Review Document For

Systems Engineering Workflow Use Case:

Evaluate System Safety

Last Updated: April 13, 2015, 2:26 PM

Table of Contents

[1. Introduction 4](#_Toc416617238)

[1.1. Intent 4](#_Toc416617239)

[1.2. Assumptions 4](#_Toc416617240)

[2. Context 4](#_Toc416617241)

[3. Items to Review 5](#_Toc416617242)

[3.1. "Evaluate System Safety" Use Case 5](#_Toc416617243)

[3.1.1. Use Case Attributes 5](#_Toc416617244)

[3.1.2. Use Case Description 5](#_Toc416617245)

[3.1.3. Use Case Related Diagrams 7](#_Toc416617246)

[3.1.4. Other Called Activities 11](#_Toc416617247)

[4. Supporting Information 12](#_Toc416617248)

[4.1. Called Activities 12](#_Toc416617249)

[4.1.1. Measure a Change Impact 12](#_Toc416617250)

[4.1.2. Conduct a Review 13](#_Toc416617251)

[4.1.3. Import Reference Materiel into Model 14](#_Toc416617252)

[4.2. Table of Definitions 14](#_Toc416617253)

[4.3. Table of Use Case List 14](#_Toc416617254)

[4.4. Table of Actors 14](#_Toc416617255)

Table of Figures

[Figure 1: Systems Engineering Workflow Use Case Context 5](#_Toc416617275)

[Figure 2: Specialty Engineering 7](#_Toc416617276)

[Figure 3: Evaluate System Safety 8](#_Toc416617277)

[Figure 4: Analyze System Hazards 9](#_Toc416617278)

[Figure 5: Design S0I with Safety Measures 10](#_Toc416617279)

[Figure 6: Safety Related Terms 11](#_Toc416617280)

[Figure 7: Measure a Change Impact 12](#_Toc416617281)

[Figure 8: Conduct a Review 13](#_Toc416617282)

[Figure 9: Import Reference Materiel into Model 14](#_Toc416617283)

Table of Tables

[Table 1: Definition of Terms 14](#_Toc416617284)

[Table 2: List of Use Cases 17](#_Toc416617285)

[Table 3: List of Actors 18](#_Toc416617286)

# Introduction

## Intent

The intent of this document is to provide the material required to support the review of the use case "Evaluate System Safety". Use the Word "Track Changes" features to suggest changes and add comments as necessary to log questions and comments. The section called "Items to Review" contains the artifacts that are to be evaluated for this review. The additional material in this document is intended to provide the appropriate context and definitions to support the review.

## Assumptions

1. The workflow use cases defined are intended to be used on large complex systems supported by large geographically diverse development teams. With smaller and simpler systems some of the use cases may not be needed or, they may require a simpler workflow. 2. The workflow use cases are described assuming a model-based approach is used to develop a system. However, many of the use cases are not dependent on using model-based techniques, since they are the very same use cases System Engineers have been using before model-based techniques were available.

# Context

The diagram below defines a typical Product Domain structure. Within this domain is the SE Development System. Systems Engineering Development System (SEDS) is the context for the Systems Engineering Workflow Use Cases. It is the system used to provide an integrated environment of tools and capabilities required to perform Systems Engineering activities and tasks. This includes the environment to support system requirements flowdown, design, analysis, verification, validation activities. The SEDS provides interfaces to external domains such as the software, mechanical, electrical engineering domains and interfaces to manufacturing, support and product management domains.

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID 6b333c0f-624b-401e-bcf2-e59ea05cc4b3.emf

Figure 1: Systems Engineering Workflow Use Case Context

# Items to Review

## "Evaluate System Safety" Use Case

### Use Case Attributes

1. The location of the use case being reviewed, "Evaluate System Safety", in the model browser is "System Engineering Operations::System Engineering Development System::SE Life Cycle Workflow Use Cases::System Development Stage::SE Domain Workflow Use Cases::Evaluate System Safety". 2. The Maturity Level is listed as "Early Activity".3. The Selection Status is listed as "Selected & Pattern".

### Use Case Description

**Goal -** The goal of this workflow use case is to evaluate the system for safety related hazards and derive a plan to mitigate these risks. **Primary Actor -Secondary Actors -Preconditions -Activity –**

1. Identify applicable safety standards
2. Identify Safety Hazards undesired events and their causes
3. Determine Risk level of each hazard
4. Analyze Hazard's faults and failures
5. Define the Safety Measures
6. Create Safety Requirements
7. Provide traceability from Safety measures to faults and to hazards
8. Conduct analysis to determine the severity level, the probability of occurrence and assess the level of risk.
9. Determine if the analysis results are acceptable for use.
   1. If it is acceptable, capture these results and show tractability to identified Hazard.
   2. If not, determine best corrective solution to eliminate or minimize the level of risk. This could be by design and/or by procedure/process
   3. Update Model and other information base
      1. Derive Safety related requirements that address Hazards.
      2. Show how these requirements are satisfied
      3. Show traceability from Hazards to Risk mitigation requirements to system elements satisfying those requirements.
10. Verify solution to determine if Hazard has been appropriately addressed.

**Post Conditions -References and Citations:**  [2} References: INCOSE Systems Engineering Handbook

[3] SEBok - Concept Definition

[7] Douglas, Bruce: Safety Analysis of UML Models

### Use Case Related Diagrams

#### Use Case Diagram

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID 31336da8-8544-453c-998b-53dbde80990e.emf

Figure 2: Specialty Engineering

#### Activity Diagrams

##### Evaluate System Safety

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID ab7251c2-a812-40be-bc90-446112a2589d.emf

Figure 3: Evaluate System Safety

##### Analyze System Hazards

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID f5f26755-798b-4551-9ffc-06af9cf4d494.emf

Figure 4: Analyze System Hazards

##### Design S0I with Safety Measures

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID ea92e31c-343e-49ca-9834-6373c9087287.emf

Figure 5: Design S0I with Safety Measures

#### Block Definition Diagrams

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID cb90a1c3-c4b0-48be-a811-3f9d3f3dd043.emf

Figure 6: Safety Related Terms

### Other Called Activities

The following Call Operations are located on the above activities.

1. Import Reference Materiel
2. Measure Change Impact
3. Conduct a Review

# Supporting Information

## Called Activities

### Measure a Change Impact

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID 1e7d1c8e-daff-4f7c-b0d7-63a5a95e1d10.emf

Figure 7: Measure a Change Impact

### Conduct a Review

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID a7e59ec1-e430-42fc-953b-a3835d243dcf.emf

Figure 8: Conduct a Review

### Import Reference Materiel into Model

C:\Users\John\Documents\SystemModeling\RhapsodyAdd-ins\DocGen/figures/GUID 930d645d-66cc-4b0c-807f-82e1c4e43798.emf

Figure 9: Import Reference Materiel into Model

## Table of Definitions

Table 1: Definition of Terms

| **Name** | **Description** |
| --- | --- |
| Stakeholder Requirements Traceability | All stakeholder requirements should have bi-directional traceability, including to their source, such as the source document or the stakeholder need. |
| Concept of Deployment |  |
| Concept of Operations | Also known as "ConOps" - Describes the way the system works from the operator's perspective. The ConOps includes the user description and summarizes the needs, goals, and characteristics of the system's user community. This includes operation, maintenance, and support personnel. |
| Concept of Support | Describes the desired support infrastructure and manpower considerations for maintaining the system after it is deployed. This includes specifying equipment, procedures, facilities, and operator training requirements. |
| Concept of Production | Describes the way the system will be manufactured, including any hazardous materials used in the process. |
| Measures of Effectiveness Needs | Measures of Effectiveness (MOEs) are the "operational" measures of success that are closely related to the achievement of the mission or operational objective being evaluated, in the intended operational environment under a specified set of conditions (i.e., how well the solution achieves the intended purpose). |
| Stakeholder Requirements | Formally documented and approved stakeholder requirements that will govern the project, including: required system capabilities, functions, and/or services; quality standards; and cost and schedule constraints. |
| Validation Criteria | May specify who will perform validation activities, and the environments of the system-of-interest. |
| MOE Data | Data provided to measure the MOEs. |
| Initial RVTM | Initial Requirements Verification and Traceability Matrix - A list of requirements, their verification attributes, and traceability. |
| Analyze Needs Outputs | A collection of output artifacts for the Stakeholder Requirements Definition Process establish the initial set of stakeholder requirements for project scope and associated agreements. |
| Analyze Needs Inputs | A collection input artifacts required for the Stakeholder Requirements Definition Process. |
| Source Documents | Extract, clarify, and prioritize all of the written directives embodied in the source documents relevant to the particular stage of procurement activity. |
| Project Constraints | Includes all other constraints from the stakeholder including cost, schedule, and solution constraints. |
| Analyze Needs Controls and Enablers | A collection control and enabler artifacts required for the Stakeholder Requirements Definition Process.  This includes:  Applicable Laws and Regulations  Industry Standards - relevant industry specifications and standards  Agreements - terms and conditions of the agreements  Project Procedures and Standards - including project plans  Project Directives  Organization/Enterprise Policies, Procedures, and Standards - including guidelines and reporting mechanisms  Organization/Enterprise Infrastructure  Project Infrastructure |
| Stakeholder Needs | Description of users' and other stakeholders' needs or services that the system of interest will provide. |
| Conceptual System Architecture | The Conceptual System Architecture (CSA) is an early view of the finalized system architecture and is typically captures in the proposal stage.  The CSA describes the basic concepts and approach of the actual system architecture. Typically more detail is captured in this early stage of development in aspects of the system that are perceived to contain more risk. In a model-based environment the CSA is captured in the form of a SysML model. A document may also be generated from the CSA model to assist in the review and to help communicate to people without access to the model. |
| Review Package | The review package describes what has changed. Typically this is measured against the previous baseline. The review package contains all the changed items and any additional needed to complete the context of those changed items.  The review package should highlight what items have been added, deleted or updated, e.g. document change bars, red lines, text color changes, annotation, etc.  The review package can consist of any type of artifact, including SysML models, documents, code, parts of the system, prototypes, etc. |
| Review Comments | The Review Comments artifact is produced as a result of reviewing a Review Package. Comments may add, delete or update items in the Review Package. Comments can be captured in many different forms, i.e. document change bars, red lines, text color changes, annotation, etc.. Each comment should identify the reviewer and the time of change,  The set of comments in the Review Comments artifact can be of multiple forms, e.g. an annotated version of the review package, a separate report, etc. |
| Regulatory Documents | Regulatory compliance documents establish a set or rules, principles or usages that describe the goals that an organization, a system or equipment should implement to ensure the awareness of and take steps to comply with relevant laws and regulations. |
| Model-based Systems Engineering | "Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases".  Ref - International Council on Systems Engineering (INCOSE), Systems Engineering Vision 2020, Version 2.03, TP-2004-004-02, September 2007. |
| Model-based Systems Development | Model-based Systems Development (MBSD) is the formalized application of modeling to support all aspects of product engineering and support system requirements, design, implementation, analysis, verification, validation, manufacturing, support and management activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases. Therefore MBSD includes domains such as MBSE, software design and implementation and mechanical design and implementation, and electrical design and implementation. |
| Product Development System | Product Development System (PDS) is the system used to provide an integrated environment of tools and capabilities required to develop products that are systems. This includes the environment for systems engineering, software design and implementation engineering, mechanical design and implementation engineering, electrical design and implementation engineering and interfaces to external domains including manufacturing support and product management. |
| System Of Interest | The system whose life cycle is under consideration (INCOSE SE Handbook). |
| Hazard | A hazard is system state that when combined with other environmental conditions inevitably leads to an accident [7]. |
| Fault | A safety fault is a non-conformance of a system that leads to a hazard [7]. |
| Safety Measure | Safety measures are activities and precautions taken to improve safety, i.e. reduce risk related to human health. [6].  A safety measure could be used to detect or mitigate a fault [7]. |
| Safety Report | The result of a safety analysis and evaluation. |

## Table of Use Case List

Table 2: List of Use Cases

| **Owner** | **Name** |
| --- | --- |
| Exploratory and Concept Stage | Response to a Customer Request |
| Exploratory and Concept Stage | Analyze Stakeholders Needs |
| Exploratory and Concept Stage | Derive System Requirements |
| Exploratory and Concept Stage | Analyze System Life-cycle Costs |
| Management Workflow Use Cases | Plan a Development Cycle |
| Management Workflow Use Cases | Manage SE Development Progress |
| Management Workflow Use Cases | Manage SE Development Environment |
| Management Workflow Use Cases | Create a Baseline |
| SE Domain Workflow Use Cases | Derive Product Architecture |
| SE Domain Workflow Use Cases | Evaluate System Safety |
| SE Domain Workflow Use Cases | Perform System RMA Engineering |
| SE Domain Workflow Use Cases | Apply System Security Engineering |
| SE Domain Workflow Use Cases | Analyze System Performance |
| SE Domain Workflow Use Cases | Allocate and Manage SWaP |
| SE Domain Workflow Use Cases | Perform a Trade Study |
| SE Domain Workflow Use Cases | Analyze Behavior Correctness |
| SE Domain Workflow Use Cases | Manage Product Lines |
| SE Domain Workflow Use Cases | Integrate Human Domain Constraints |
| SE Domain Workflow Use Cases | Perform Environmental Engineering |
| SE Domain Workflow Use Cases | Collaborate with Implementation Domain Team |
| SE Domain Workflow Use Cases | Perform EMI Engineering |
| Validation and Verification Workflow Use Cases | Develop Verification Plan and Procedures |
| Validation and Verification Workflow Use Cases | Develop a System Integration Plan |
| Validation and Verification Workflow Use Cases | Execute a Verification Test Procedure |
| Validation and Verification Workflow Use Cases | Provide V&V Status |
| Production Stage | Support Produceability Engineering |
| Product and Service Life Management Stage | Support Initial Installation |
| Product and Service Life Management Stage | Architect Sustainability System |
| Product and Service Life Management Stage | Evaluate Change Request |
| Product and Service Life Management Stage | Support System Modernization Plan |
| Product and Service Life Management Stage | Support System Disposal and Retirement |

## Table of Actors

Table 3: List of Actors

| **Name** | **Description** |
| --- | --- |
| Manufacturing Engineer | Manufacturing engineering is a discipline of engineering dealing with different manufacturing practices and includes the research, design and development of systems, processes, machines, tools and equipment. The manufacturing engineer's primary focus is to turn raw materials into a new or updated product in the most economic, efficient and effective way possible [8]. |
| Program Manager | \*\* consider product manager |
| Engineering Mgr. | Engineering Management is a specialized form of management that is concerned with the application of engineering principles to business practice. Engineering management is a career that brings together the technological problem-solving savvy of engineering and the organizational, administrative, and planning abilities of management in order to oversee complex enterprises from conception to completion. [8] |
| Customer | A customer (sometimes known as a client, buyer, or purchaser) is the recipient of a good, service, product, or idea, obtained from a seller, vendor, or supplier for a monetary or other valuable consideration. [8] |
| Software Engineer | Software engineers apply the principles of software engineering to the design, development, maintenance, testing, and evaluation of the software and systems that make computers or anything containing software work.[8] |
| Mechanical Engineer | Mechanical engineering is the discipline that applies the principles of engineering, physics, and materials science for the design, analysis, manufacturing, and maintenance of mechanical systems. It is the branch of engineering that involves the design, production, and operation of machinery [8]. |
| Electrical Engineer | Electrical engineers apply the principles of electrical engineering to the design, development, maintenance and testing of electrical equipment. Electrical engineering includes the study and application of electricity, electronics, and electromagnetism. [8] |
| Stakeholder | A person, group or organization with an interest in a project. [8] |
| System Architect | Looks across all aspects of the system to ensure the overall system meets the stakeholders' needs. |
| Systems Engineer | A systems engineer is a person or role who supports an interdisciplinary approach and means to enable the realization of successful systems. In particular, the systems engineer often serves to elicit and translate customer needs into specifications that can be realized by the system development team. In order to help realize successful systems, the systems engineer supports a set of life cycle processes beginning early in conceptual design and continuing throughout the life cycle of the system through its manufacture, deployment, use and disposal. The systems engineer must analyze, specify, design, and verify the system to ensure that it's functional, interface, performance, physical, and other quality characteristics, and cost are balanced to meet the needs of the system stakeholders.  A systems engineer helps ensure the elements of the system fit together to accomplish the objectives of the whole, and ultimately satisfy the needs of the customers and other stakeholders who will acquire and use the system. |
| SWaP SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with size weight and power meets the overall stakeholder's needs. |
| Security SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with data security and system security meets the overall stakeholder's needs. |
| Safety SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with the operational safety of the system meet the overall stakeholder's needs. |
| Analyst | This actor's role of System Engineering is responsible for executing a defined analytical study focused on mitigating risk. |
| Environmental SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with environmental factors including temperature, humidity, UV exposure, radiation, magnetic forces, vibration, and others, meet the overall stakeholder's needs and all appropriate regulatory requirements. |
| Infrastructure SysEng | This actor's role of System Engineering is responsible to ensure all requirements meet the overall stakeholder's needs associated with areas of engineering including systems communications, network hardware and design, enclosures, computing hardware, system management, system time keeping and other, meet the overall stakeholder's needs. |
| V & V SysEng | This actor's role of System Engineering is responsible to ensure all requirements of the system are verified and the overall system is validated to meet the overall stakeholder's needs. |
| Human Factors SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with the interaction of the systems and humans. |
| EMI SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with electronic emissions meet the overall stakeholder's needs and meet associated regulatory agency requirements. |
| RMA SysEng | This actor's role of System Engineering is responsible to ensure all requirements associated with reliability, maintainability and availability meet the overall stakeholder's needs. |