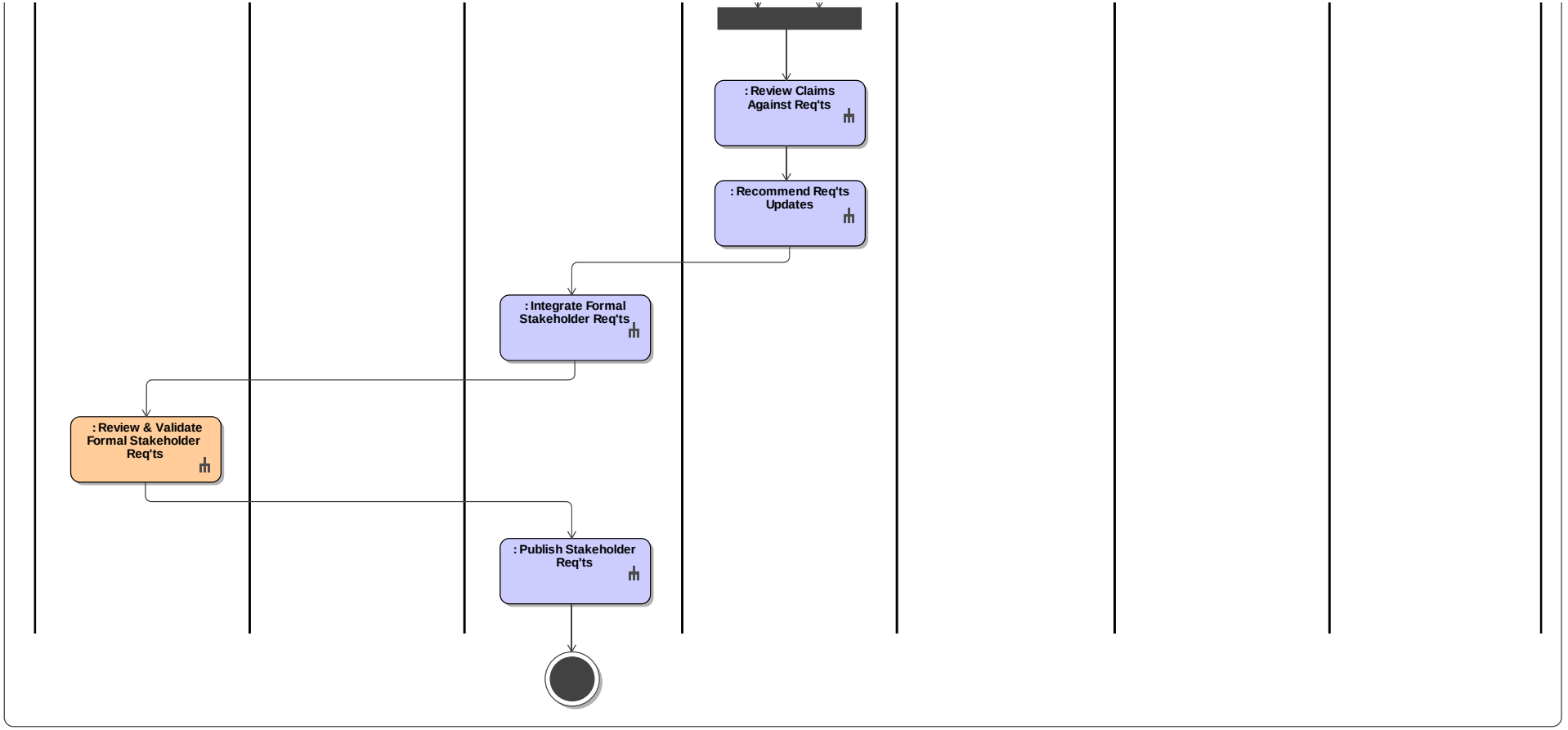

bdd [Activity] Stakeholder Req'ts Defn Process [Stakeholder Req'ts Analysis Activities]
Outcomes from ISO 15288 Technical Process 6.4.1 Stakeholder Requirements Definition:
--- Required characteristics, context of use, and operational concepts
--- System constraints
--- Stakeholder requirements defined
--- Traceability of stakeholder requirements to stakeholders and their needs
--- Stakeholder validation requirements defined
Stakeholders
Stakeholders perform these actions as part of the elicitation of req'ts by the Systems Engineers. See ISO 15288 6.4.1.3
Systems Engineer
See additional elaboration of SE activities to meet all ISO 15288 6.4.1.3 actions (separate bdd)
Specialty Engineer
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).
Device Designer-Developer
Design engineers perform these actions in support of systems engineers and specialty engineers.
«activity» Define Needed Capabilities
«activity» Express Needs, Shortfalls, Goals
«activity» Express User/Stakeholder Constraints
«activity» Review & Validate Formal Stakeholder Req'ts
«activity» Engineer Stakeholder Capabilities
«activity» Analyze Stakeholder Capability Needs
«activity» Define Intended Use & Operational Concept
«activity» Define System Boundaries, Constraints, & Integration 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 Assurance Case Claims
«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
«activity» Evaluate Historical Design Info
«activity» Review/Characterize Historical Design Info
«activity» Review/Characterize Historical Failures/Reliabilitiy


bdd [Activity] Engineer Stakeholder Capabilities (parameter, parameter1, parameter2, parameter3, parameter4, parameter5, parameter6, parameter7, parameter8, parameter9, parameter10, parameter11, parameter12, parameter13) [SE Activities Details]
«activity»
Engineer Stakeholder Capabilities
«activity»
Analyze Stakeholder Capability Needs
«activity»
Identify Stakeholders/Representatives
«activity»
Provide Elicitation Support to Stakeholders
«activity»
Analyze Stakeholder Capability Needs
«activity»
Analyze Stakeholder Constraints
«activity»
Analyze Stakeholder Inputs to form Req'ts
«activity»
Define Intended Use & Operational Concept
«activity»
Define Intended Uses
«activity»
Define Operational Concept
«activity»
Verify Use/Opnl Concept with User
«activity»
Define System Boundaries, Constraints, & Integration Context
«activity»
Define System Boundaries
«activity»
Define System Integration Context
«activity»
Define non-Stakeholder Constraints
«activity»
Create System Use Cases
«activity»
Define Use Scenarios
«activity»
Define Typical Activity Sequences
«activity»
Define User-System Interactions
«activity»
Analyze Req'ts to Mitigate Hazards & Risks
«activity»
Define Req'ts for Mitigations
«activity»
Determine Req'd Mitigations
«activity»
Formalize Stakeholder Needs as Req'ts
«activity»
Formalize Prelim Verification Approaches
«activity»
Formalize Stakeholder Operational Req'ts
«activity»
Formalize Integration Req'ts
«activity»
Formalize Risk Mitigation Req'ts
«activity»
Integrate Formal Stakeholder Req'ts
«activity»
Publish Stakeholder Req'ts
«activity»
Define Top-Level Assurance Case Claims
«activity»
Define Top-Level Assurance Claims
«activity»
Recommend Req'ts Updates
«activity»
Review Claims Against Req'ts


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 and their 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
: Engineer Stakeholder Capabilities
Capability Needs
Operational constraints
Verification of Stakeholder Req'ts
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
: Perform Preliminary Hazard Assessment
Environment descpn
Use descpn
Prelim Hazard-Safety Analysis
Hazard-Safety design issues
Historical failure info
: Evaluate Historical Design Info
Normal-excursion conditions
Integration environment
Operational environment
Historical design info
Historical failure info
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.

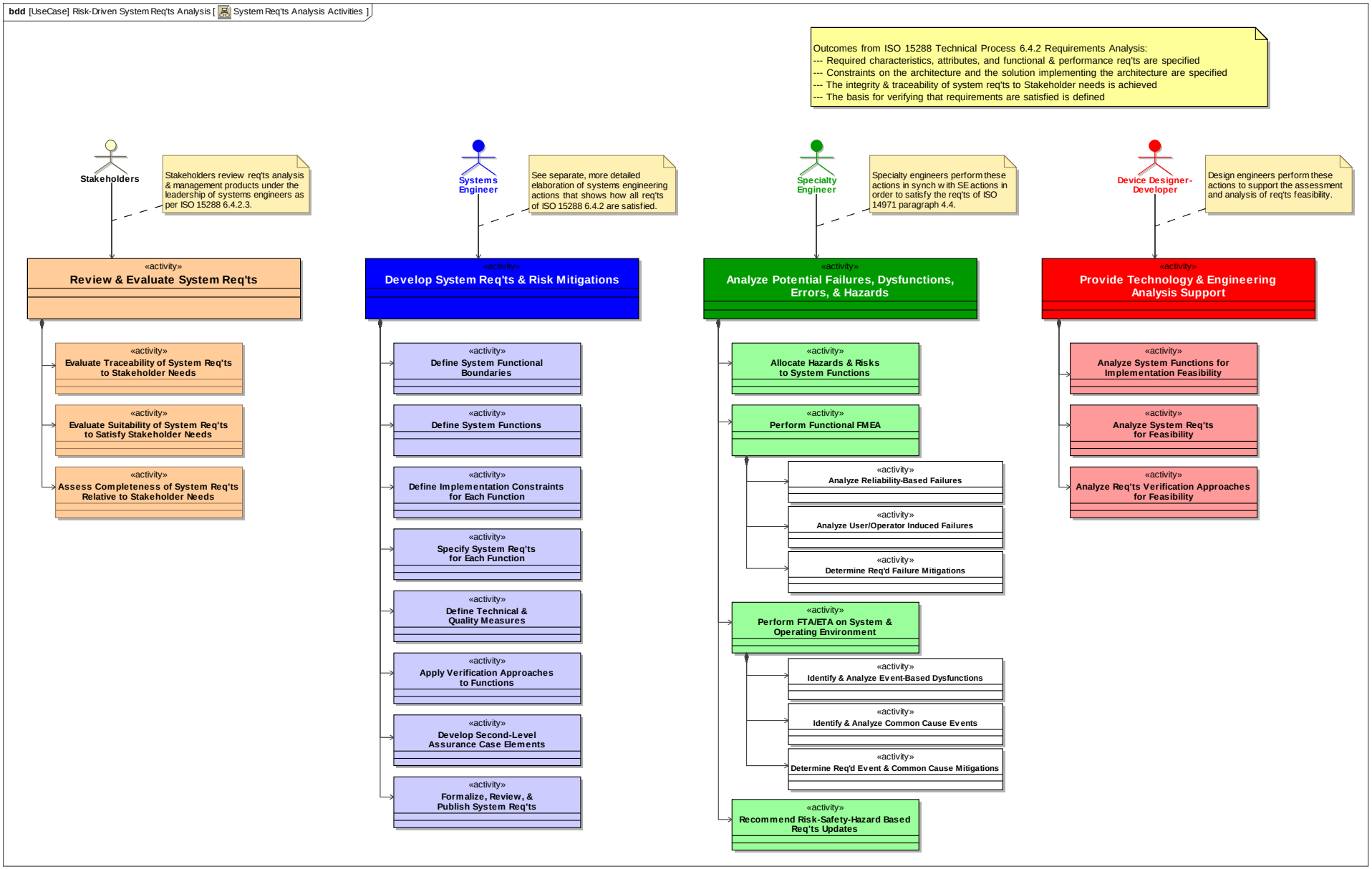

act [Activity] Stakeholder Req'ts Defn Process [Stakeholder Req'ts Risk-Driven Activity Flow]
Stakeholders
SE/Architect
SE/Req'ts Mgr
SE/Risk Mgr
SE/Verification Mgr
Specialty Engineer
Device Designer-Developer
: Express Needs, Shortfalls, Goals
: Analyze Stakeholder Capability Needs
: Define Intended 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

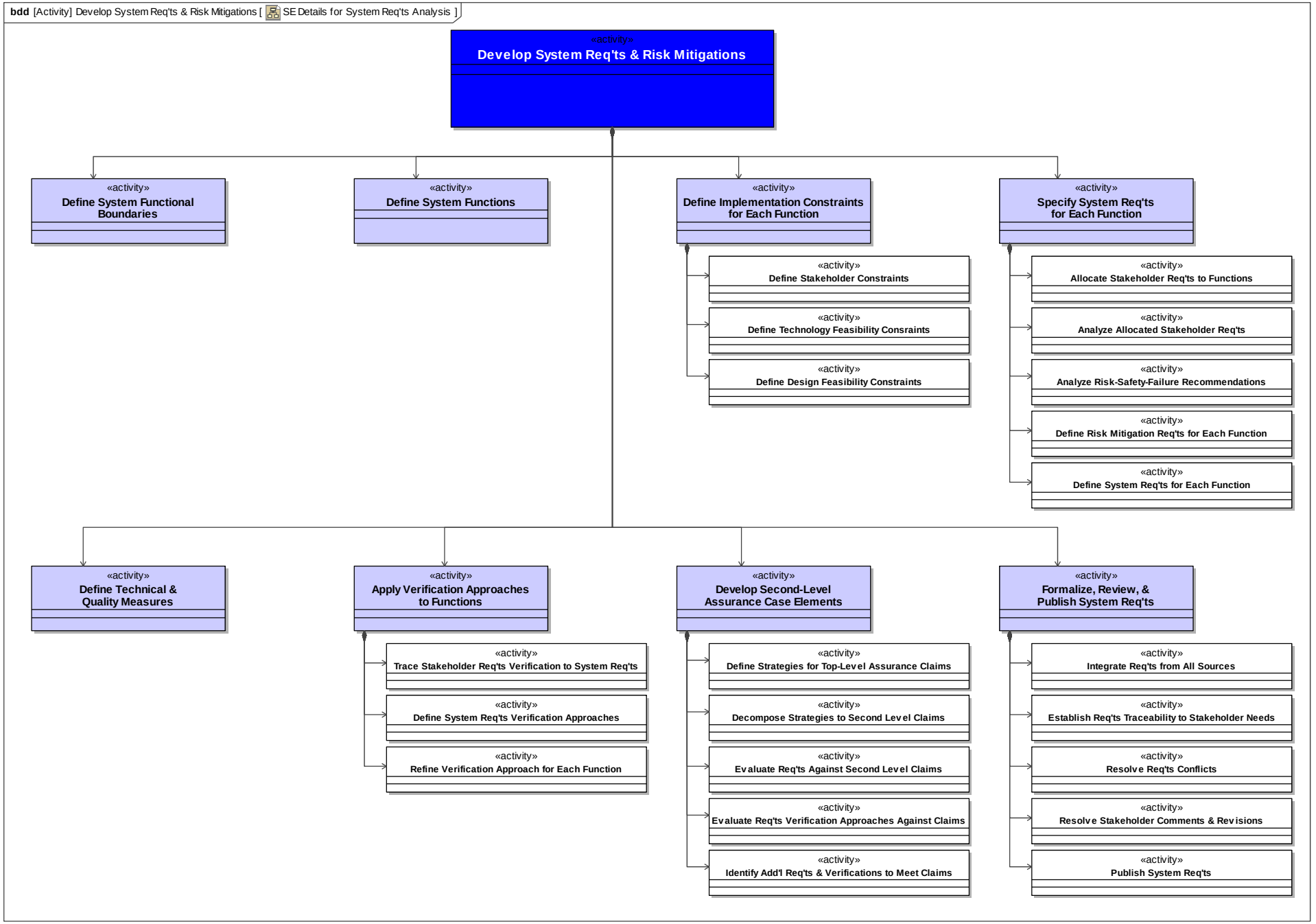

: Formalize Stakeholder Operational Req'ts
: Identify Hazards from Operating Environment
: Identify Hazards from Integrating Environment
: Identify Hazards from Failure & Dysfunction
: Identify Hazards from Operator Error/Misuse
: Define Safety Issues for Req'ts Analysis
: Formalize Risk Mitigation Req'ts
: Define Top-Level Safety Claims
: Formalize Prelim Verification Approaches

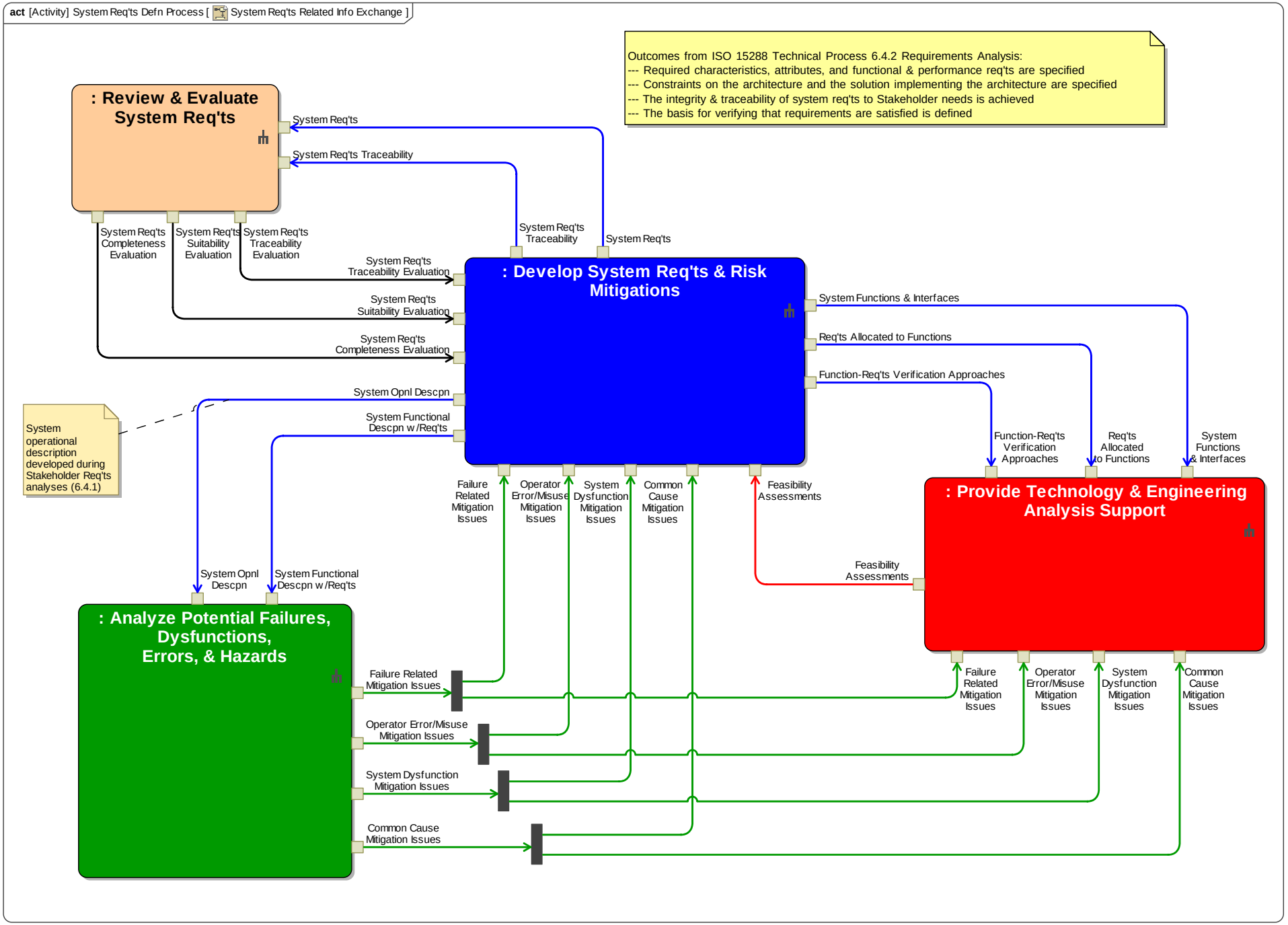

: Review Claims Against Req'ts
: Recommend Req'ts Updates
: Integrate Formal Stakeholder Req'ts
: Review & Validate Formal Stakeholder Req'ts
: Publish Stakeholder Req'ts

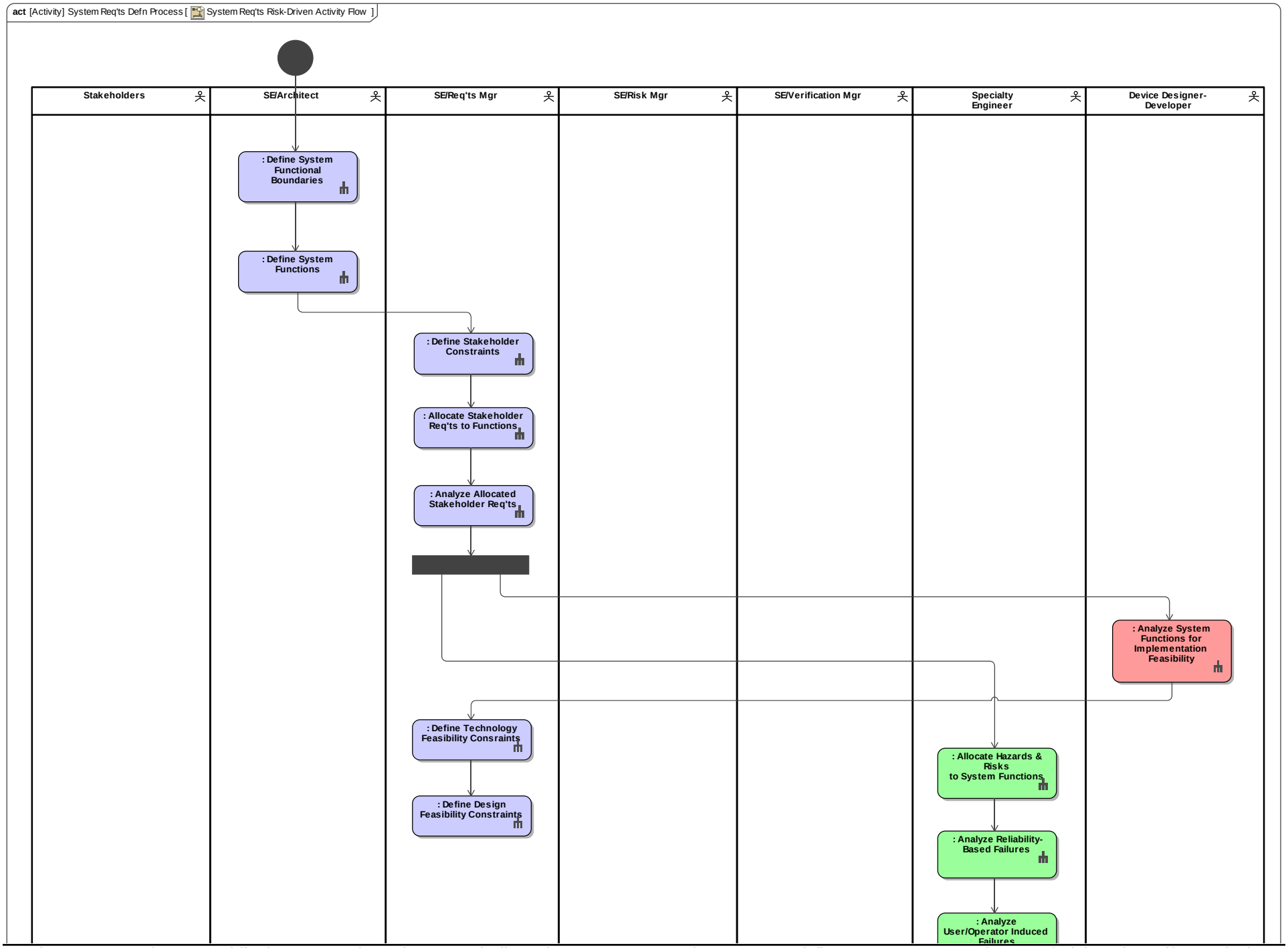
Applying Risk-Hazard-Safety Management Across the System Lifecycle

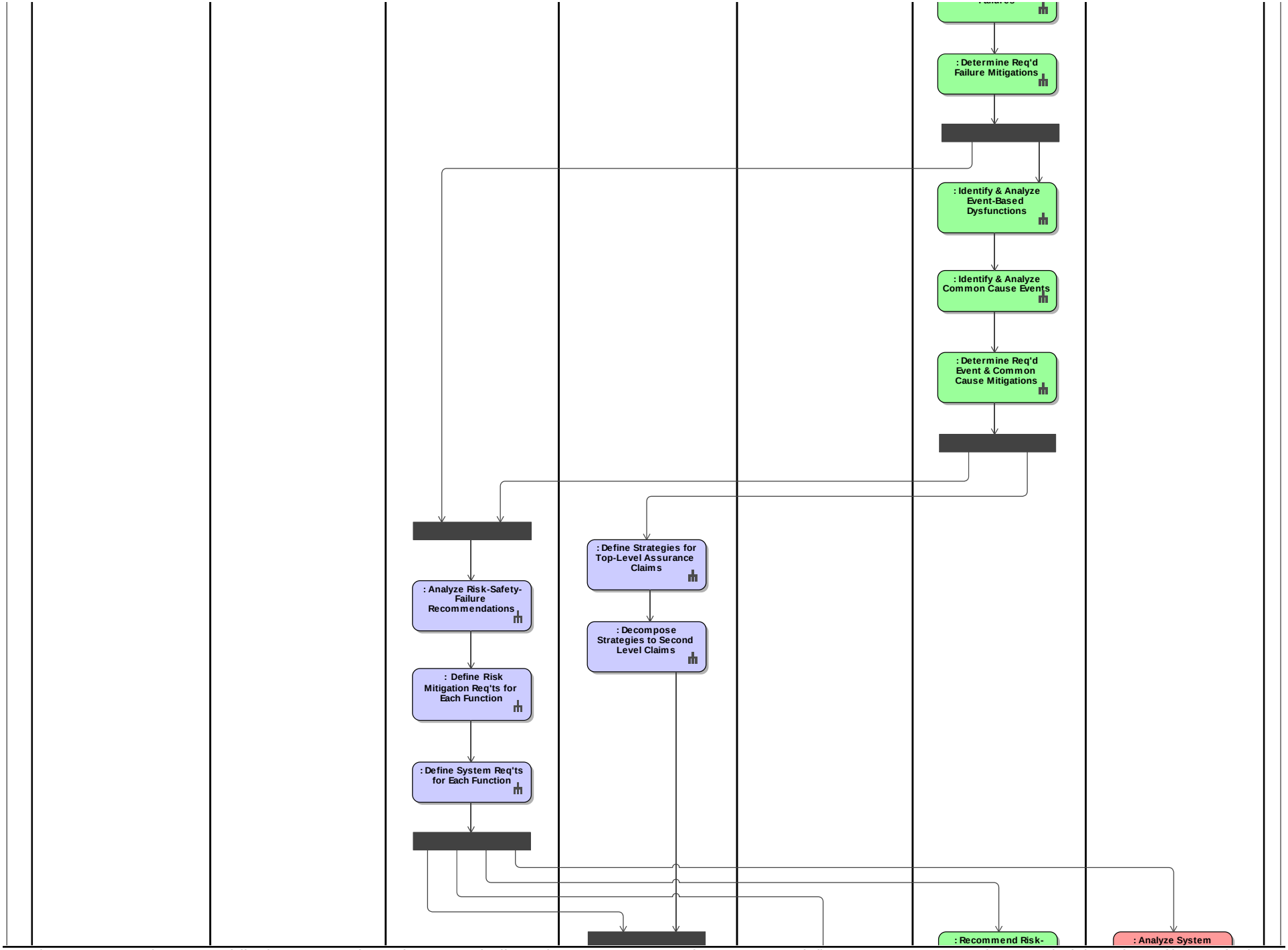
Modeling ISO 15288-ISO 14971 Integration: Process Model 2 – 6.4.2 Requirements Analysis Process

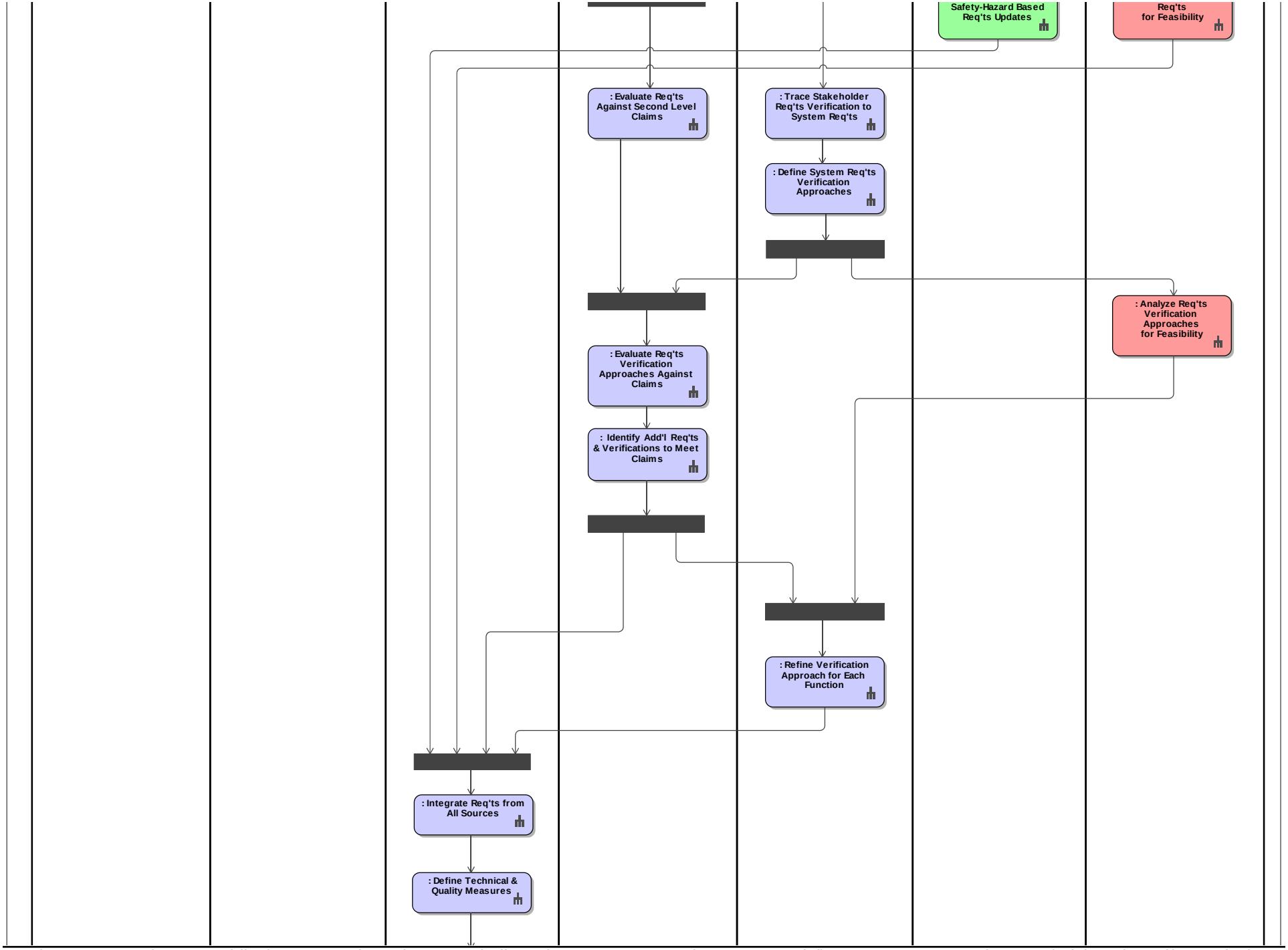

bdd [UseCase] Risk-Driven System Req'ts Analysis [System Req'ts Analysis Activities]
Outcomes from ISO 15288 Technical Process 6.4.2 Requirements Analysis:
--- Required characteristics, attributes, and functional & performance req'ts are specified
--- Constraints on the architecture and the solution 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
Stakeholders review req'ts analysis & management products under the leadership of systems engineers as per ISO 15288 6.4.2.3.
Systems Engineer
See separate, more detailed elaboration of systems engineering actions that shows how all req'ts of ISO 15288 6.4.2 are satisfied.
Specialty Engineer
Specialty engineers perform these actions in synch with SE actions in order to satisfy the req'ts of ISO 14971 paragraph 4.4.
Device Designer-Developer
Design engineers perform these actions to support the assessment and analysis of req'ts feasibility.
«activity» Review & Evaluate System Req'ts
«activity» Evaluate Traceability of System Req'ts to Stakeholder Needs
«activity» Evaluate Suitability of System Req'ts to Satisfy Stakeholder Needs
«activity» Assess Completeness of System Req'ts Relative to Stakeholder Needs
«activity» Develop System Req'ts & Risk Mitigations
«activity» Define System Functional Boundaries
«activity» Define System Functions
«activity» Define Implementation Constraints for Each Function
«activity» Specify System Req'ts for Each Function
«activity» Define Technical & Quality Measures
«activity» Apply Verification Approaches to Functions
«activity» Develop Second-Level Assurance Case Elements
«activity» Formalize, Review, & Publish System Req'ts
«activity» Analyze Potential Failures, Dysfunctions, Errors, & Hazards
«activity» Allocate Hazards & Risks to System Functions
«activity» Perform Functional FMEA
«activity» Analyze Reliability-Based Failures
«activity» Analyze User/Operator Induced Failures
«activity» Determine Req'd Failure Mitigations
«activity» Perform FTA/ETA on System & Operating Environment
«activity» Identify & Analyze Event-Based Dysfunctions
«activity» Identify & Analyze Common Cause Events
«activity» Determine Req'd Event & Common Cause Mitigations
«activity» Recommend Risk-Safety-Hazard Based Req'ts Updates
«activity» Provide Technology & Engineering Analysis Support
«activity» Analyze System Functions for Implementation Feasibility
«activity» Analyze System Req'ts for Feasibility
«activity» Analyze Req'ts Verification Approaches for Feasibility

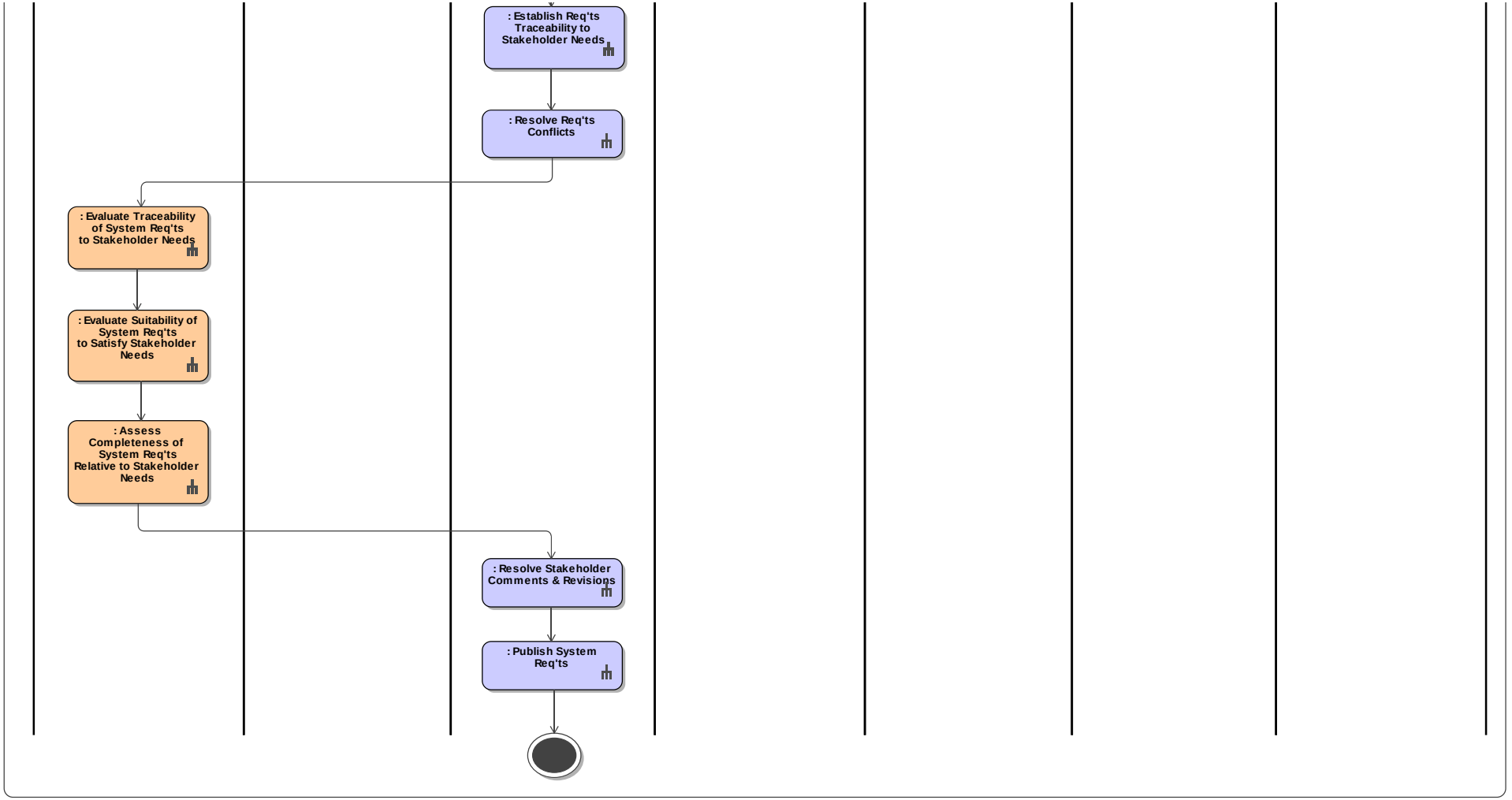

bdd [Activity] Develop System Req'ts & Risk Mitigations [SE Details for System Req'ts Analysis]
«activity»
Develop System Req'ts & Risk Mitigations
«activity»
Define System Functional Boundaries
«activity»
Define System Functions
«activity»
Define Implementation Constraints for Each Function
«activity»
Define Stakeholder Constraints
«activity»
Define Technology Feasibility Consraints
«activity»
Define Design Feasibility Constraints
«activity»
Specify System Req'ts for Each Function
«activity»
Allocate Stakeholder Req'ts to Functions
«activity»
Analyze Allocated Stakeholder Req'ts
«activity»
Analyze Risk-Safety-Failure Recommendations
«activity»
Define Risk Mitigation Req'ts for Each Function
«activity»
Define System Req'ts for Each Function
«activity»
Define Technical & Quality Measures
«activity»
Apply Verification Approaches to Functions
«activity»
Trace Stakeholder Req'ts Verification to System Req'ts
«activity»
Define System Req'ts Verification Approaches
«activity»
Refine Verification Approach for Each Function
«activity»
Develop Second-Level Assurance Case Elements
«activity»
Define Strategies for Top-Level Assurance Claims
«activity»
Decompose Strategies to Second Level Claims
«activity»
Evaluate Req'ts Against Second Level Claims
«activity»
Evaluate Req'ts Verification Approaches Against Claims
«activity»
Identify Add'l Req'ts & Verifications to Meet Claims
«activity»
Formalize, Review, & Publish System Req'ts
«activity»
Integrate Req'ts from All Sources
«activity»
Establish Req'ts Traceability to Stakeholder Needs
«activity»
Resolve Req'ts Conflicts
«activity»
Resolve Stakeholder Comments & Revisions
«activity»
Publish System Req'ts


act [Activity] System Req'ts Defn Process [System Req'ts Related Info Exchange]
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
: Review & Evaluate System Req'ts
System Req'ts
System Req'ts Traceability
System Req'ts Completeness Evaluation
System Req'ts Suitability Evaluation
System Req'ts Traceability Evaluation
: Develop System Req'ts & Risk Mitigations
System Req'ts Traceability
System Req'ts
System Req'ts Traceability Evaluation
System Req'ts Suitability Evaluation
System Req'ts Completeness Evaluation
System Functions & Interfaces
Req'ts Allocated to Functions
Function-Req'ts Verification Approaches
System Opnl Descpn
System Functional Descpn w/Req'ts
System operational description developed during Stakeholder Req'ts analyses (6.4.1)
Function-Req'ts Verification Approaches
Req'ts Allocated to Functions
System Functions & Interfaces
Failure Related Mitigation Issues
Operator Error/Misuse Mitigation Issues
System Dysfunction Mitigation Issues
Common Cause Mitigation Issues
Feasibility Assessments
: Provide Technology & Engineering Analysis Support
Feasibility Assessments
System Opnl Descpn
System Functional Descpn w/Req'ts
: Analyze Potential Failures, Dysfunctions, Errors, & Hazards
Failure Related Mitigation Issues
Operator Error/Misuse Mitigation Issues
System Dysfunction Mitigation Issues
Common Cause Mitigation Issues
Failure Related Mitigation Issues
Operator Error/Misuse Mitigation Issues
System Dysfunction Mitigation Issues
Common Cause Mitigation Issues


act [Activity] System Req'ts Defn Process [System Req'ts Risk-Driven Activity Flow]
Stakeholders
SE/Architect
SE/Req'ts Mgr
SE/Risk Mgr
SE/Verification Mgr
Specialty Engineer
Device Designer-Developer
: Define System Functional Boundaries
: Define System Functions
: Define Stakeholder Constraints
: Allocate Stakeholder Req'ts to Functions
: Analyze Allocated Stakeholder Req'ts
: Analyze System Functions for Implementation Feasibility
: Define Technology Feasibility Consraints
: Define Design Feasibility Constraints
: Allocate Hazards & Risks to System Functions
: Analyze Reliability-Based Failures
: Analyze User/Operator Induced Failures

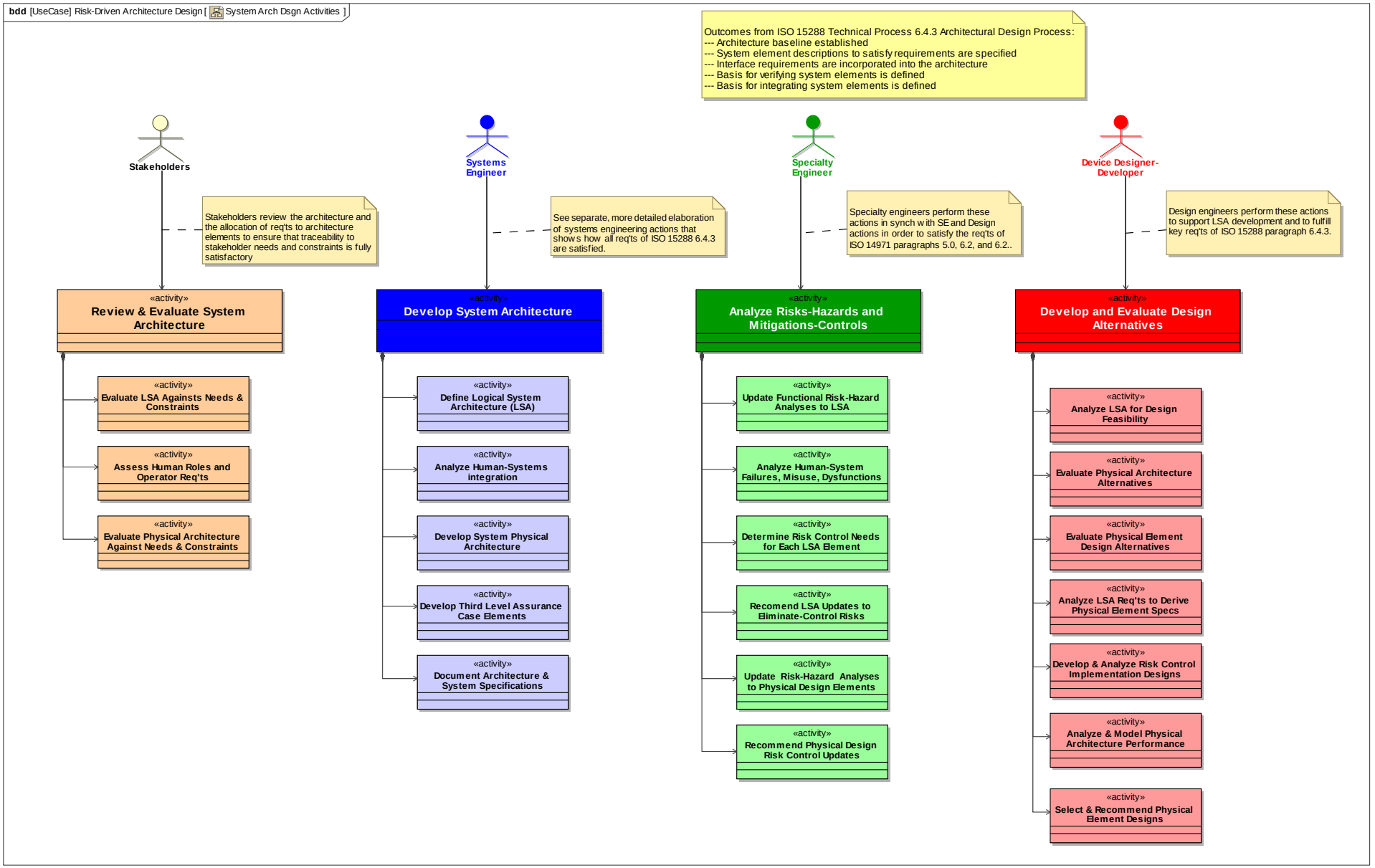

: Determine Req'd Failure Mitigations
: Identify & Analyze Event-Based Dysfunctions
: Identify & Analyze Common Cause Events
: Determine Req'd Event & Common Cause Mitigations
: Define Strategies for Top-Level Assurance Claims
: Decompose Strategies to Second Level Claims
: Analyze Risk-Safety-Failure Recommendations
: Define Risk Mitigation Req'ts for Each Function
: Define System Req'ts for Each Function
: Recommend Risk-
: Analyze System

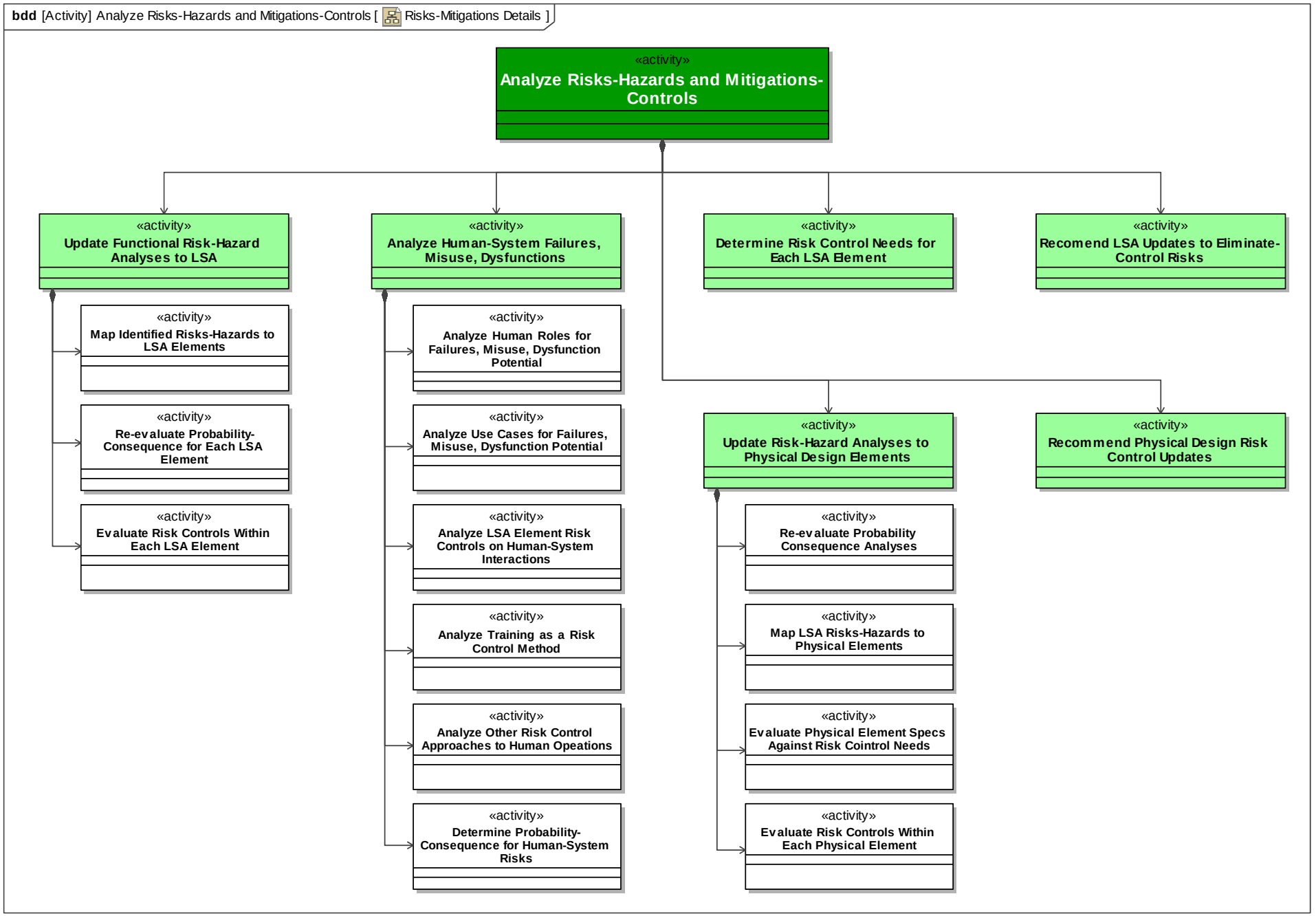

Safety-Hazard Based Req'ts Updates
Req'ts for Feasibility
: Evaluate Req'ts Against Second Level Claims
: Trace Stakeholder Req'ts Verification to System Req'ts
: Define System Req'ts Verification Approaches
: Analyze Req'ts Verification Approaches for Feasibility
: Evaluate Req'ts Verification Approaches Against Claims
: Identify Add'l Req'ts & Verifications to Meet Claims
: Refine Verification Approach for Each Function
: Integrate Req'ts from All Sources
: Define Technical & Quality Measures

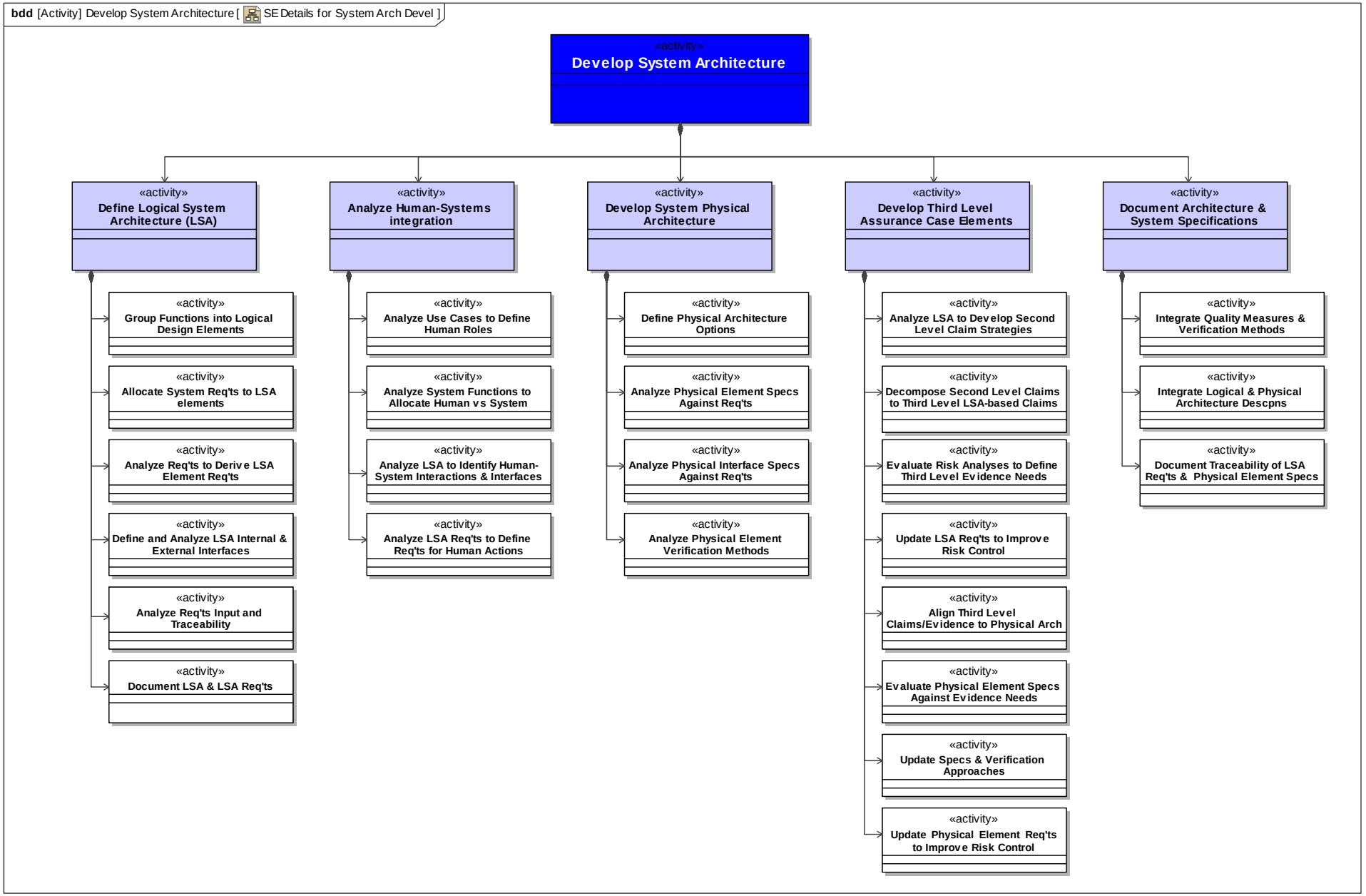

: Establish Req'ts Traceability to Stakeholder Needs
: Resolve Req'ts Conflicts
: Evaluate Traceability of System Req'ts to Stakeholder Needs
: Evaluate Suitability of System Req'ts to Satisfy Stakeholder Needs
: Assess Completeness of System Req'ts Relative to Stakeholder Needs
: Resolve Stakeholder Comments & Revisions
: Publish System Req'ts

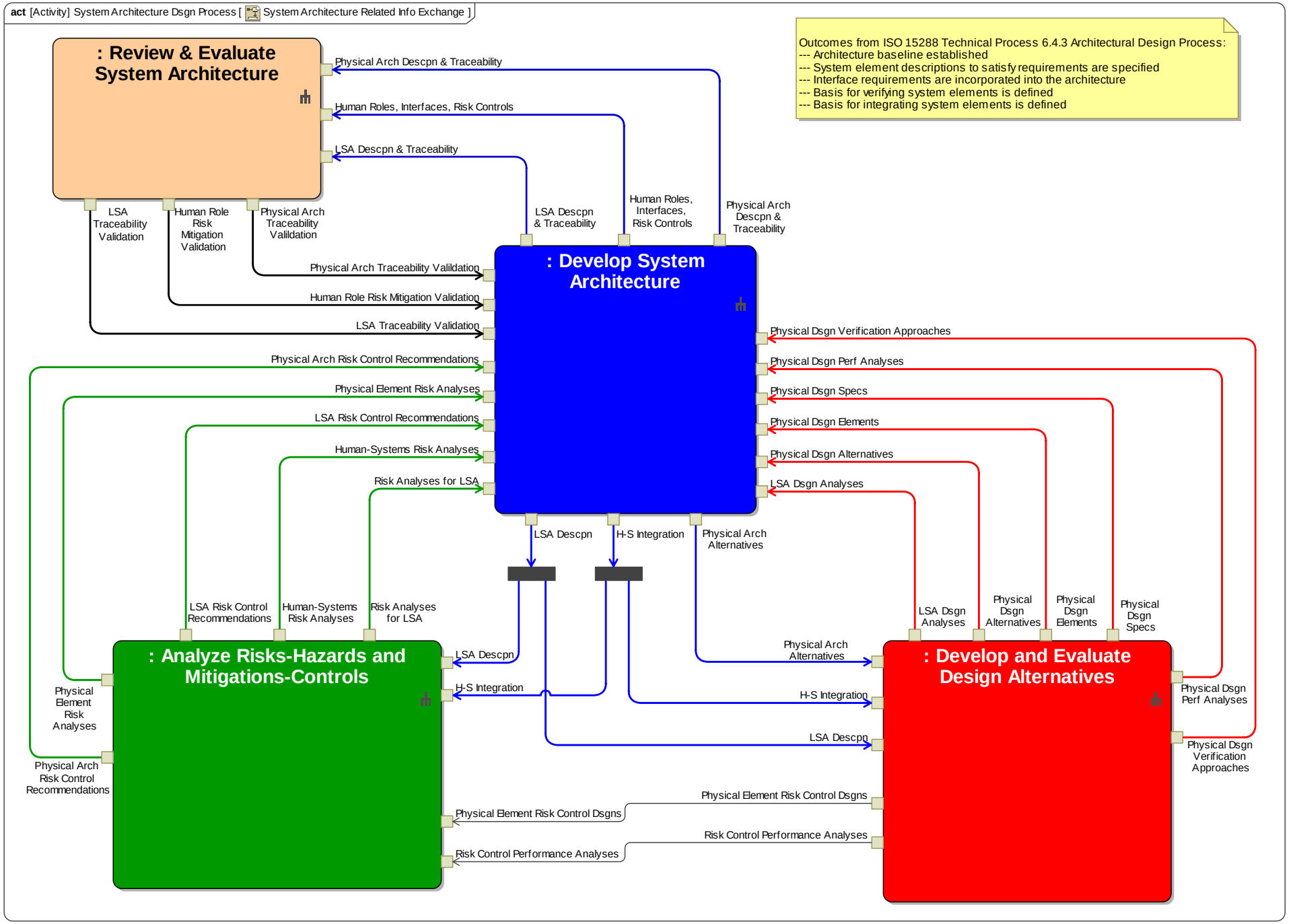
Applying Risk-Hazard-Safety Management Across the System Lifecycle

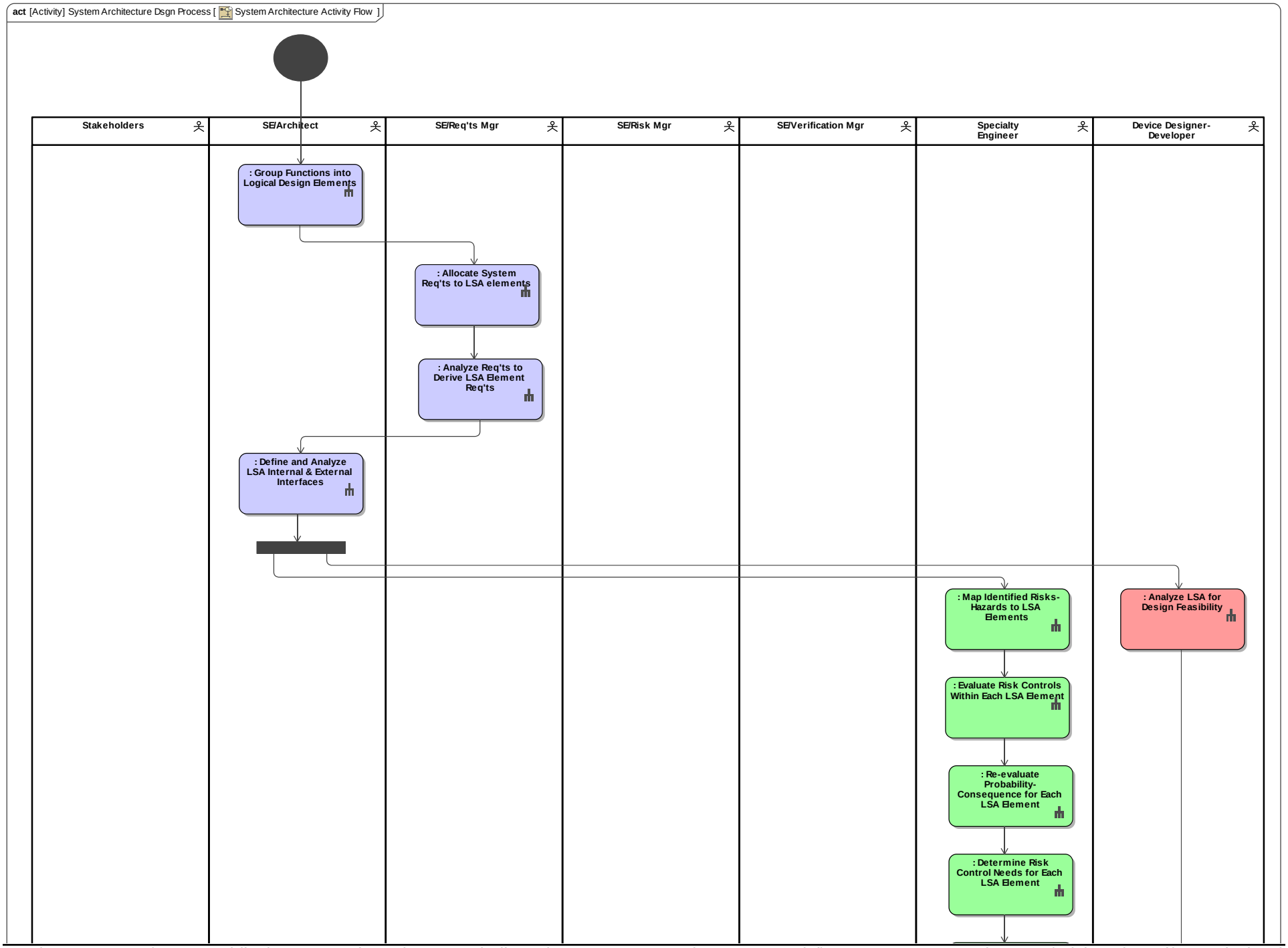
Modeling ISO 15288-ISO 14971 Integration: Process Model 3 – 6.4.3 Architecture Development Process

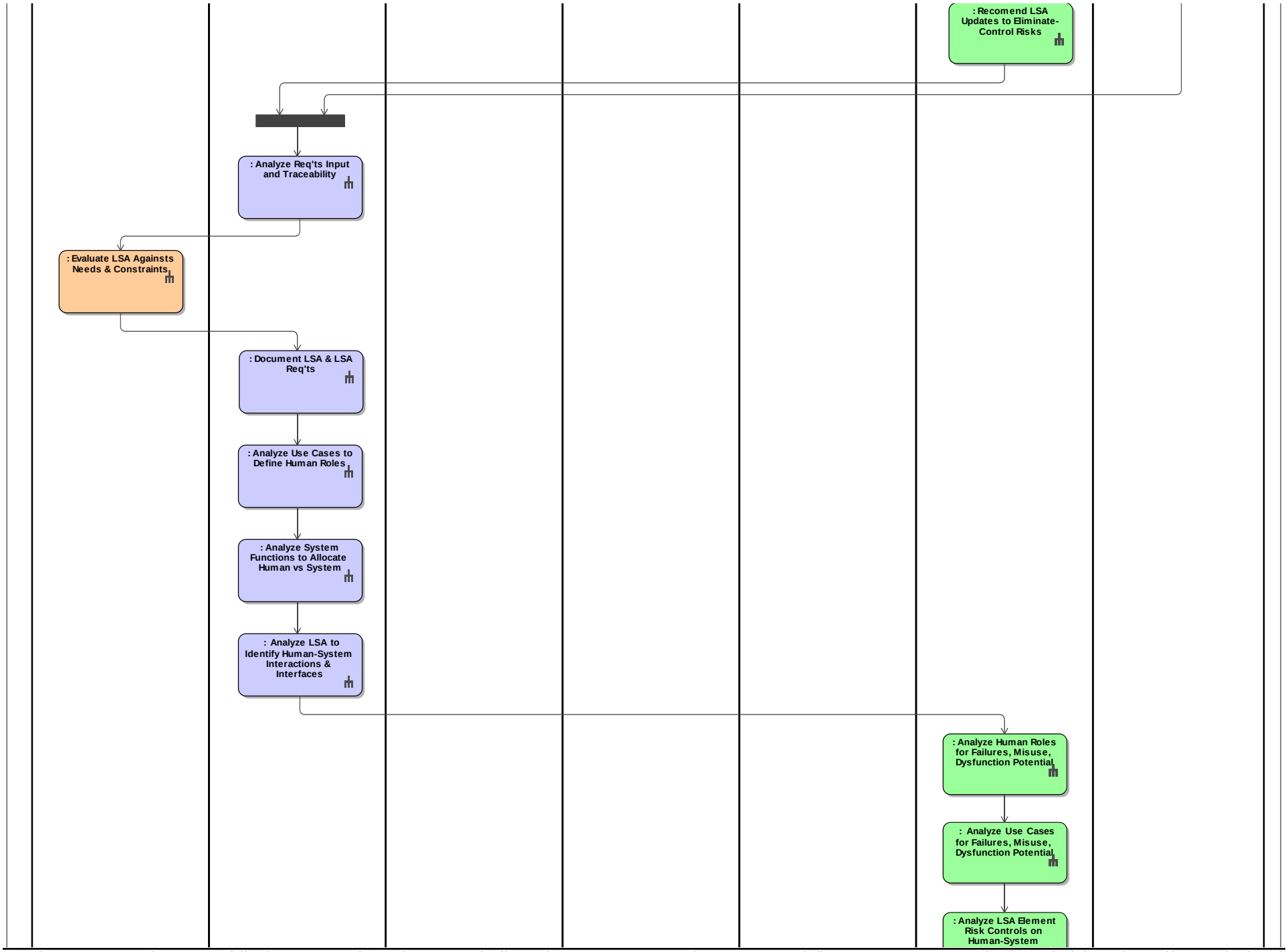

bdd [UseCase] Risk-Driven Architecture Design [System Arch Dsgn Activities]
Outcomes from ISO 15288 Technical Process 6.4.3 Architectural Design Process:
--- Architecture baseline established
--- System element descriptions to satisfy requirements are specified
--- Interface requirements are incorporated into the architecture
--- Basis for verifying system elements is defined
--- Basis for integrating system elements is defined
Stakeholders
Systems Engineer
Specialty Engineer
Device Designer-Developer
Stakeholders review the architecture and the allocation of req'ts 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 req'ts of ISO 15288 6.4.3 are satisfied.
Specialty engineers perform these actions in synch with SE and Design actions in order to satisfy the req'ts of ISO 14971 paragraphs 5.0, 6.2, and 6.2..
Design engineers perform these actions to support LSA development and to fulfill key req'ts of ISO 15288 paragraph 6.4.3.
«activity» Review & Evaluate System Architecture
«activity» Develop System Architecture
«activity» Analyze Risks-Hazards and Mitigations-Controls
«activity» Develop and Evaluate Design Alternatives
«activity» Evaluate LSA Againsts Needs & Constraints
«activity» Assess Human Roles and Operator Req'ts
«activity» Evaluate Physical Architecture Against Needs & Constraints
«activity» Define Logical System Architecture (LSA)
«activity» Analyze Human-Systems integration
«activity» Develop System Physical Architecture
«activity» Develop Third Level Assurance Case Elements
«activity» Document Architecture & System Specifications
«activity» Update Functional Risk-Hazard Analyses to LSA
«activity» Analyze Human-System Failures, Misuse, Dysfunctions
«activity» Determine Risk Control Needs for Each LSA Element
«activity» Recomend LSA Updates to Eliminate-Control Risks
«activity» Update Risk-Hazard Analyses to Physical Design Elements
«activity» Recommend Physical Design Risk Control Updates
«activity» Analyze LSA for Design Feasibility
«activity» Evaluate Physical Architecture Alternatives
«activity» Evaluate Physical Element Design Alternatives
«activity» Analyze LSA Req'ts to Derive Physical Element Specs
«activity» Develop & Analyze Risk Control Implementation Designs
«activity» Analyze & Model Physical Architecture Performance
«activity» Select & Recommend Physical Element Designs

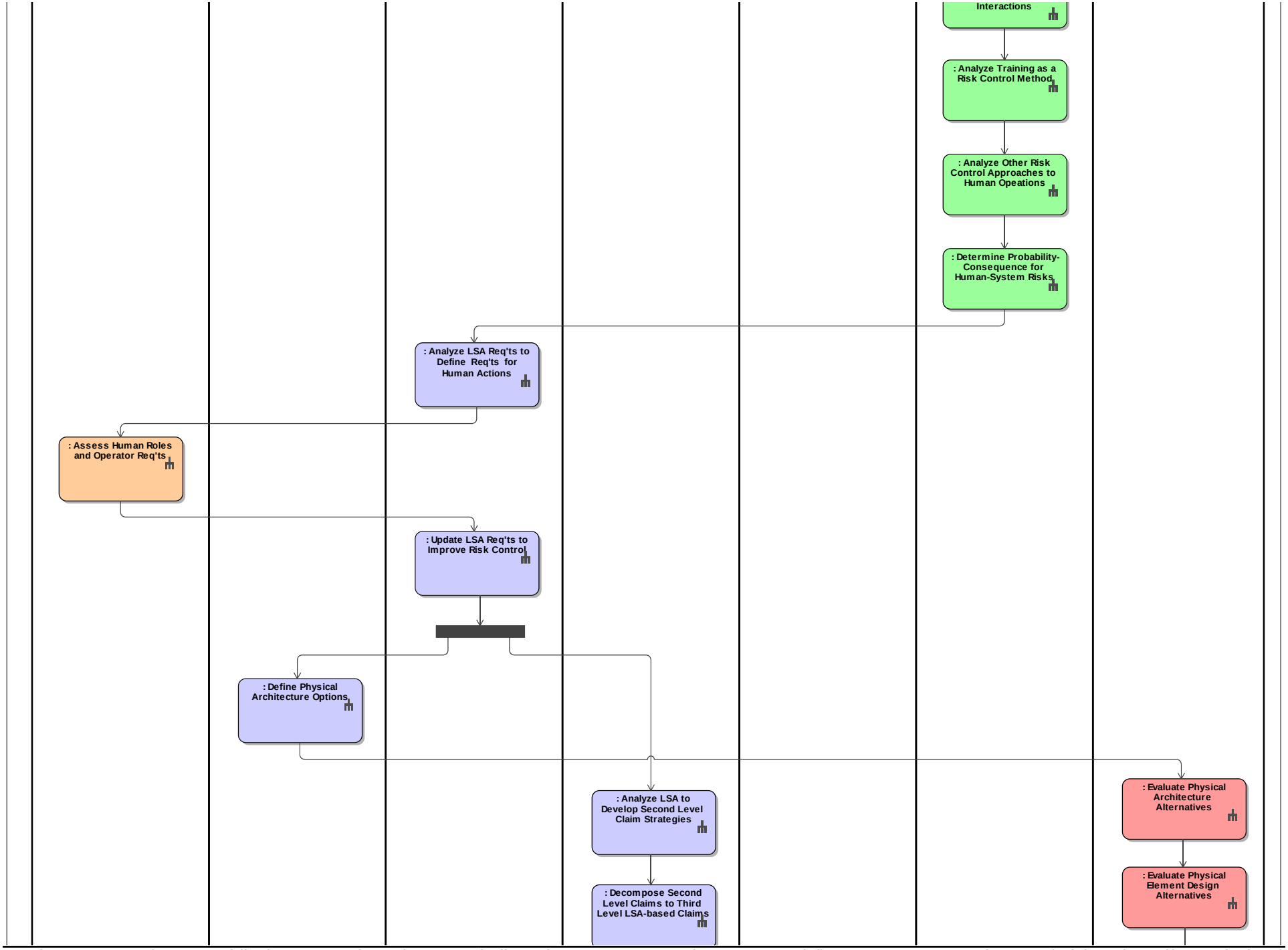

bdd [Activity] Analyze Risks-Hazards and Mitigations-Controls [Risks-Mitigations Details]
«activity»
Analyze Risks-Hazards and Mitigations-Controls
«activity»
Update Functional Risk-Hazard Analyses to LSA
«activity»
Analyze Human-System Failures, Misuse, Dysfunctions
«activity»
Determine Risk Control Needs for Each LSA Element
«activity»
Recomend LSA Updates to Eliminate-Control Risks
«activity»
Map Identified Risks-Hazards to LSA Elements
«activity»
Re-evaluate Probability-Consequence for Each LSA Element
«activity»
Evaluate Risk Controls Within Each LSA Element
«activity»
Analyze Human Roles for Failures, Misuse, Dysfunction Potential
«activity»
Analyze Use Cases for Failures, Misuse, Dysfunction Potential
«activity»
Analyze LSA Element Risk Controls on Human-System Interactions
«activity»
Analyze Training as a Risk Control Method
«activity»
Analyze Other Risk Control Approaches to Human Opeations
«activity»
Determine Probability-Consequence for Human-System Risks
«activity»
Update Risk-Hazard Analyses to Physical Design Elements
«activity»
Recommend Physical Design Risk Control Updates
«activity»
Re-evaluate Probability Consequence Analyses
«activity»
Map LSA Risks-Hazards to Physical Elements
«activity»
Evaluate Physical Element Specs Against Risk Cointrol Needs
«activity»
Evaluate Risk Controls Within Each Physical Element

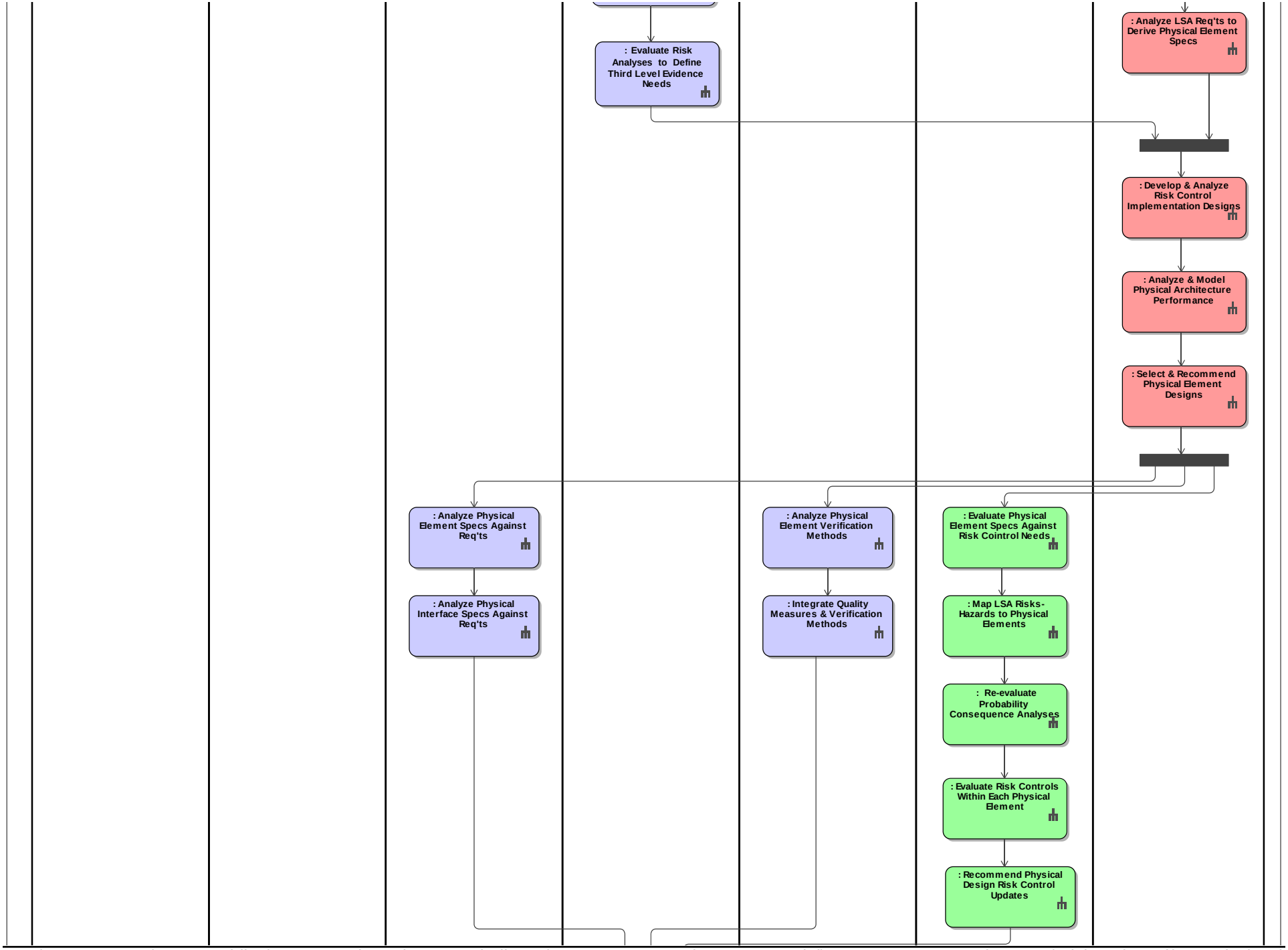

bdd [Activity] Develop System Architecture [SE Details for System Arch Devel]
«activity»
Develop System Architecture
«activity»
Define Logical System Architecture (LSA)
«activity»
Analyze Human-Systems integration
«activity»
Develop System Physical Architecture
«activity»
Develop Third Level Assurance Case Elements
«activity»
Document Architecture & System Specifications
«activity»
Group Functions into Logical Design Elements
«activity»
Allocate System Req'ts to LSA elements
«activity»
Analyze Req'ts to Derive LSA Element Req'ts
«activity»
Define and Analyze LSA Internal & External Interfaces
«activity»
Analyze Req'ts Input and Traceability
«activity»
Document LSA & LSA Req'ts
«activity»
Analyze Use Cases to Define Human Roles
«activity»
Analyze System Functions to Allocate Human vs System
«activity»
Analyze LSA to Identify Human-System Interactions & Interfaces
«activity»
Analyze LSA Req'ts to Define Req'ts for Human Actions
«activity»
Define Physical Architecture Options
«activity»
Analyze Physical Element Specs Against Req'ts
«activity»
Analyze Physical Interface Specs Against Req'ts
«activity»
Analyze Physical Element Verification Methods
«activity»
Analyze LSA to Develop Second Level Claim Strategies
«activity»
Decompose Second Level Claims to Third Level LSA-based Claims
«activity»
Evaluate Risk Analyses to Define Third Level Evidence Needs
«activity»
Update LSA Req'ts to Improve Risk Control
«activity»
Align Third Level Claims/Evidence to Physical Arch
«activity»
Evaluate Physical Element Specs Against Evidence Needs
«activity»
Update Specs & Verification Approaches
«activity»
Update Physical Element Req'ts to Improve Risk Control
«activity»
Integrate Quality Measures & Verification Methods
«activity»
Integrate Logical & Physical Architecture Descpns
«activity»
Document Traceability of LSA Req'ts & Physical Element Specs

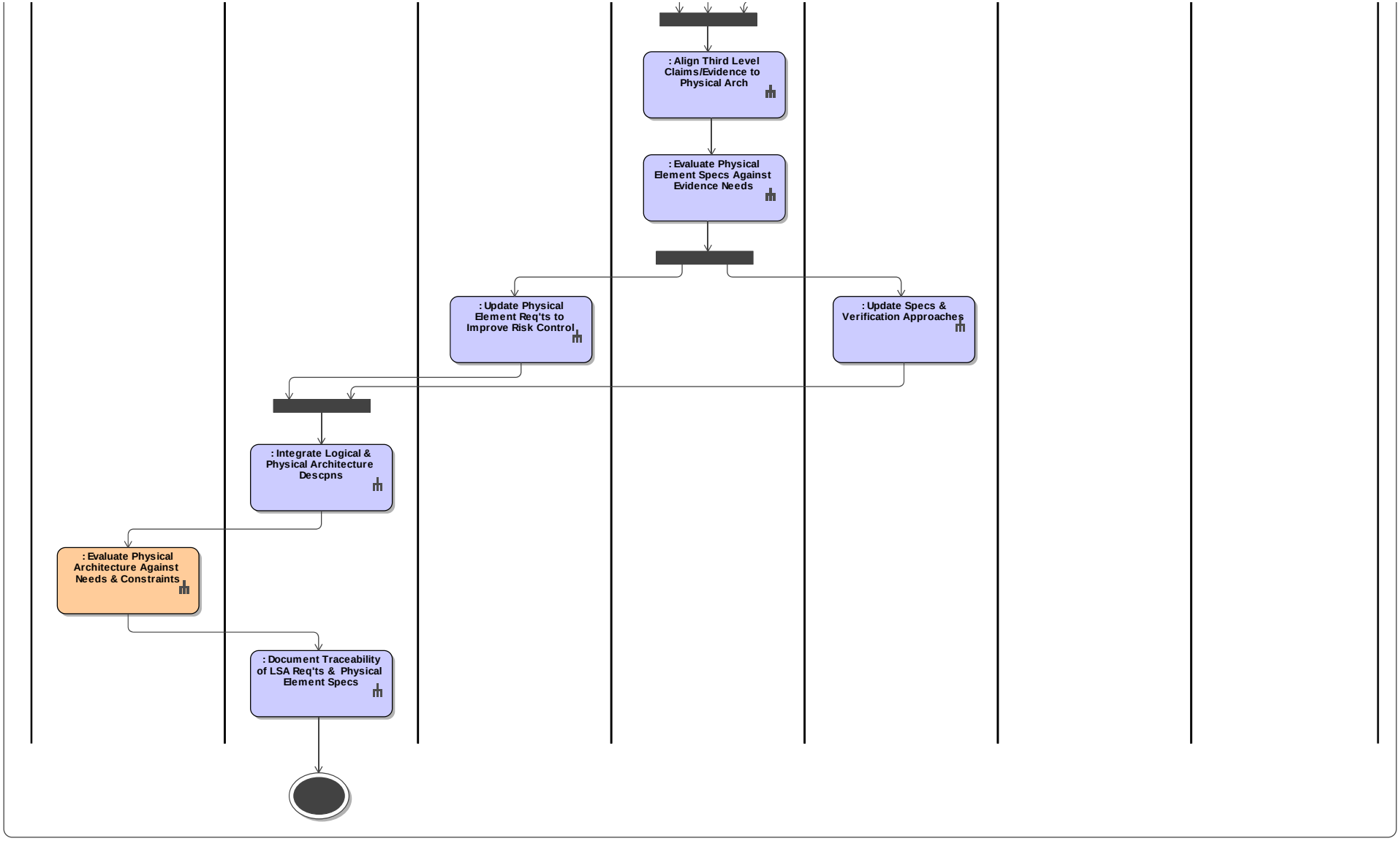

act [Activity] System Architecture Dsgn Process [System Architecture Related Info Exchange]
Outcomes from ISO 15288 Technical Process 6.4.3 Architectural Design Process:
--- Architecture baseline established
--- System element descriptions to satisfy requirements are specified
--- Interface requirements are incorporated into the architecture
--- Basis for verifying system elements is defined
--- Basis for integrating system elements is defined
: Review & Evaluate System Architecture
Physical Arch Descpn & Traceability
Human Roles, Interfaces, Risk Controls
LSA Descpn & Traceability
LSA Traceability Validation
Human Role Risk Mitigation Validation
Physical Arch Traceability Validation
LSA Descpn & Traceability
Human Roles, Interfaces, Risk Controls
Physical Arch Descpn & Traceability
: Develop System Architecture
Physical Arch Traceability Validation
Human Role Risk Mitigation Validation
LSA Traceability Validation
Physical Arch Risk Control Recommendations
Physical Element Risk Analyses
LSA Risk Control Recommendations
Human-Systems Risk Analyses
Risk Analyses for LSA
Physical Dsgn Verification Approaches
Physical Dsgn Perf Analyses
Physical Dsgn Specs
Physical Dsgn Elements
Physical Dsgn Alternatives
LSA Dsgn Analyses
LSA Descpn
H-S Integration
Physical Arch Alternatives
LSA Risk Control Recommendations
Human-Systems Risk Analyses
Risk Analyses for LSA
LSA Dsgn Analyses
Physical Dsgn Alternatives
Physical Dsgn Elements
Physical Dsgn Specs
: Analyze Risks-Hazards and Mitigations-Controls
LSA Descpn
H-S Integration
Physical Arch Alternatives
: Develop and Evaluate Design Alternatives
Physical Element Risk Analyses
Physical Arch Risk Control Recommendations
H-S Integration
LSA Descpn
Physical Dsgn Perf Analyses
Physical Dsgn Verification Approaches
Physical Element Risk Control Dsgns
Risk Control Performance Analyses
Physical Element Risk Control Dsgns
Risk Control Performance Analyses


act [Activity] System Architecture Dsgn Process [System Architecture Activity Flow]
Stakeholders
SE/Architect
SE/Req'ts Mgr
SE/Risk Mgr
SE/Verification Mgr
Specialty Engineer
Device Designer-Developer
: Group Functions into Logical Design Elements
: Allocate System Req'ts to LSA elements
: Analyze Req'ts to Derive LSA Element Req'ts
: Define and Analyze LSA Internal & External Interfaces
: Map Identified Risks-Hazards to LSA Elements
: Analyze LSA for Design Feasibility
: Evaluate Risk Controls Within Each LSA Element
: Re-evaluate Probability-Consequence for Each LSA Element
: Determine Risk Control Needs for Each LSA Element


: Recomend LSA Updates to Eliminate-Control Risks
: Analyze Req'ts Input and Traceability
: Evaluate LSA Againsts Needs & Constraints
: Document LSA & LSA Req'ts
: Analyze Use Cases to Define Human Roles
: Analyze System Functions to Allocate Human vs System
: Analyze LSA to Identify Human-System Interactions & Interfaces
: Analyze Human Roles for Failures, Misuse, Dysfunction Potential
: Analyze Use Cases for Failures, Misuse, Dysfunction Potential
: Analyze LSA Element Risk Controls on Human-System

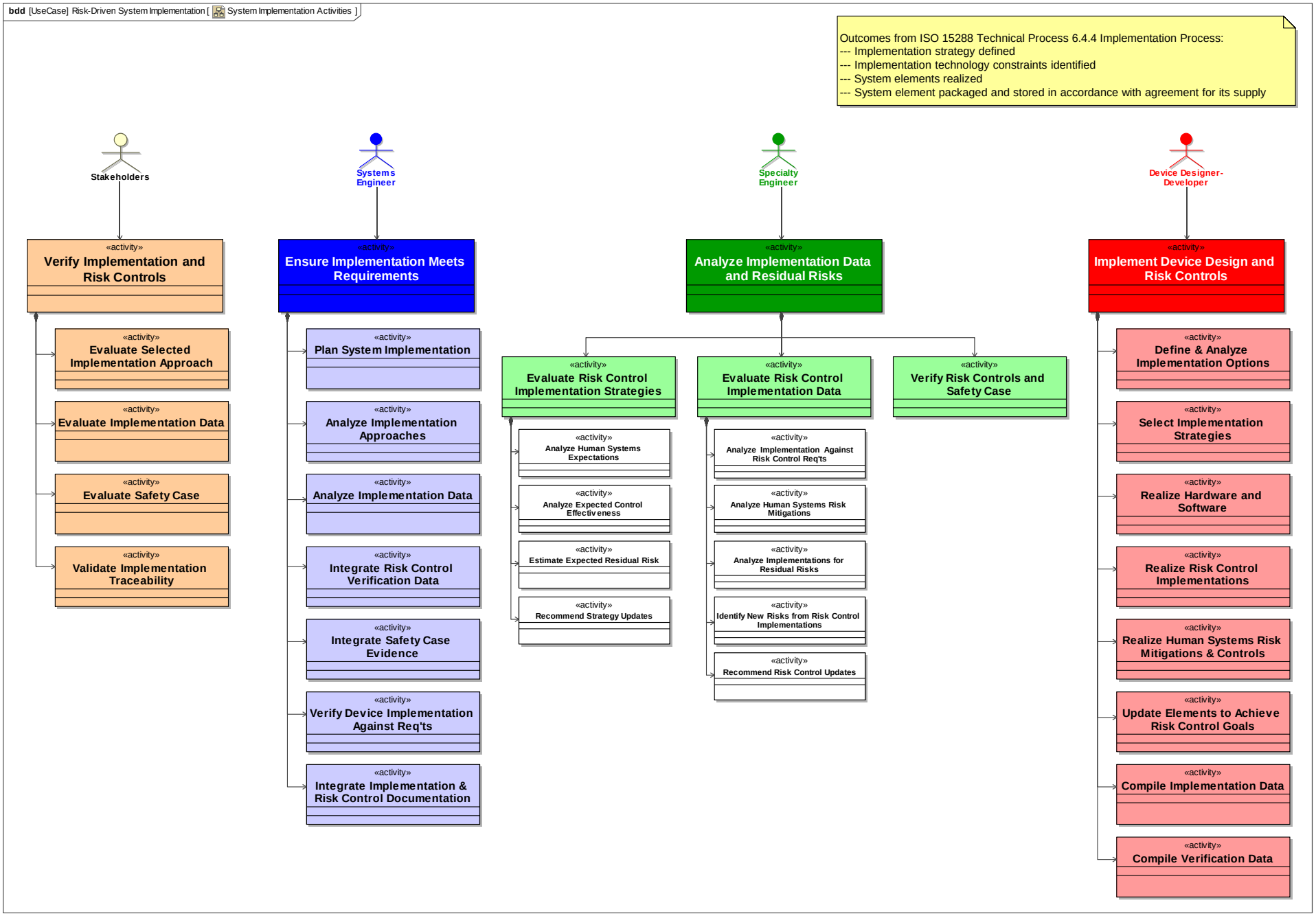

Interactions
: Analyze Training as a Risk Control Method
: Analyze Other Risk Control Approaches to Human Opeations
: Determine Probability-Consequence for Human-System Risks
: Analyze LSA Req'ts to Define Req'ts for Human Actions
: Assess Human Roles and Operator Req'ts
: Update LSA Req'ts to Improve Risk Control
: Define Physical Architecture Options
: Analyze LSA to Develop Second Level Claim Strategies
: Decompose Second Level Claims to Third Level LSA-based Claims
: Evaluate Physical Architecture Alternatives
: Evaluate Physical Element Design Alternatives

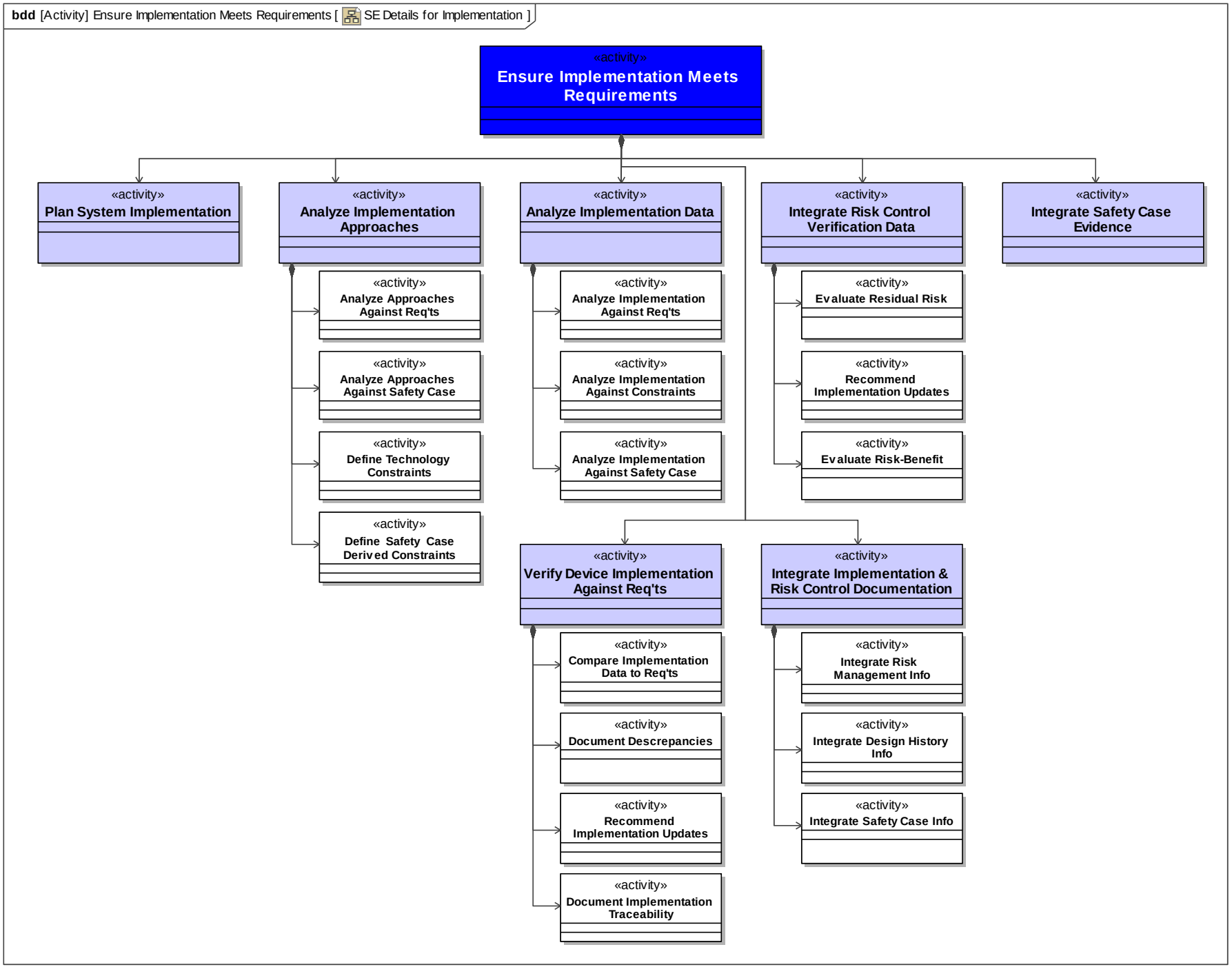

: Evaluate Risk Analyses to Define Third Level Evidence Needs
: Analyze LSA Req'ts to Derive Physical Element Specs
: Develop & Analyze Risk Control Implementation Designs
: Analyze & Model Physical Architecture Performance
: Select & Recommend Physical Element Designs
: Analyze Physical Element Specs Against Req'ts
: Analyze Physical Interface Specs Against Req'ts
: Analyze Physical Element Verification Methods
: Integrate Quality Measures & Verification Methods
: Evaluate Physical Element Specs Against Risk Cointrol 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

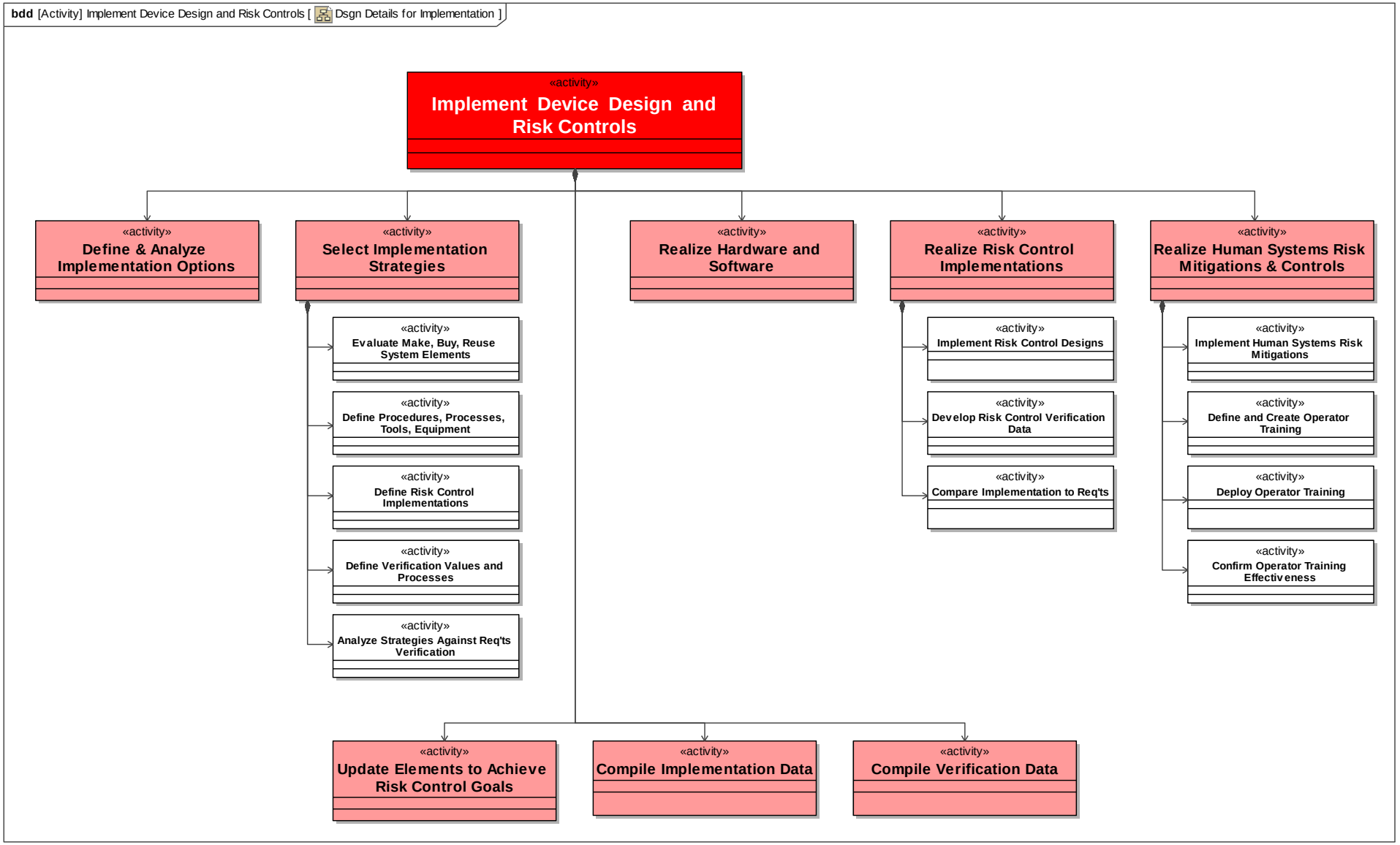

: Align Third Level Claims/Evidence to Physical Arch
: Evaluate Physical Element Specs Against Evidence Needs
: Update Physical Element Req'ts to Improve Risk Control
: Update Specs & Verification Approaches
: Integrate Logical & Physical Architecture Descpns
: Evaluate Physical Architecture Against Needs & Constraints
: Document Traceability of LSA Req'ts & Physical Element Specs

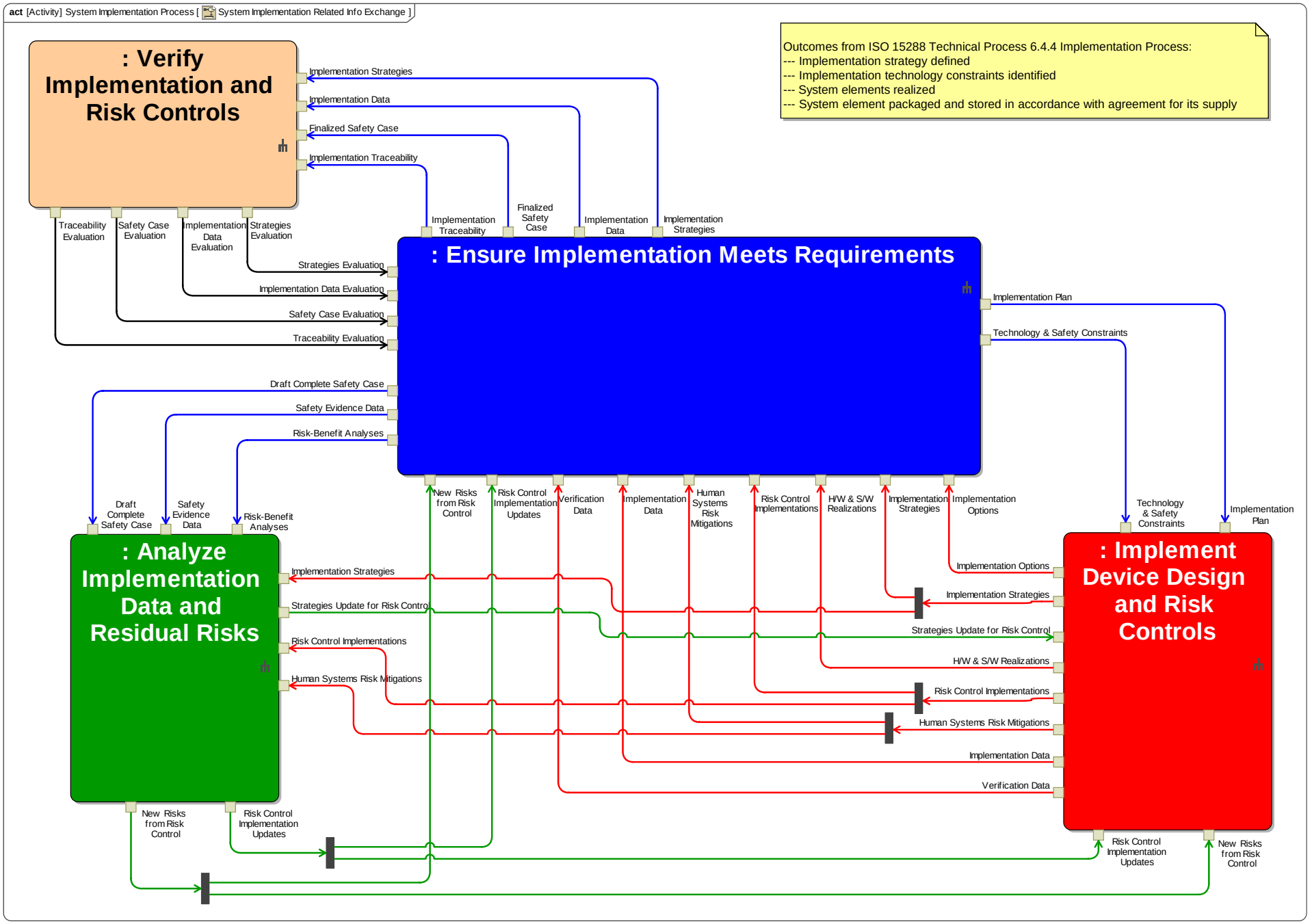
Applying Risk-Hazard-Safety Management Across the System Lifecycle

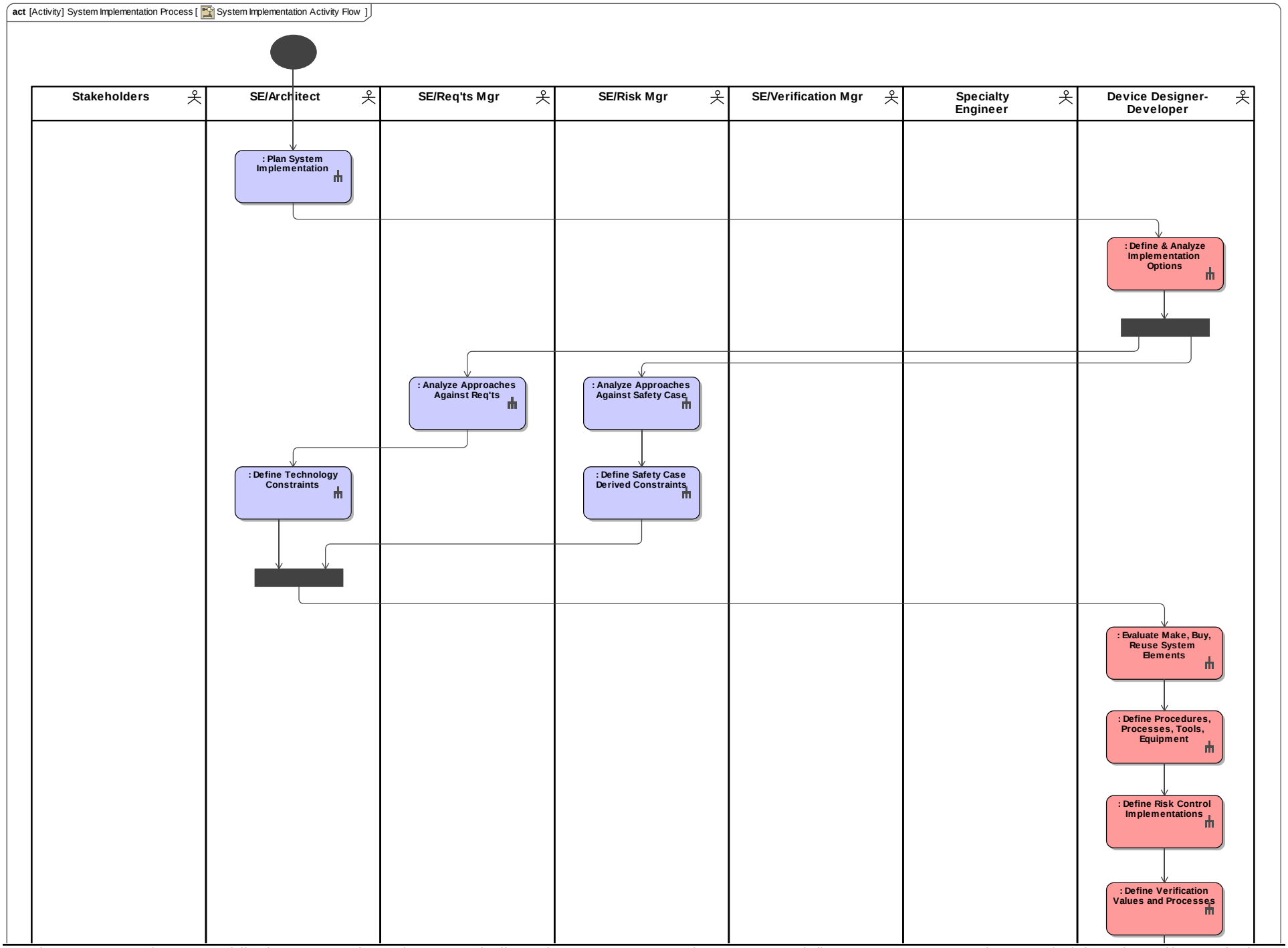
Modeling ISO 15288-ISO 14971 Integration: Process Model 4 – 6.4.4 System Implementation Process

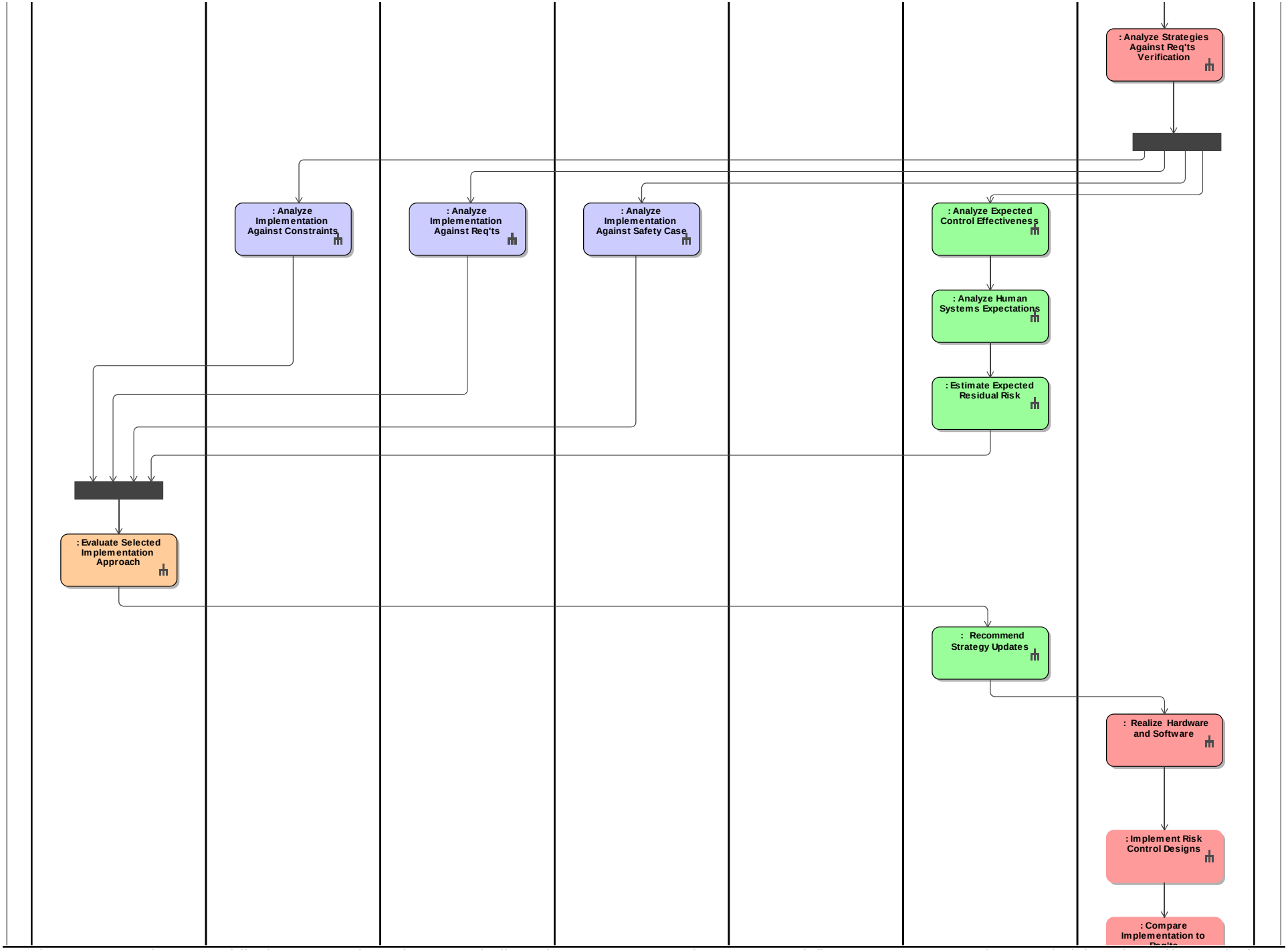

bdd [UseCase] Risk-Driven System Implementation [System Implementation Activities]
Outcomes from ISO 15288 Technical Process 6.4.4 Implementation Process:
--- Implementation strategy defined
--- Implementation technology constraints identified
--- System elements realized
--- System element packaged and stored in accordance with agreement for its supply
Stakeholders
Systems Engineer
Specialty Engineer
Device Designer-Developer
«activity» Verify Implementation and Risk Controls
«activity» Evaluate Selected Implementation Approach
«activity» Evaluate Implementation Data
«activity» Evaluate Safety Case
«activity» Validate Implementation Traceability
«activity» Ensure Implementation Meets Requirements
«activity» Plan System Implementation
«activity» Analyze Implementation Approaches
«activity» Analyze Implementation Data
«activity» Integrate Risk Control Verification Data
«activity» Integrate Safety Case Evidence
«activity» Verify Device Implementation Against Req'ts
«activity» Integrate Implementation & Risk Control Documentation
«activity» Analyze Implementation Data and Residual Risks
«activity» Evaluate Risk Control Implementation Strategies
«activity» Analyze Human Systems Expectations
«activity» Analyze Expected Control Effectiveness
«activity» Estimate Expected Residual Risk
«activity» Recommend Strategy Updates
«activity» Evaluate Risk Control Implementation Data
«activity» Analyze Implementation Against Risk Control Req'ts
«activity» Analyze Human Systems Risk Mitigations
«activity» Analyze Implementations for Residual Risks
«activity» Identify New Risks from Risk Control Implementations
«activity» Recommend Risk Control Updates
«activity» Verify Risk Controls and Safety Case
«activity» Implement Device Design and Risk Controls
«activity» Define & Analyze Implementation Options
«activity» Select Implementation Strategies
«activity» Realize Hardware and Software
«activity» Realize Risk Control Implementations
«activity» Realize Human Systems Risk Mitigations & Controls
«activity» Update Elements to Achieve Risk Control Goals
«activity» Compile Implementation Data
«activity» Compile Verification Data

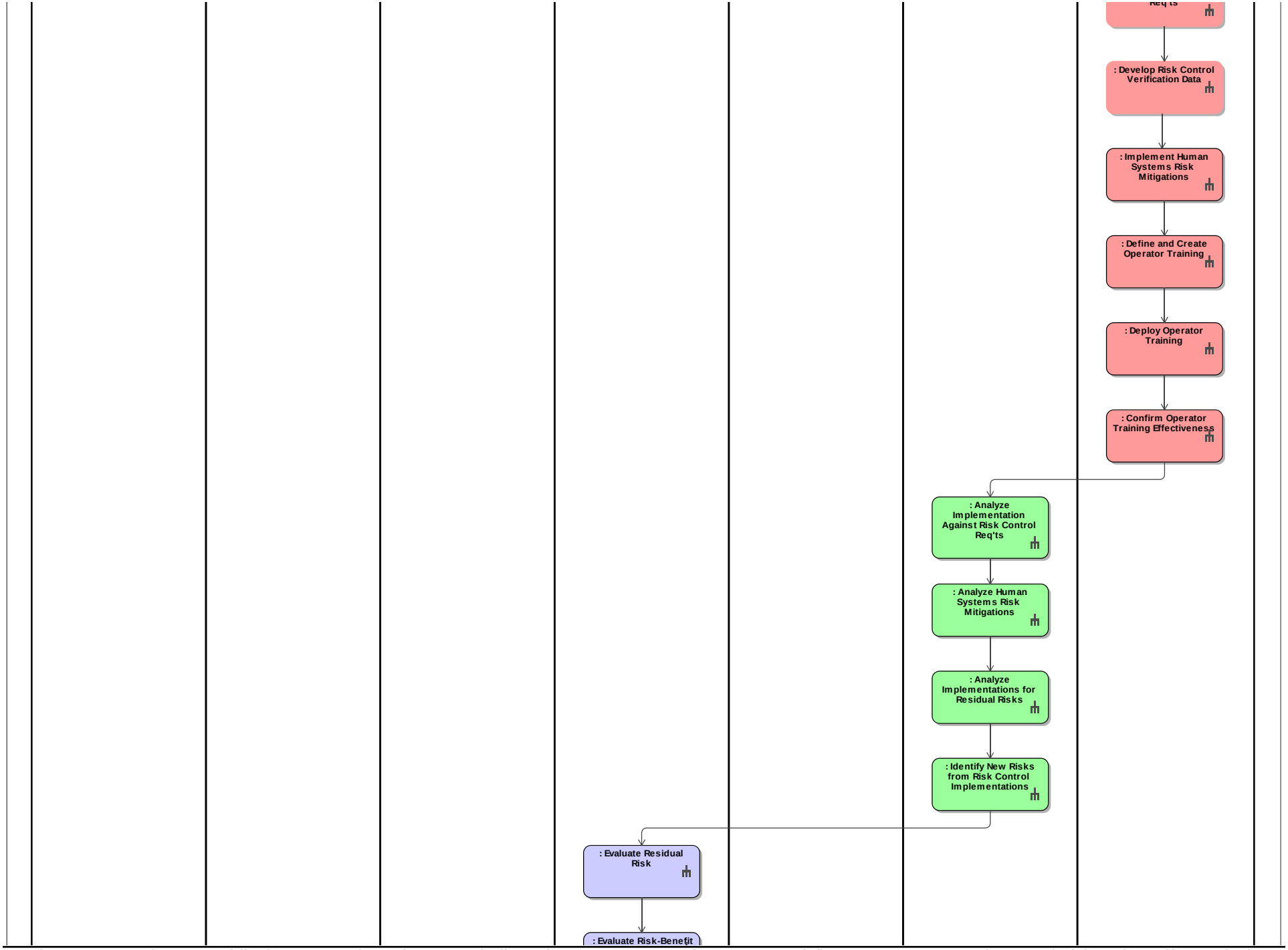

bdd [Activity] Ensure Implementation Meets Requirements [SE Details for Implementation]
«activity»
Ensure Implementation Meets Requirements
«activity»
Plan System Implementation
«activity»
Analyze Implementation Approaches
«activity»
Analyze Approaches Against Req'ts
«activity»
Analyze Approaches Against Safety Case
«activity»
Define Technology Constraints
«activity»
Define Safety Case Derived Constraints
«activity»
Analyze Implementation Data
«activity»
Analyze Implementation Against Req'ts
«activity»
Analyze Implementation Against Constraints
«activity»
Analyze Implementation Against Safety Case
«activity»
Integrate Risk Control Verification Data
«activity»
Evaluate Residual Risk
«activity»
Recommend Implementation Updates
«activity»
Evaluate Risk-Benefit
«activity»
Integrate Safety Case Evidence
«activity»
Verify Device Implementation Against Req'ts
«activity»
Compare Implementation Data to Req'ts
«activity»
Document Descrepancies
«activity»
Recommend Implementation Updates
«activity»
Document Implementation Traceability
«activity»
Integrate Implementation & Risk Control Documentation
«activity»
Integrate Risk Management Info
«activity»
Integrate Design History Info
«activity»
Integrate Safety Case Info

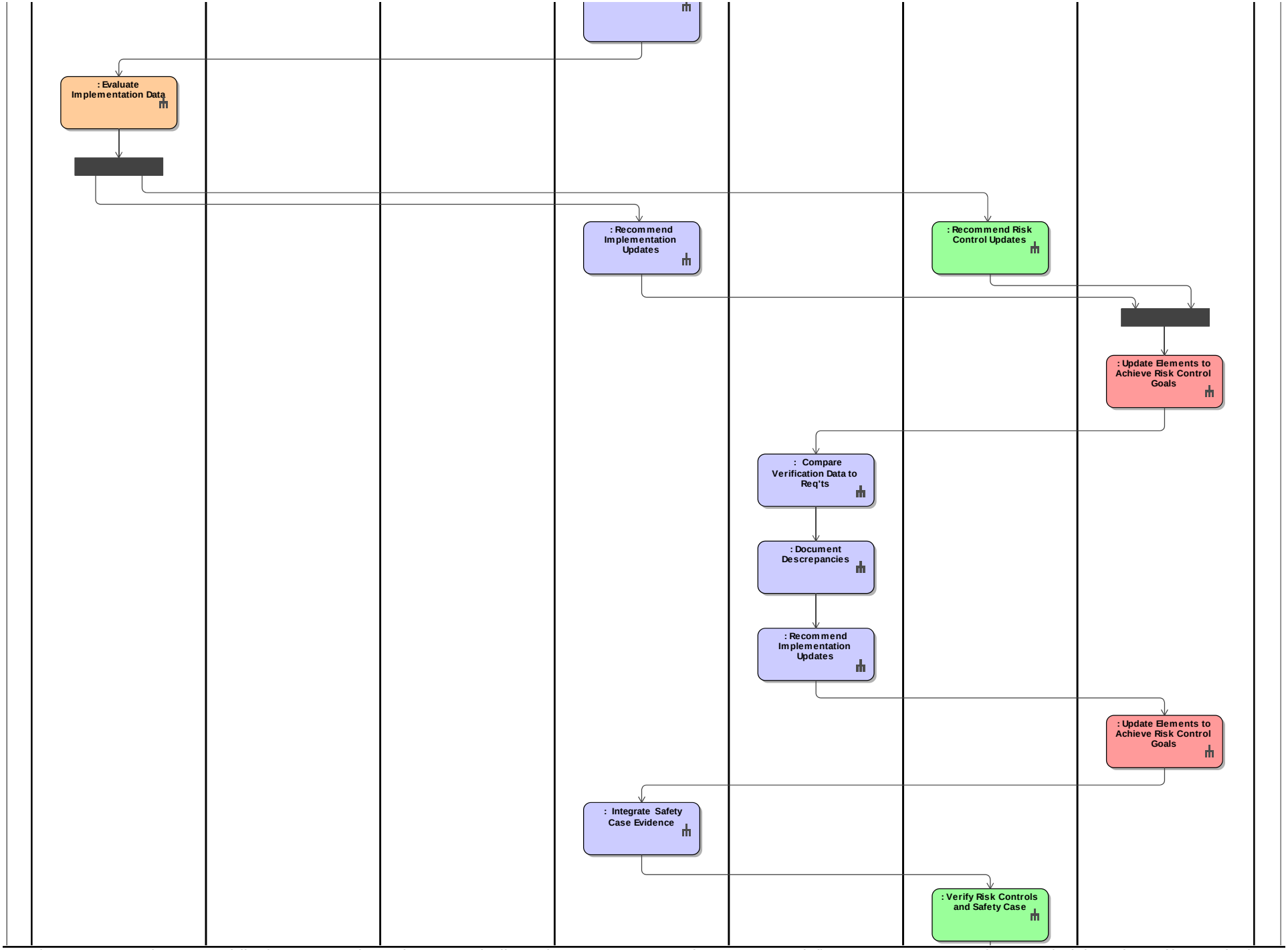

bdd [Activity] Implement Device Design and Risk Controls [Dsgn Details for Implementation]
«activity»
Implement Device Design and Risk Controls
«activity»
Define & Analyze Implementation Options
«activity»
Select Implementation Strategies
«activity»
Realize Hardware and Software
«activity»
Realize Risk Control Implementations
«activity»
Realize Human Systems Risk Mitigations & Controls
«activity»
Evaluate Make, Buy, Reuse System Elements
«activity»
Define Procedures, Processes, Tools, Equipment
«activity»
Define Risk Control Implementations
«activity»
Define Verification Values and Processes
«activity»
Analyze Strategies Against Req'ts Verification
«activity»
Implement Risk Control Designs
«activity»
Develop Risk Control Verification Data
«activity»
Compare Implementation to Req'ts
«activity»
Implement Human Systems Risk Mitigations
«activity»
Define and Create Operator Training
«activity»
Deploy Operator Training
«activity»
Confirm Operator Training Effectiveness
«activity»
Update Elements to Achieve Risk Control Goals
«activity»
Compile Implementation Data
«activity»
Compile Verification Data

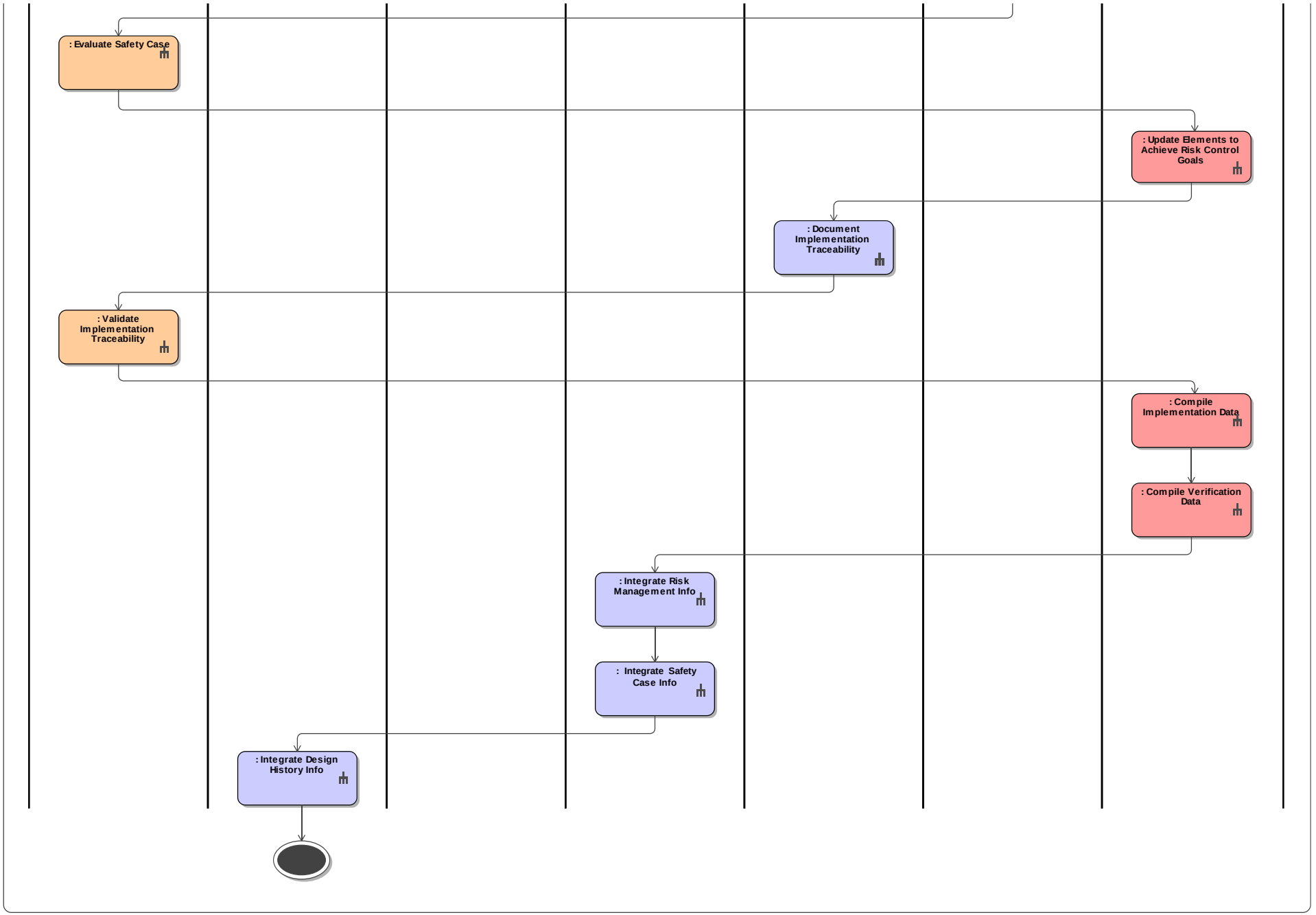

act [Activity] System Implementation Process [System Implementation Related Info Exchange]
: Verify Implementation and Risk Controls
Outcomes from ISO 15288 Technical Process 6.4.4 Implementation Process:
--- Implementation strategy defined
--- Implementation technology constraints identified
--- System elements realized
--- System element packaged and stored in accordance with agreement for its supply
Implementation Strategies
Implementation Data
Finalized Safety Case
Implementation Traceability
Traceability Evaluation
Safety Case Evaluation
Implementation Data Evaluation
Strategies Evaluation
: Ensure Implementation Meets Requirements
Implementation Plan
Technology & Safety Constraints
Draft Complete Safety Case
Safety Evidence Data
Risk-Benefit Analyses
New Risks from Risk Control
Risk Control Implementation Updates
Verification Data
Human Systems Risk Mitigations
H/W & S/W Realizations
Implementation Options
: Analyze Implementation Data and Residual Risks
: Implement Device Design and Risk Controls


act [Activity] System Implementation Process [System Implementation Activity Flow]
Stakeholders
SE/Architect
SE/Req'ts Mgr
SE/Risk Mgr
SE/Verification Mgr
Specialty Engineer
Device Designer-Developer
: Plan System Implementation
: Define & Analyze Implementation Options
: Analyze Approaches Against Req'ts
: Analyze Approaches Against Safety Case
: Define Technology Constraints
: Define Safety Case Derived Constraints
: 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
: Analyze Implementation Against Constraints
: Analyze Implementation Against Req'ts
: Analyze Implementation Against Safety Case
: Analyze Expected Control Effectiveness
: Analyze Human Systems Expectations
: Estimate Expected Residual Risk
: Evaluate Selected Implementation Approach
: Recommend Strategy Updates
: Realize Hardware and Software
: Implement Risk Control Designs
: Compare Implementation to


: Develop Risk Control Verification Data
: Implement Human Systems Risk Mitigations
: Define and Create Operator Training
: Deploy Operator Training
: Confirm Operator Training Effectiveness
: Analyze Implementation Against Risk Control Req'ts
: Analyze Human Systems Risk Mitigations
: Analyze Implementations for Residual Risks
: Identify New Risks from Risk Control Implementations
: Evaluate Residual Risk
: Evaluate Risk-Benefit


: Evaluate Implementation Data
: Recommend Implementation Updates
: Recommend Risk Control Updates
: Update Elements to Achieve Risk Control Goals
: Compare Verification Data to Req'ts
: Document Descrepancies
: Recommend Implementation Updates
: Update Elements to Achieve Risk Control Goals
: Integrate Safety Case Evidence
: Verify Risk Controls and Safety Case


: Evaluate Safety Case
: Update Elements to Achieve Risk Control Goals
: Document Implementation Traceability
: Validate Implementation Traceability
: Compile Implementation Data
: Compile Verification Data
: Integrate Risk Management Info
: Integrate Safety Case Info
: Integrate Design History Info