32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA
June 25 - 30, 2022

Myron Hecht and Ross Raymond

A SysML Profile for MIL-STD-882E (System Safety)

Outline

- What is a SysML Profile?
- What is MIL STD 882E?
- Small Example SysML Profile
- System Safety Profile Metamodel
- System Safety Profile Outputs and Reports
- Demonstration
- Conclusions

What is a SysML Profile?

- A way of customizing SysML to enhance its use in a specific domain
- Benefits
  - Integration of domain specific information into an architecture model
  - Retrieval of domain specific information (analyses, reports) automatically and on demand
  - Enables cross-cutting concerns such as safety, reliability, security, supportability to be addressed throughout the MBSE design process rather than as an afterthought
- Components
  - Meta-Models
  - Stereotypes, Tags, and Relationships
  - Constraints
  - Preconfigured Views
  - Model Exports

What is MIL STD 882E?

- Provides a standard, generic method for the identification, classification, and mitigation of hazards.
- Identifies the U.S. Department of Defense (DoD) approach for identifying hazards and assessing and risks in the development, test, production, use, and disposal of defense systems.
- Required for DoD acquisitions (DoD Instruction DI 5000.02 par. 16; “The Program manager will use the methodology in MIL STD 882E”)

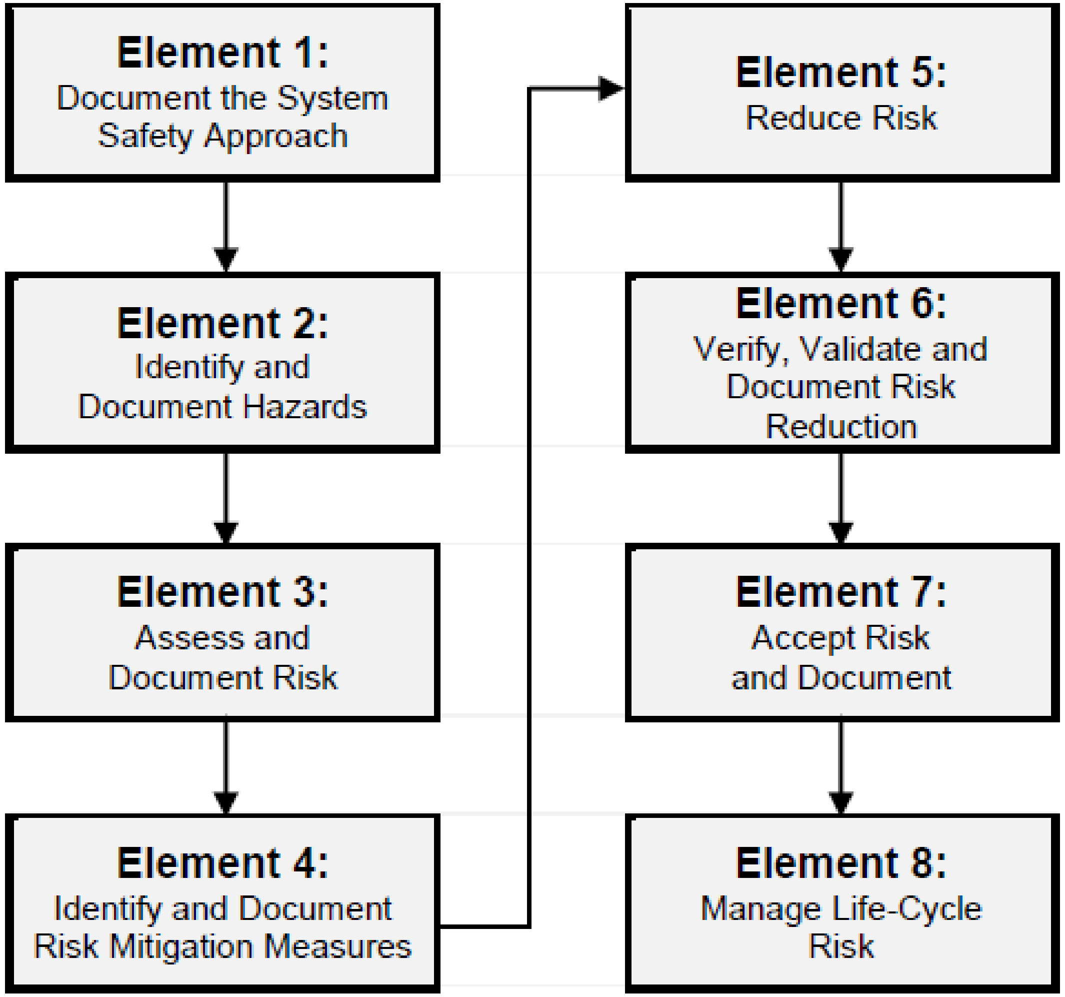
What does the profile for MIL STD 882E do in an MBSE development?

Animated

Provides data definitions for hazard identification

Supports safety risk assessment and documentation and integration with programmatic risk

Provides data definitions, queries, and output formats for mitigation measures



Element 1: Document the System Safety Approach

Element 2: Identify and Document Hazards

Element 3: Assess and Document Risk

Element 4: Identify and Document Risk Mitigation Measures

Element 5: Reduce Risk

Element 6: Verify, Validate and Document Risk Reduction

Element 7: Accept Risk and Document

Element 8: Manage Life-Cycle Risk

Enables status monitoring of mitigation actions

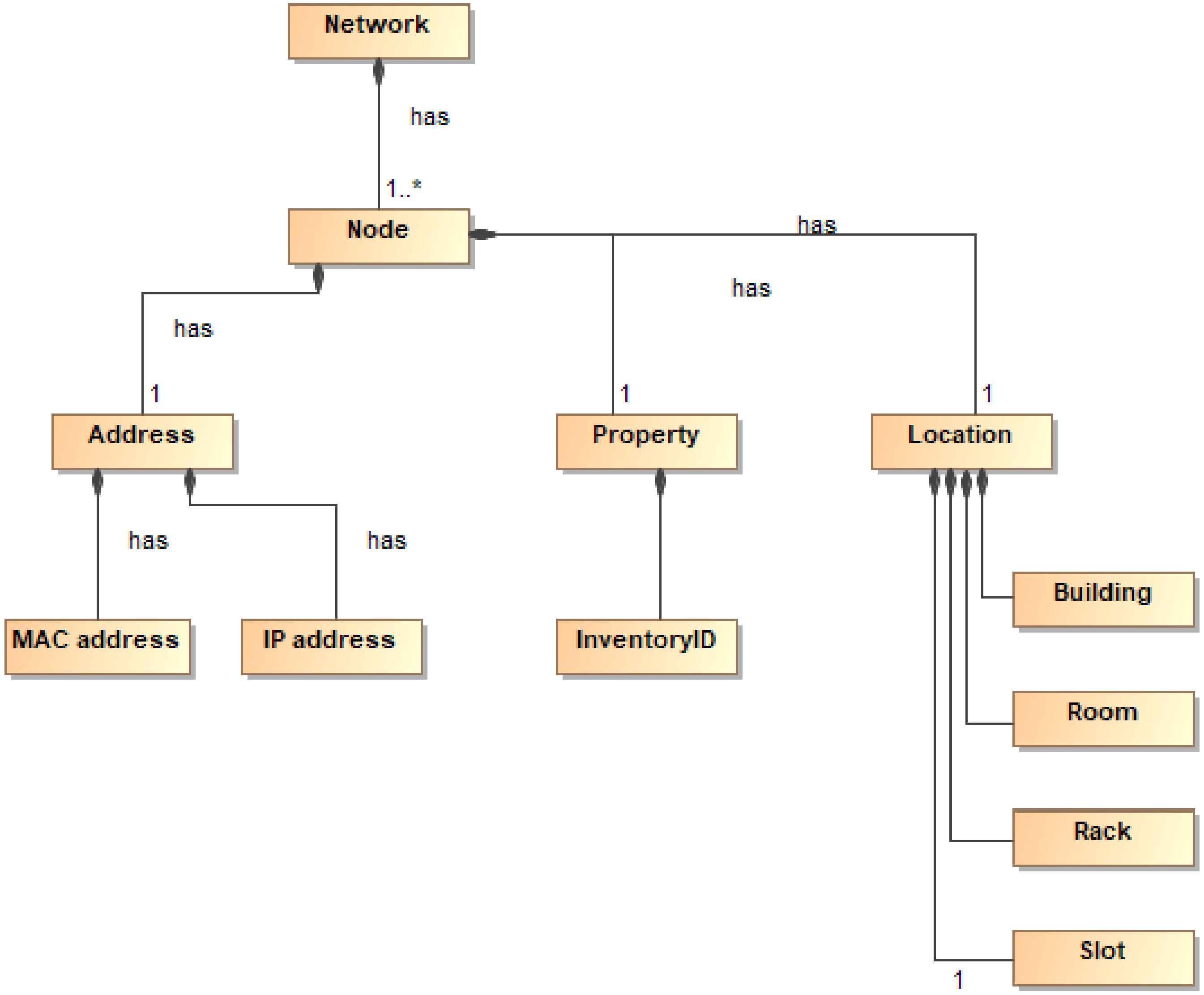
Generates documentation of hazard identification and risk and mitigation

Generates SSHAR, SHAR, and risk matrices

Source: MIL-STD-882E Fig. 1

Simple Meta-Model for a Local Area Network (LAN)

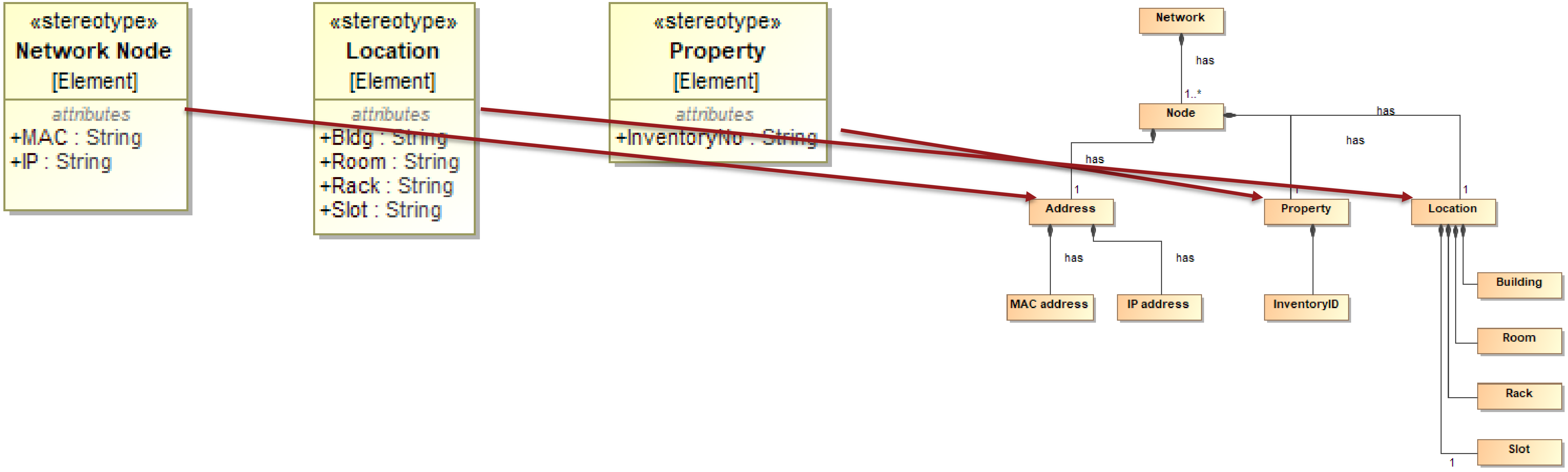
- Meta-Models describe the relationships between profile concepts
- A profile begins with a concept, translated into the modeling language and refined
  - *For example, define the concepts for a local area computer network (LAN)*



Stereotypes for the LAN Meta-Model

Animated

Using the LAN meta-model, we define a simple profile that consists of 3 stereotypes

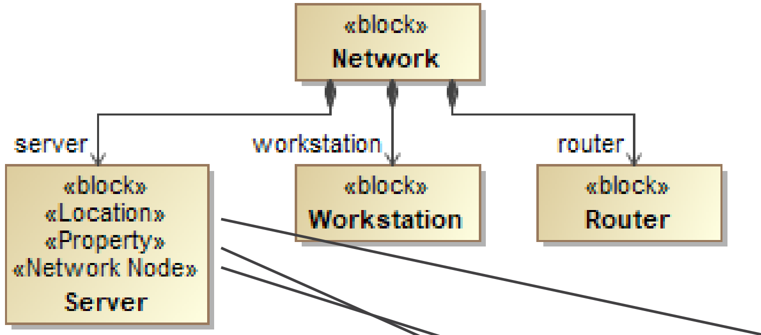


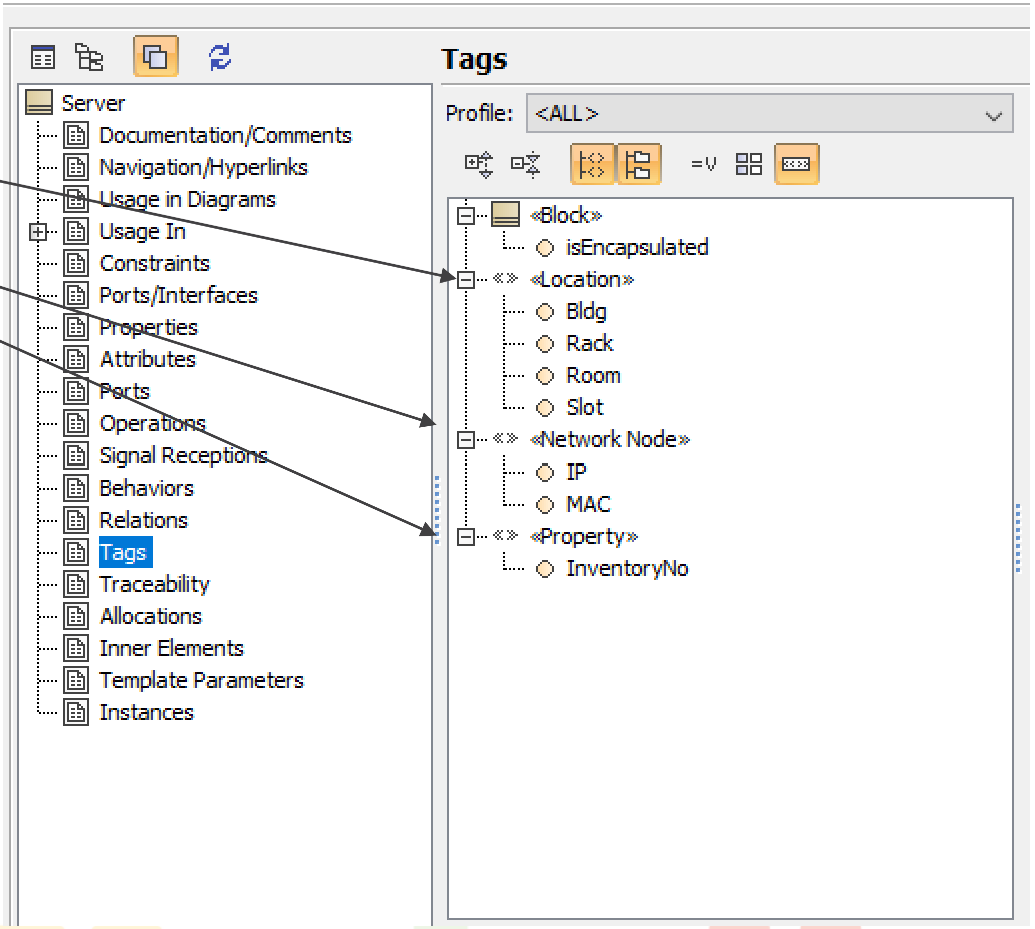
«stereotype»
Network Node
[Element]
attributes
+MAC : String
+IP : String

«stereotype»
Location
[Element]
attributes
+Bldg : String
+Room : String
+Rack : String
+Slot : String

«stereotype»
Property
[Element]
attributes
+InventoryNo : String

Applying the LAN Stereotypes




Tags

Server
- Documentation/Comments
- Navigation/Hyperlinks
- Usage in Diagrams
- Usage In
- Constraints
- Ports/Interfaces
- Properties
- Attributes
- Ports
- Operations
- Signal Receptions
- Behaviors
- Relations
- Tags
- Traceability
- Allocations
- Inner Elements
- Template Parameters
- Instances

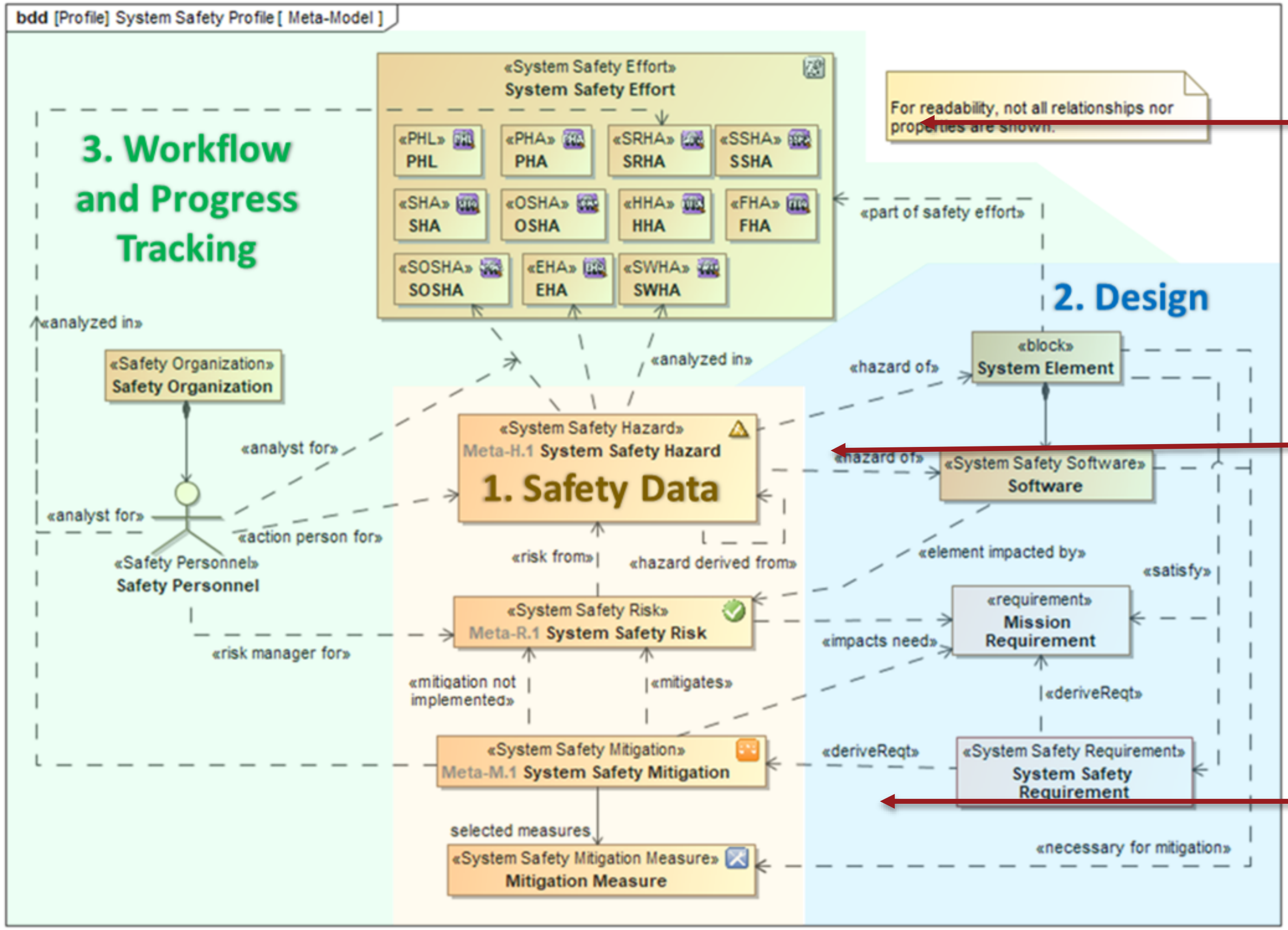
Profile: <ALL>

- «Block»
  - isEncapsulated
- «Location»
  - Bldg
  - Rack
  - Room
  - Slot
- «Network Node»
  - IP
  - MAC
- «Property»
  - InventoryNo

When the three stereotypes are applied to a standard SysML block, the block “becomes” a network node inheriting the “tags”

System Safety Profile Meta-Model

Animated

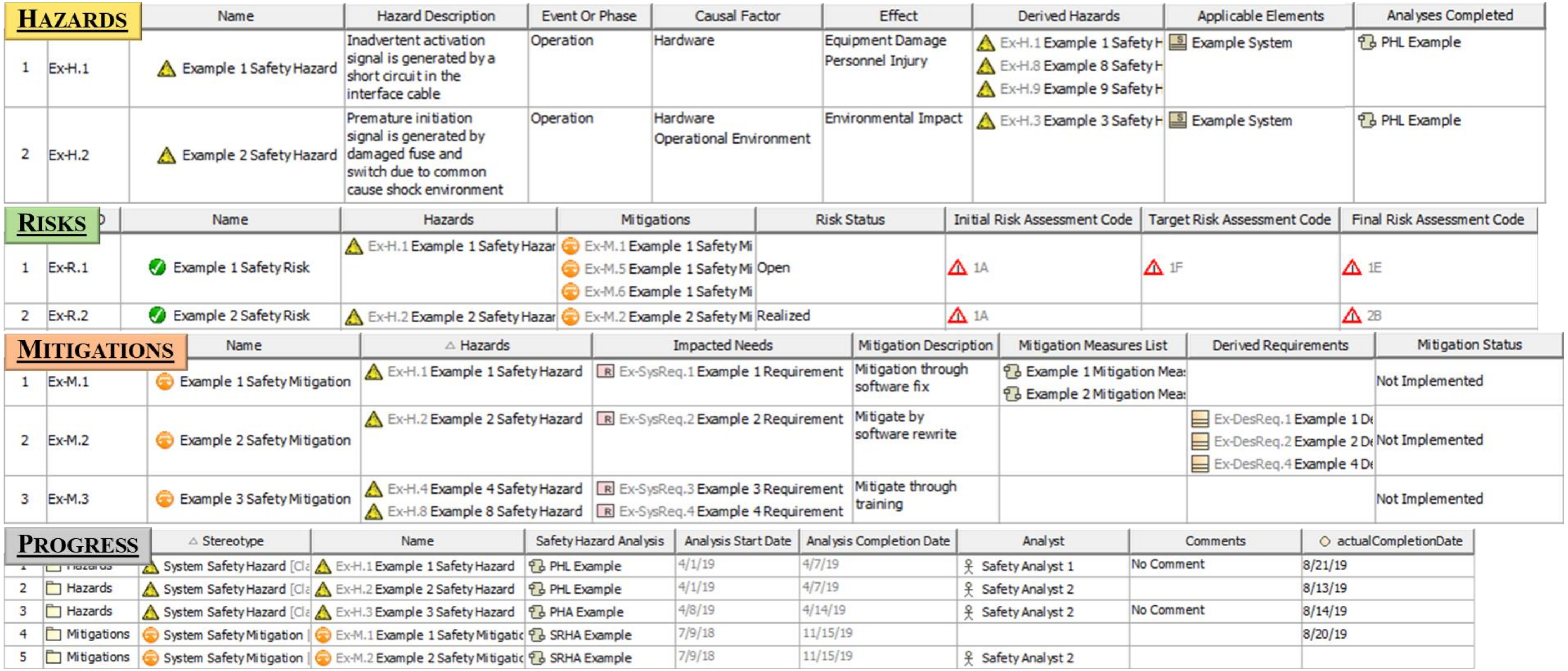


Task 200 analyses

Hazard element

Hazard tracking and mitigation

Tables produced from Queries into Profile



Hazards		Name	Hazard Description	Event Or Phase	Causal Factor	Effect	Derived Hazards	Applicable Elements	Analyses Completed
1	Ex-H.1	Example 1 Safety Hazard	Inadvertent activation signal is generated by a short circuit in the interface cable	Operation	Hardware	Equipment Damage Personnel Injury	Ex-H.1 Example 1 Safety H Ex-H.8 Example 8 Safety H Ex-H.9 Example 9 Safety H	Example System	PHL Example
2	Ex-H.2	Example 2 Safety Hazard	Premature initiation signal is generated by damaged fuse and switch due to common cause shock environment	Operation	Hardware Operational Environment	Environmental Impact	Ex-H.3 Example 3 Safety H	Example System	PHL Example

Risks	D	Name	Hazards	Mitigations	Risk Status	Initial Risk Assessment Code	Target Risk Assessment Code	Final Risk Assessment Code
1	Ex-R.1	Example 1 Safety Risk	Ex-H.1 Example 1 Safety Hazar	Ex-M.1 Example 1 Safety Mi Ex-M.5 Example 1 Safety Mi Ex-M.6 Example 1 Safety Mi	Open	1A	1F	1E
2	Ex-R.2	Example 2 Safety Risk	Ex-H.2 Example 2 Safety Hazar	Ex-M.2 Example 2 Safety Mi	Realized	1A		2B

Mitigations		Name	△ Hazards	Impacted Needs	Mitigation Description	Mitigation Measures List	Derived Requirements	Mitigation Status
1	Ex-M.1	Example 1 Safety Mitigation	Ex-H.1 Example 1 Safety Hazard	Ex-SysReq.1 Example 1 Requirement	Mitigation through software fix	Example 1 Mitigation Mea: Example 2 Mitigation Mea:		Not Implemented
2	Ex-M.2	Example 2 Safety Mitigation	Ex-H.2 Example 2 Safety Hazard	Ex-SysReq.2 Example 2 Requirement	Mitigate by software rewrite		Ex-DesReq.1 Example 1 De Ex-DesReq.2 Example 2 De Ex-DesReq.4 Example 4 De	Not Implemented
3	Ex-M.3	Example 3 Safety Mitigation	Ex-H.4 Example 4 Safety Hazard Ex-H.8 Example 8 Safety Hazard	Ex-SysReq.3 Example 3 Requirement Ex-SysReq.4 Example 4 Requirement	Mitigate through training			Not Implemented

Progress		△ Stereotype	Name	Safety Hazard Analysis	Analysis Start Date	Analysis Completion Date	Analyst	Comments	○ actualCompletionDate
1	Hazards	System Safety Hazard [Cl:	Ex-H.1 Example 1 Safety Hazard	PHL Example	4/1/19	4/7/19	Safety Analyst 1	No Comment	8/21/19
2	Hazards	System Safety Hazard [Cl:	Ex-H.2 Example 2 Safety Hazard	PHL Example	4/1/19	4/7/19	Safety Analyst 2		8/13/19
3	Hazards	System Safety Hazard [Cl:	Ex-H.3 Example 3 Safety Hazard	PHA Example	4/8/19	4/14/19	Safety Analyst 2	No Comment	8/14/19
4	Mitigations	System Safety Mitigation		Ex-M.1 Example 1 Safety Mitigatic	SRHA Example	7/9/18	11/15/19			8/20/19
5	Mitigations	System Safety Mitigation		Ex-M.2 Example 2 Safety Mitigatic	SRHA Example	7/9/18	11/15/19	Safety Analyst 2		

Implemented using generic table capability of Cameo Systems Modeler

Profile Dependency (traceability matrices)

Matrix Name	Elements	Description
System Hazard Trace	System Safety Hazard System Design Elements	Traces hazards to their associated system design elements
Derived Hazards	System Safety Hazard	Traces hazards derived from others through the analyses
Hazards to Risks	System Safety Hazard System Safety Risk	Traces hazards to their corresponding risk
Risks to Mitigations	System Safety Risk System Safety Mitigation	Traces risks to their corresponding mitigations
Mitigations to Measures	System Safety Mitigation Mitigation Measure	Traces mitigations to their corresponding mitigation measures
Mitigations to Hazards (implied)	System Safety Mitigation System Safety Hazard	Implied trace from mitigations to hazards by navigating through the intermediary risk element
Hazard Analysis Assignment	System Safety Hazard System Safety Hazard Analysis	Traces hazards to analysis activities
Safety Effort Trace	System Safety Effort System Design Elements	Traces system design elements to system-level safety analysis efforts
Personnel Resource Allocation	System Safety Organization System Safety Personnel Any assignable model element	Provides traces from annotated personnel or organization representations to appropriate model elements, including assigning analysts, risk managers, and risk authorities
Additional Matrices	Any connected model elements	Additional matrices may be created as needed

Model Exports: Risk Matrix

System Safety Risk Matrix (template)

- Risk level summary lists the number of hazards in each risk level
- First number counts hazards in each risk category
- Second number counts the hazards planned for this category after all mitigations

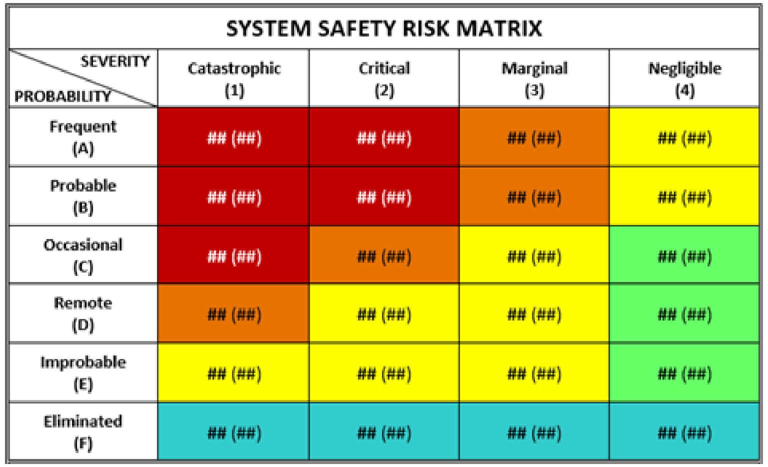
Risk Burndown (export with data)

- Shows planned risk reduction based on Risk, Mitigation strategy, mitigation measures, and mitigation action profile model elements
- Shows actuals based on dates in mitigation measure and mitigation action profile model elements

– *Model templates were created within the profile*

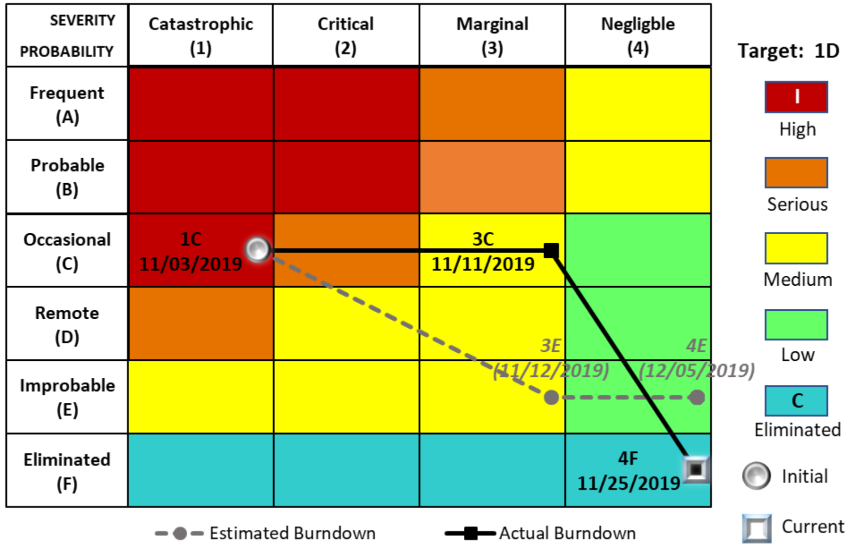
– *Templates can automatically export data to Microsoft Office (and Open Office osd) files*

– *Implemented using “Report” and Velocity Template Language (VTL) capabilities of Cameo Systems Modeler*

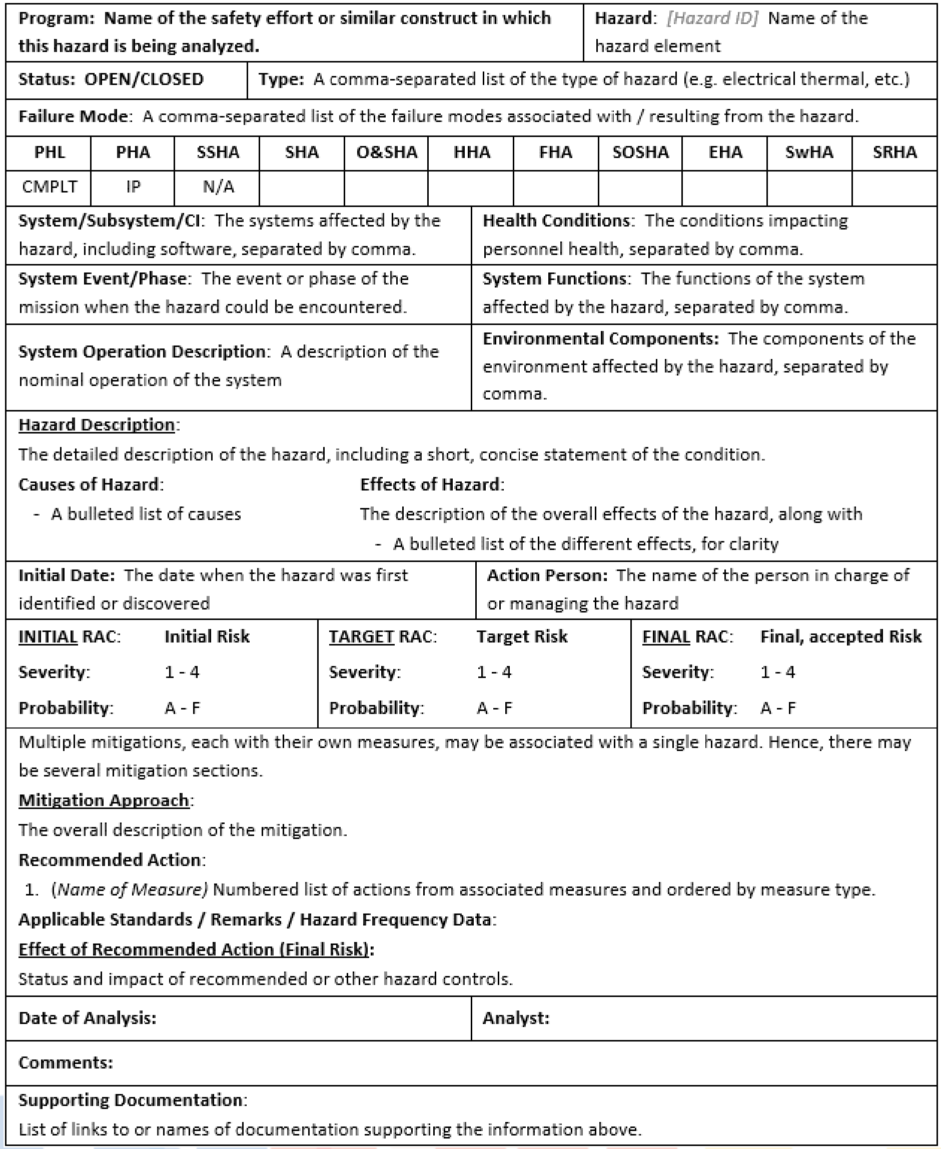


SYSTEM SAFETY RISK MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	## (##)	## (##)	## (##)	## (##)
Probable (B)	## (##)	## (##)	## (##)	## (##)
Occasional (C)	## (##)	## (##)	## (##)	## (##)
Remote (D)	## (##)	## (##)	## (##)	## (##)
Improbable (E)	## (##)	## (##)	## (##)	## (##)
Eliminated (F)	## (##)	## (##)	## (##)	## (##)



Model Exports: Template for MIL STD 882E System/Subsystem Hazard Analysis Report (SSHAR)* Template



Program: Name of the safety effort or similar construct in which this hazard is being analyzed.

Hazard: *[Hazard ID]* Name of the hazard element

Status: OPEN/CLOSED

Type: A comma-separated list of the type of hazard (e.g. electrical thermal, etc.)

Failure Mode: A comma-separated list of the failure modes associated with / resulting from the hazard.

PHL	PHA	SSHA	SHA	O&SHA	HHA	FHA	SOSHA	EHA	SwHA	SRHA
CMPLT	IP	N/A								

System/Subsystem/CI: The systems affected by the hazard, including software, separated by comma.

Health Conditions: The conditions impacting personnel health, separated by comma.

System Event/Phase: The event or phase of the mission when the hazard could be encountered.

System Functions: The functions of the system affected by the hazard, separated by comma.

System Operation Description: A description of the nominal operation of the system

Environmental Components: The components of the environment affected by the hazard, separated by comma.

Hazard Description:

The detailed description of the hazard, including a short, concise statement of the condition.

Causes of Hazard:

- A bulleted list of causes

Effects of Hazard:

The description of the overall effects of the hazard, along with

- A bulleted list of the different effects, for clarity

Initial Date: The date when the hazard was first identified or discovered

Action Person: The name of the person in charge of or managing the hazard

INITIAL RAC:	**Initial Risk**	**TARGET RAC**:	**Target Risk**	**FINAL RAC**:	**Final, accepted Risk**
Severity:	1 - 4	**Severity**:	1 - 4	**Severity**:	1 - 4
Probability:	A - F	**Probability**:	A - F	**Probability**:	A - F

Multiple mitigations, each with their own measures, may be associated with a single hazard. Hence, there may be several mitigation sections.

Mitigation Approach:

The overall description of the mitigation.

Recommended Action:

1. *(Name of Measure)* Numbered list of actions from associated measures and ordered by measure type.

Applicable Standards / Remarks / Hazard Frequency Data:

Effect of Recommended Action (Final Risk):

Status and impact of recommended or other hazard controls.

Date of Analysis:

Analyst:

Comments:

Supporting Documentation:

List of links to or names of documentation supporting the information above.

- Template combines information from hazards, system descriptions, mitigation status, safety and personnel.
- Exported as a Microsoft Word document

Implemented using "Report" and Velocity Template Language (VTL) capabilities of Cameo Systems Modeler

*DI-SAFT-80101C

Demonstration

Summary and Conclusions

- A profile was created to tailor SysML for a program that combines system safety domain-specific needs with the system design model
- Benefits of using SysML profiles for this program include:
  - Combining program- and domain-specific information with the system design model
    - Safety data can be entered directly into the primary architecture model
  - Allocation and tracking of requirements safety conformance
    - Allows data to be retrieved into views and reports
  - Enabling communication between system modelers and system safety domain experts
  - Presenting up-to-date status information on system safety
  - Generating domain artifacts and other reports with a few clicks

References

1. MIL-STD-822E: System Safety, U.S. Department of Defense, 2012.
2. DoD 5000.02: Operation of the Defense Acquisition System, January, 2015
3. DI-SAFT-80101C, System Safety Hazard Analysis Report (SSHAR), June 2015.
4. SysML 1.5 language specification, https://www.omg.org/spec/SysML/1.5, May, 2017