How Can SysML Support Certification?

Presented to
System Engineering Research Center "SERC Talks"

by
Myron Hecht
Aerospace Corporation

June 11, 2024

Agenda

- Definition of Certification
- Three Approaches to Using SysML in Certification
  - “Native” SysML
  - Use of a Profile to Extend SysML to a Specific Domain
  - Use of the SysML Model Itself for Certification
- Conclusions

Definition of Certification

General Definition: The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.

-- International Standards Organization; iso.org/certification.html

- Legal requirements (Contractual or non-contractual) identify by which independent body/bodies (the certification authority) the certification(s) must be issued
- The certification authority defines the form of the evidence that the seeker of the certification (applicant) must provide in order for it to provide the certification
- This definition is frequently in the form of a standard (e.g., MIL-STD-882E, ISO 26262, RTCA DO 178C, IEEE-Std-603-1991, etc.) or certification authority publication
- The standard or publication will usually define specific requirements and acceptance criteria that the applicant must meet

“Native” SysML

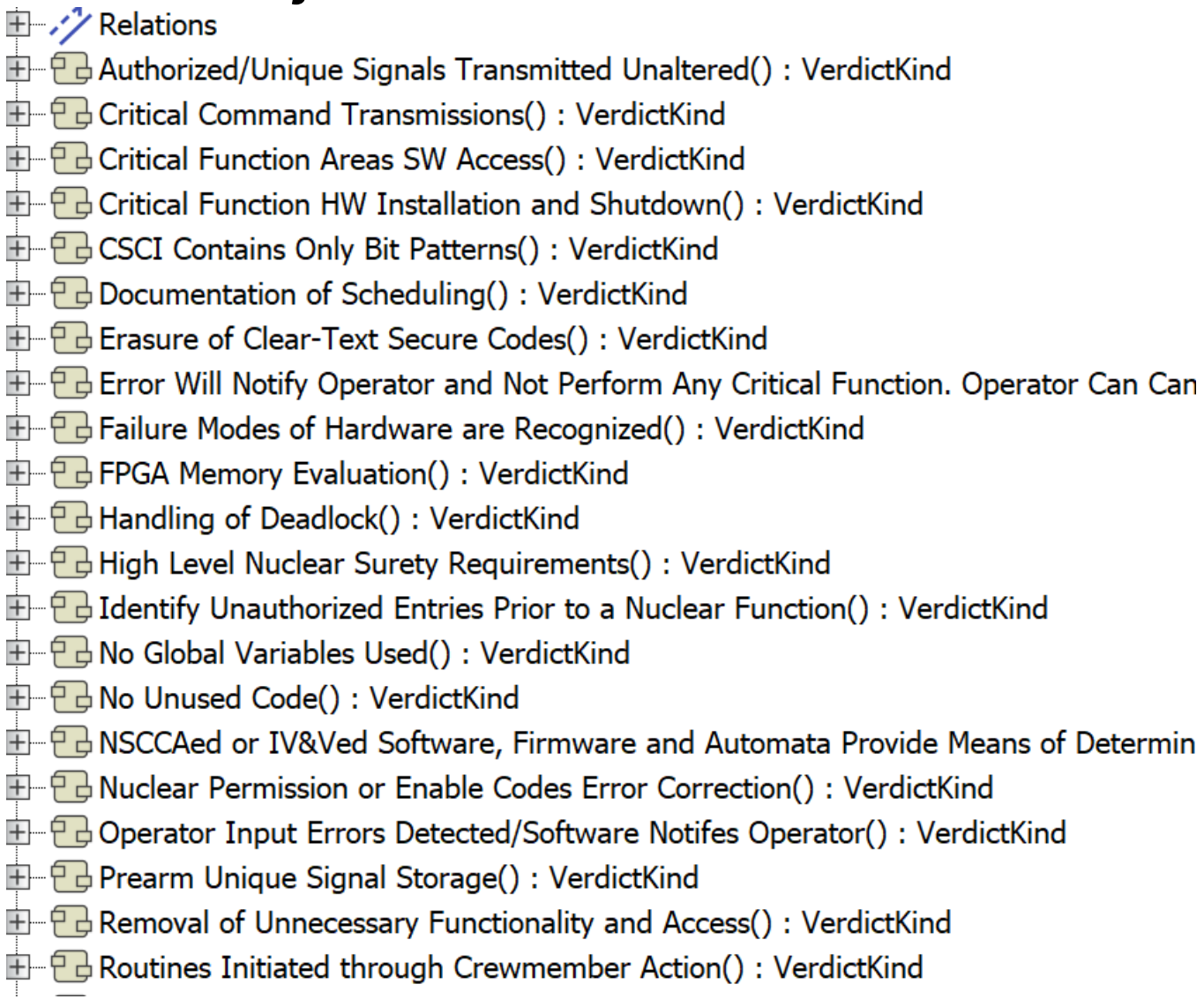
Model Based Certification Process

1. Ingest certification requirements as SysML requirements
2. Define the verification methods (certification objectives) for each of the requirements
3. Locate the relevant model elements in Create Block Diagrams (SysML BDDs and IBDs) of the system undergoing certification
4. Allocate the requirements to the system components
5. Allocate the verification methods to the requirements
6. Generate Traceability matrices showing certification requirements and verification objectives vs. components
7. Generate Certification Plan listing certification requirements and verification methods, and evidence by component
8. Obtain Certification Authority Approval of the Certification Plan
9. Execute the Certification plan and produce the evidence
10. Submit the evidence to the certification authority in the format it requires

Requirements Imported into SysML modeling tool

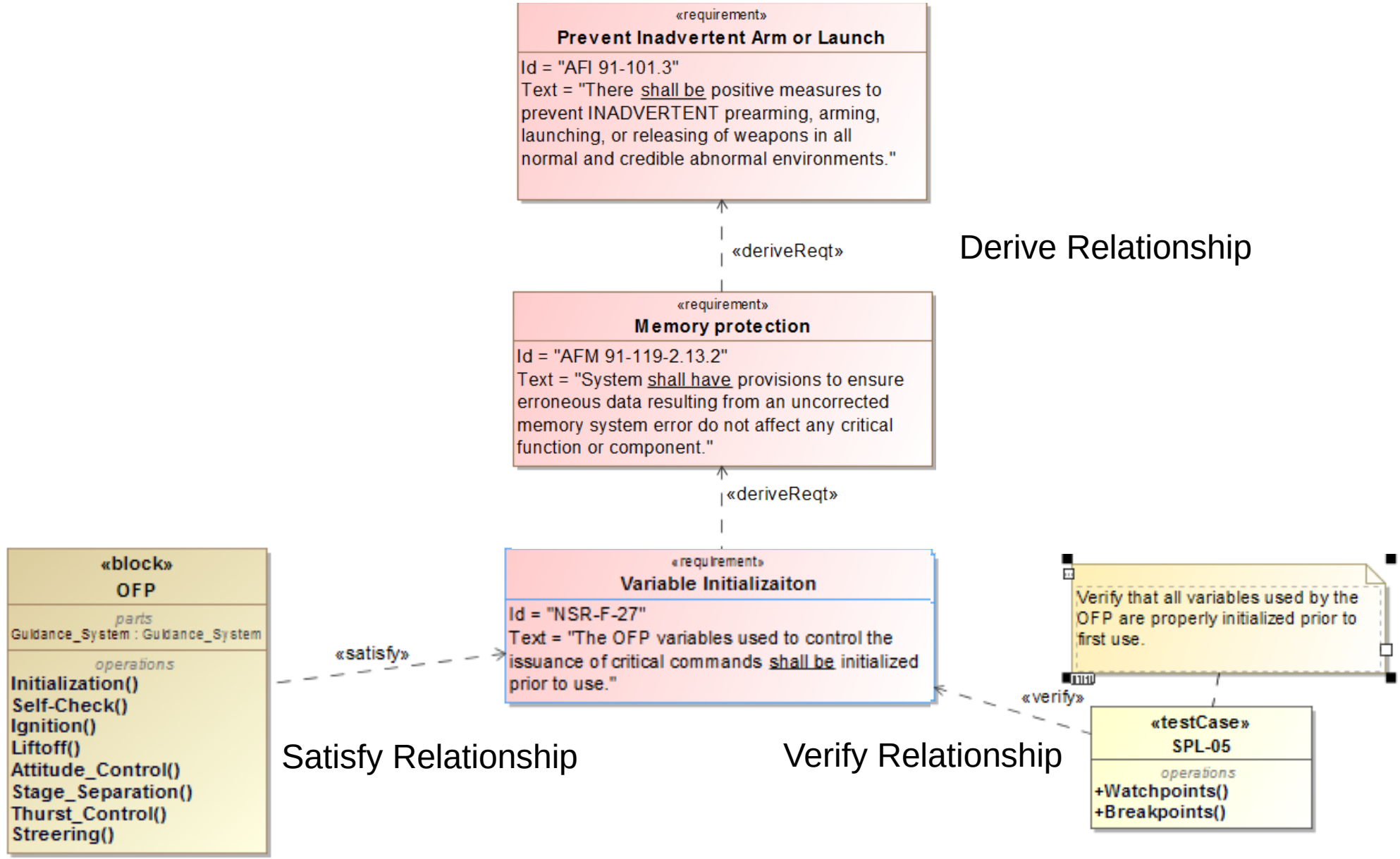
#	Id	△ Name	Text
188	119.2.3.c	R 119.2.3.c Higher Order Language (HOL) 3	Use of Assembly or Machine Language shall be justified in the NCIS in accordance with AFI 63-125, paragraph 3.2.2. Otherwise, a request for deviation shall be submitted.
189	119.2.3.d	R 119.2.3.d Higher Order Language (HOL) 4	The original language shall be used when modifying critical software.
190	119.2.5.a	R 119.2.5.a Fault Tolerance 1	Software shall be designed to provide self-check, confidence or test routines to verify the integrity and proper state of hardware devices that affect or execute critical functions.
191	119.2.5.b	R 119.2.5.b Fault Tolerance 2	Software shall be designed to detect critical function failure modes during power-up and operation.
192	119.2.5.c	R 119.2.5.c Fault Tolerance 3	Transitory faults (such as corrupted message packets) that do not indicate degraded processing capability shall be detected and dealt with, but do not necessarily need to be reported to the operator.
193	119.2.5.d	R 119.2.5.d Fault Tolerance 4	The system specification shall specify acceptable transitory fault rates.
194	119.2.5.e	R 119.2.5.e Fault Tolerance 5	Troubleshooting and maintenance operations shall prohibit using any nuclear weapon as a troubleshooting tool.

Definition of Verification Objectives



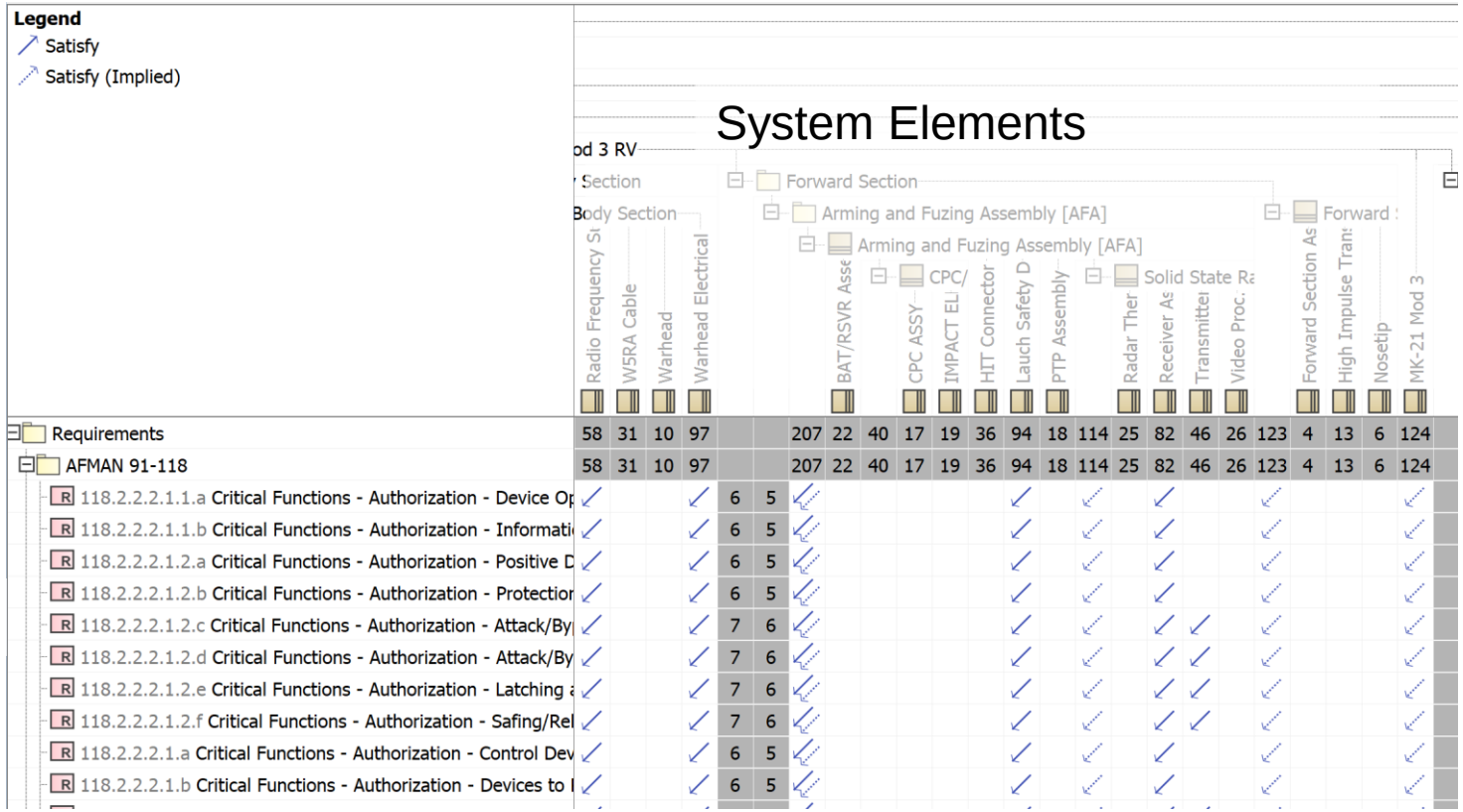
Verification Criteria from Section 3 of AFMAN 91-119

Allocation of Requirements and Verification Methods



Requirements Allocation Matrix

Requirements



Tables showing Requirements and Verification Objectives for Each Component

Component	Allocated Requirements	Related Verification Objectives
Arming and Fuzing Assembly [AFA] [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Reentry System [RS]::Reentry Vehicle [RV]::MK-21 Mod 3 RV::Forward Section::Forward Section]	*118.2.2.2.1.1.a* Critical Functions - Authorization - Device Operation *118.2.2.2.1.1.b* Critical Functions - Authorization - Information Control Concept *118.2.2.2.1.2.a* Critical Functions - Authorization - Positive Design Features *118.2.2.2.1.2.b* Critical Functions - Authorization - Protection Against Inadvertent Operation *118.2.2.2.1.2.c* Critical Functions - Authorization - Attack/Bypass of Device *118.2.2.2.1.2.d* Critical Functions - Authorization - Attack/Bypass Indication *118.2.2.2.1.2.e* Critical Functions - Authorization - Latching and Protection *118.2.2.2.1.2.f* Critical Functions - Authorization - Safing/Relocking Function *118.2.2.2.1.a* Critical Functions - Authorization - Control Devices *118.2.2.2.1.b* Critical Functions - Authorization - Devices to Prevent Prearming/Arming *118.2.2.2.2.1.a* Critical Functions - Prearming - Uniquely Coded Signal *118.2.2.2.2.1.b* Critical Functions - Prearming - Command Signal Unavailable *118.2.2.2.2.2.a* Critical Functions - Prearming - Isolation from Circuits *118.2.2.2.2.2.b* Critical Functions - Prearming - Avoid Wires that Carry Power *118.2.2.2.2.a* Critical Functions - Prearming - Command *118.2.2.2.2.b* Critical Functions - Prearming - Separation from Authorization Function *118.2.2.2.2.c* Critical Functions - Prearming - Preclusion *118.2.2.2.3.a* Critical Functions - Launching - Control	A&F system chemical compatibility AMAC and release systems independence Authorized/Unique Signals Transmitted Unaltered Certification evidence for embedded software and firmware Certification evidence for non-specialized COTS equipment Certification evidence for specialized COTS equipment Common ground reference for signal returns Conformance to MIL-STD- 461 and MIL-STD-464 Critical circuit isolation Design criteria for EMR protection Device authorization through command and control channels

Requirement	Components	Verification Objectives
'9.2.10.a Idle Operations 1	MIL-STD-1750A CPU [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer [MGC]::Missile Guidance Computer [MGC]::Computer Memory Module [CMM]]	CSCI Contains Only Bit Patterns
'9.2.10.b Idle Operations 2	MIL-STD-1750A CPU [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer [MGC]::Missile Guidance Computer [MGC]::Computer Memory Module [CMM]]	CSCI Contains Only Bit Patterns
'9.2.12.a Initialization and utdown 1	Missile Guidance Computer [MGC] [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer [MGC]]	NSCCAed or IV&Ved Software, Firmware and Automata Provide Means of Determining Correct Code or Logic
119.2.12.b Initialization and Shutdown 2	Missile Guidance Computer [MGC] [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer [MGC]]	Identify Unauthorized Entries Prior to a Nuclear Function
119.2.13.2.a Memory Protection 1	Memory Arbiter and IO Bus Controller [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer [MGC]::Missile Guidance Computer [MGC]::Computer Memory Module [CMM]]	Failure Modes of Hardware are Recognized
119.2.13.2.b Memory Protection 2	Memory Arbiter and IO Bus Controller [System Structure::MMIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::NS50 MGS::Missile Guidance Computer	SW Wait, Stop, and Halt States

Generation of the Certification Plan from the Model using a Template

Table of Contents

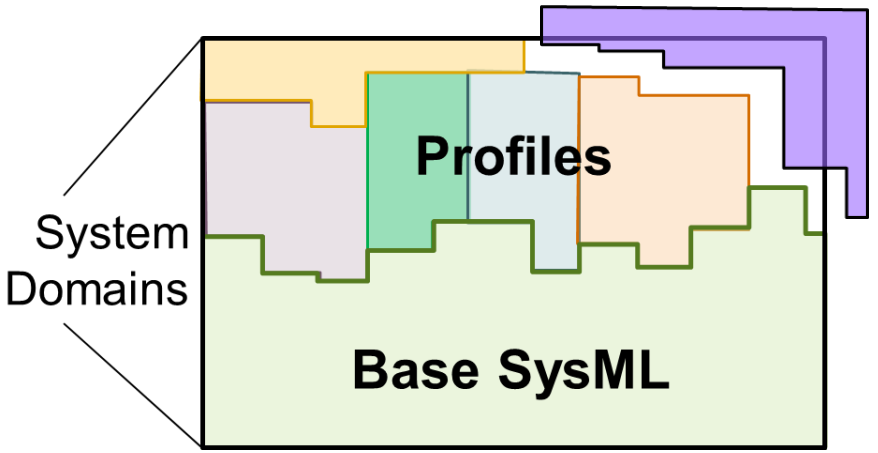
Discussion

- Advantages
  - The Applicant uses tool capabilities to automate production of required documentation in the form expected by the Certification Authority (usually Microsoft Office or .pdf file formats)
    - Document generation is supported by features in major SysML tools (Templates or Virtual Documents)
  - With automated generation, “design freezes” are not necessary
  - The Certification Agency receives the documentation in the conventional form – does not need to be aware that a model has been used to produce it
- Disadvantages
  - Requirements, verification methods, satisfy relations, and verify relations describe certification activities, but they don’t actually perform them
  - Documentation generation and templates are not standard within SysML – templates are not portable and specific capabilities vary by tool

Use of a Profile to Extend SysML to a Specific Domain

What is a Profile?

- Profiles tailor SysML to a specific purpose
  - *A system unique "dialect" of the modeling language (adding concepts and relations to tailor it to a specific domain)*
- A profile consists of
  - ***Meta-Model**, for profile organization and identification of relations*
  - ***Profile elements***
    - **Stereotypes** (i.e. labels), for distinguishing types of elements
    - **Tags** (i.e. properties), for describing types of elements
      - *Manually-specified fields*
      - *"Derived" Properties, using model navigation and scripts*
    - **Relationships**, for connecting types of elements
      - *Include their own properties*
    - **Constraints,** for limiting values on tags (if applicable)
  - ***Views into the model***
    - Pre-configured **diagrams and tables**, for displaying the new information
  - ***Templates for Exported Artifacts***
    - Templates for external **documents and reports**, for extracting profile information

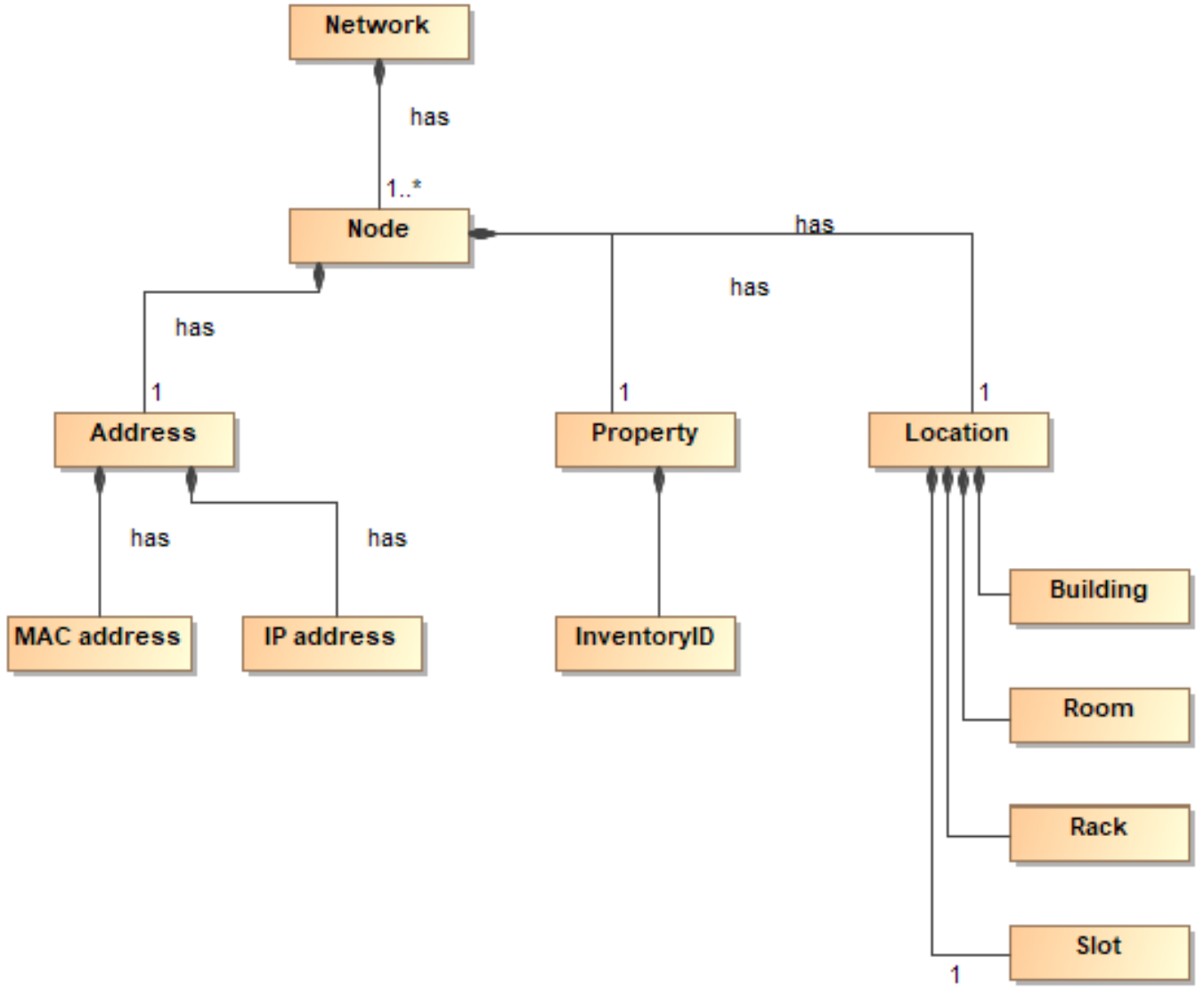


What does a Profile Consist Of?

- A profile consists of
  - ***Meta-Model**, for profile organization and identification of relations*
  - ***Profile elements***
    - **Stereotypes** (i.e. labels), for distinguishing types of elements
    - **Tags** (i.e. properties), for describing types of elements
      - *Manually-specified fields*
      - *“Derived” Properties, using model navigation and scripts*
    - **Relationships**, for connecting types of elements
      - *Include their own properties*
    - **Constraints,** for limiting values on tags (if applicable)
  - ***Views into the model***
    - Pre-configured **diagrams and tables**, for displaying the new information
  - ***Exported Artifacts***
    - Templates for external **documents and reports**, for extracting profile information

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

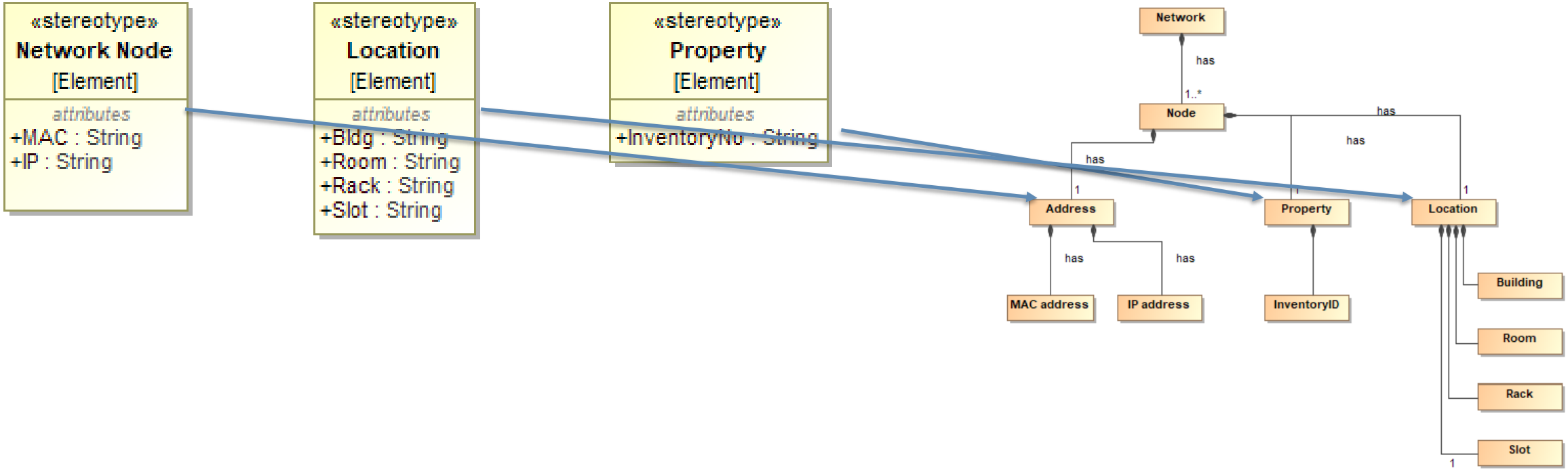
- Meta-Models describe the relationships between profile concepts
- A profile begins with a concept, translated into the modeling language and refined
  - *For example, define the concepts for a local area computer network (LAN)*



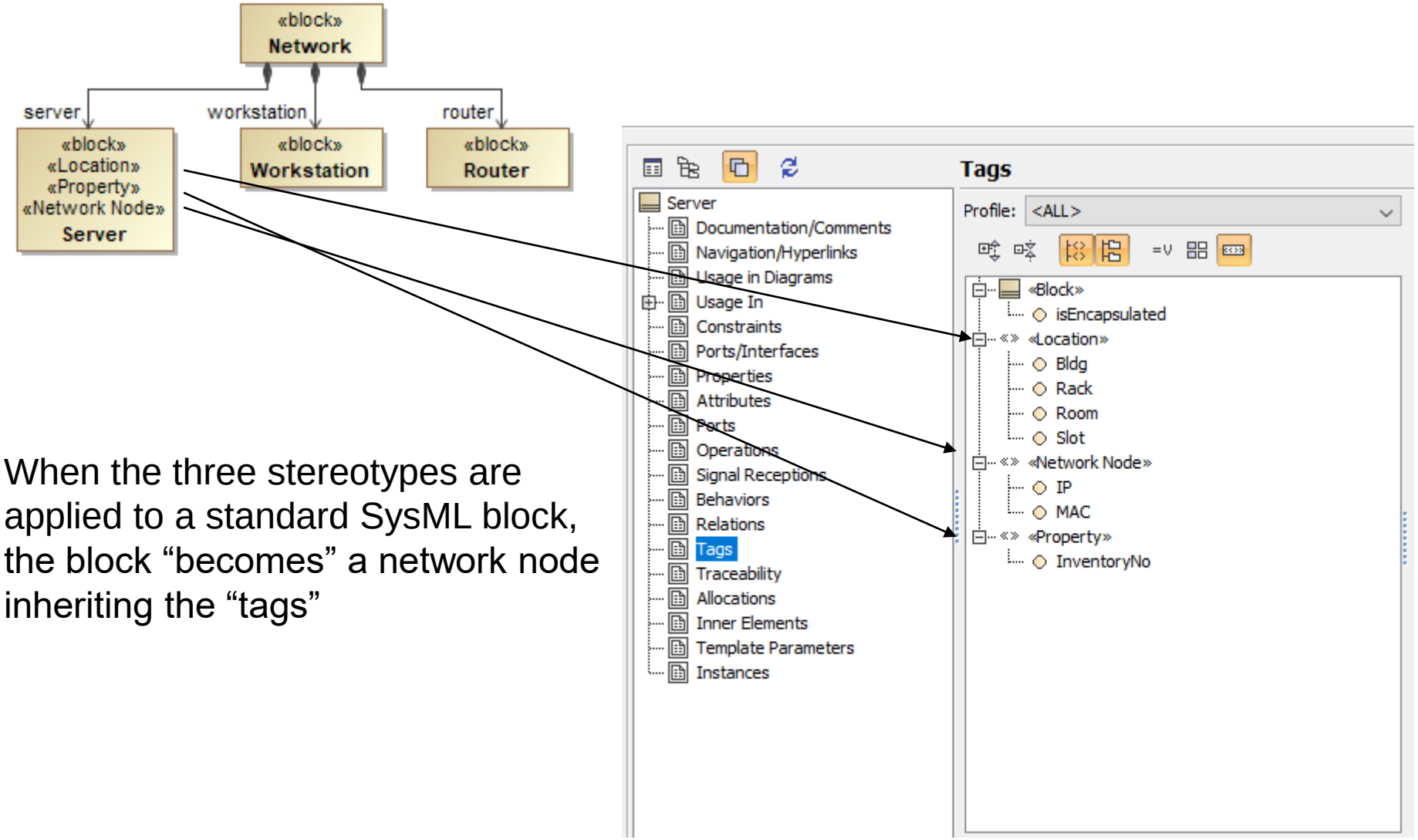
Stereotypes for the LAN Meta-Model

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

Animated



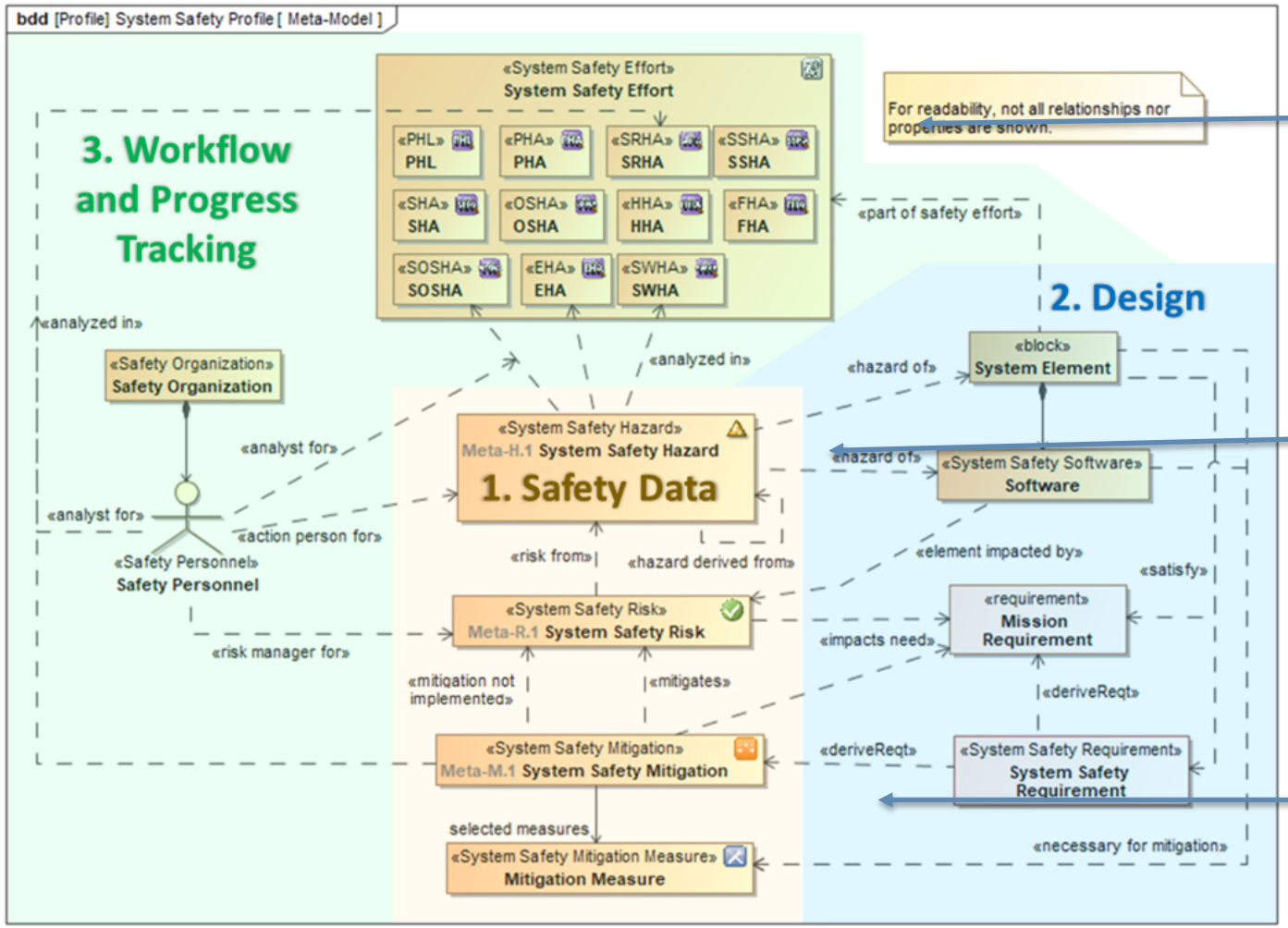
Applying the LAN Stereotypes



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 in the 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

		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

Model Exports: Risk Matrix

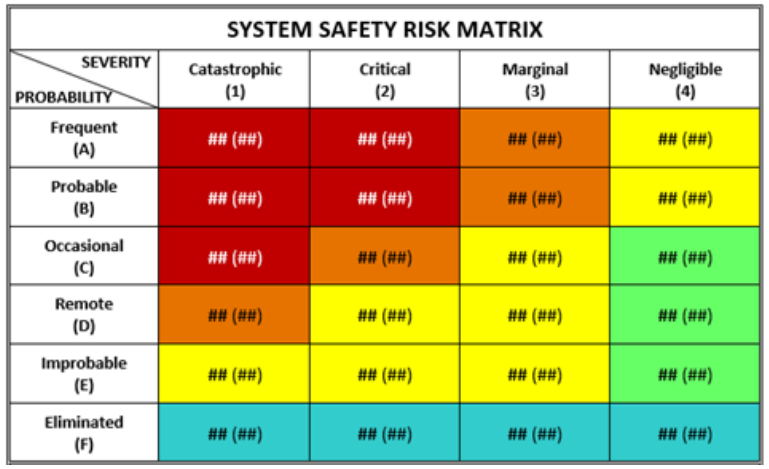
System Safety Risk Matrix (template)

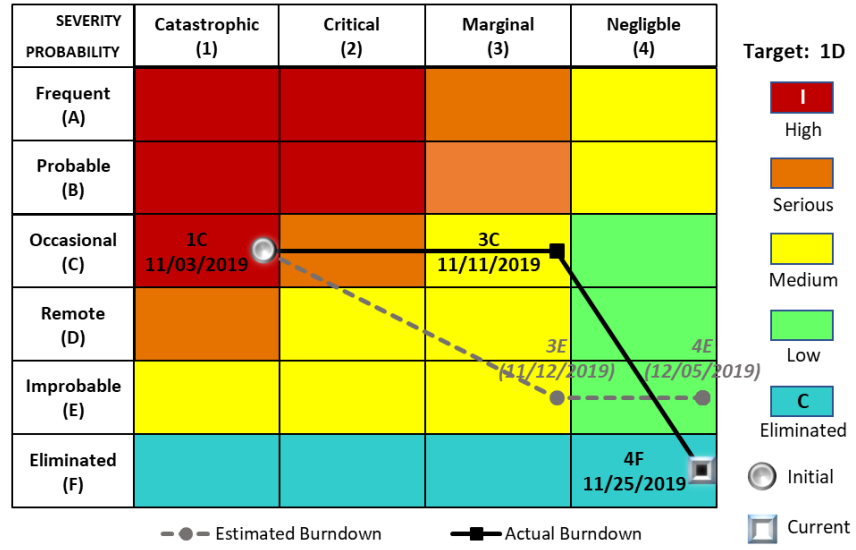
- *Risk level summary lists the number of hazards in each risk level*
- *First number counts hazards in each risk category*
- *Second number counts the hazards planned for this category after all mitigations*

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*





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

Discussion

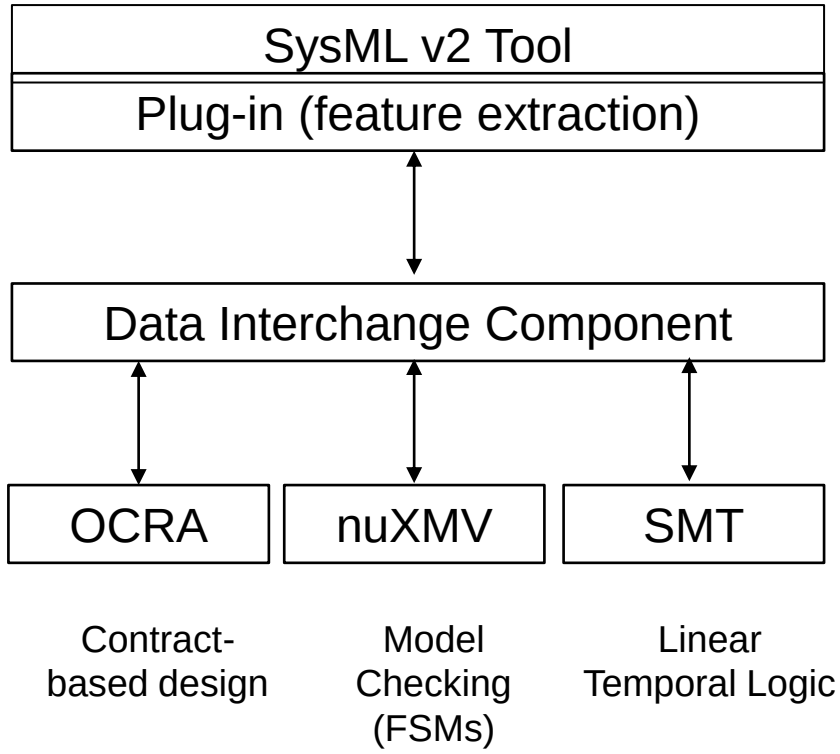
- Advantages
  - Combines program- and domain-specific information with the system design model
    - Allows relevant certification data to be entered directly into the primary architecture model
  - Allows allocation and tracking of certification requirements conformance
    - Allows data to be retrieved into views and reports
  - Enables the system modelers to more easily communicate with domain experts
  - Presents up-to-date system information on certification status in common, pre-configured formats
  - Generates Certification Authority specific artifacts on demand
  - The Certification Agency receives the documentation in the conventional form – does not need to be aware that a model has been used t*o produce it*
- Disadvantages
  - Profiles describe certification activities, they don’t perform them
  - Correct and complete profiles require significant time and resources to create
  - Features such as document generation are not portable among different models

Use of the Model Itself

Description

- Modelers insert elements inserted into the SysML model at design time. Subsequently, the model is processed and analyzed by formal methods tools
- Because of its textual representation, SysML v2 is well suited to use of the model itself for certification
- Showing satisfaction of properties agreed upon with the Certification Authority would be the basis for certification

A pipeline such as this enables well-established formal methods tools to be connected to the model and used for analysis

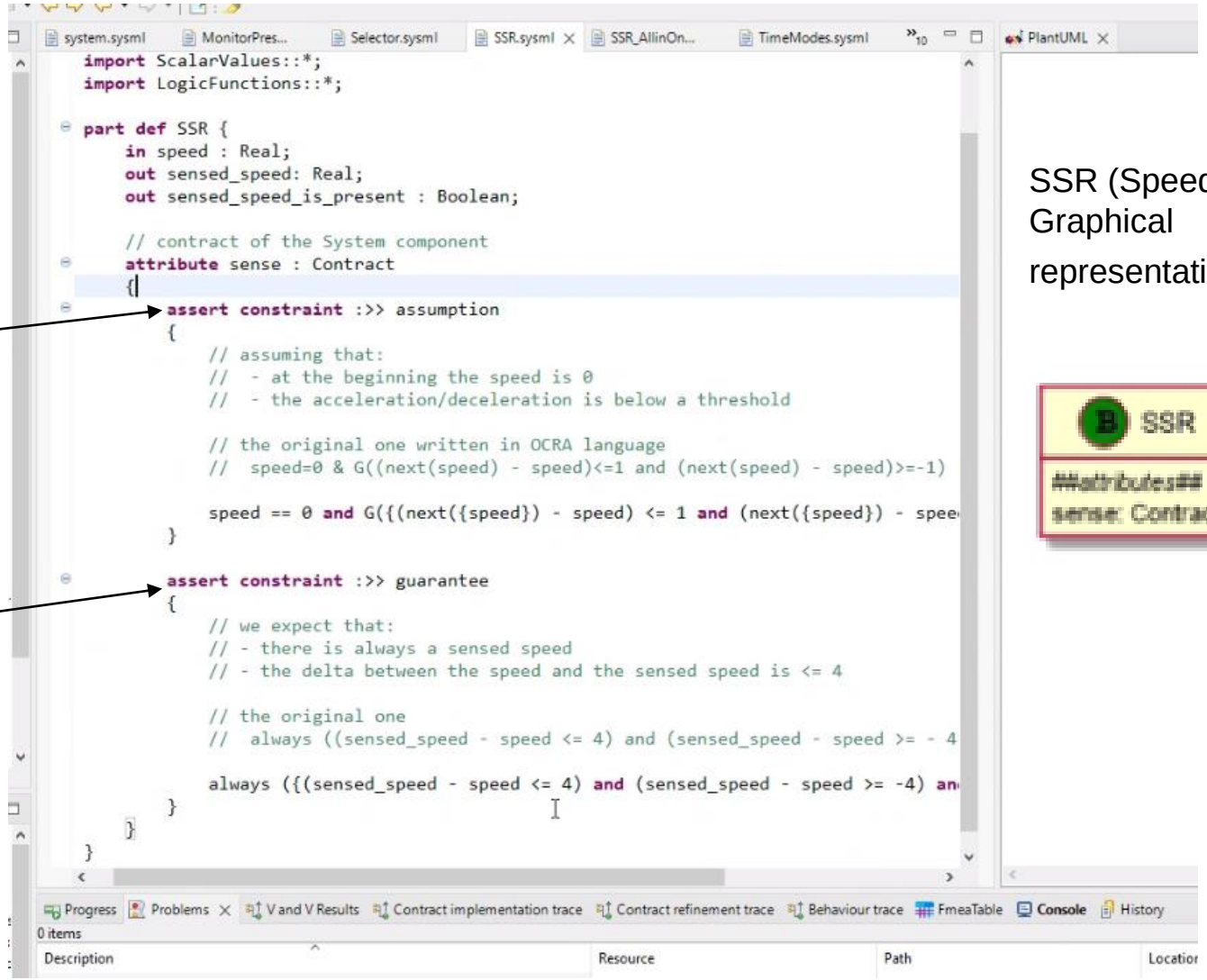


Example: SysML Block Definition with Assumption-Guarantee Contract

Contained in SysML models
Tools such as OCRA can reason about Assumptions and Guarantees

Assumption attribute
defines properties to be satisfied by the context (the environment) in which a component is used

Guarantee attribute
describes bounds on the behavior of the component when the context satisfies the assumptions

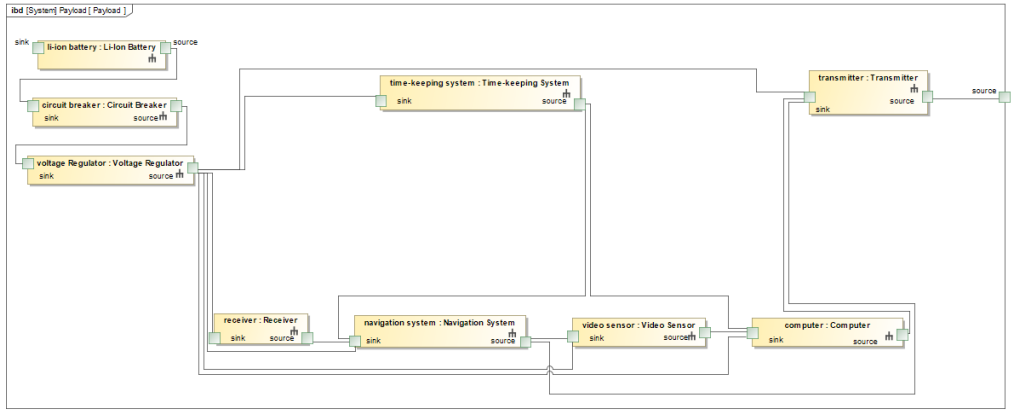


SSR (Speed Sensor) Graphical representation)

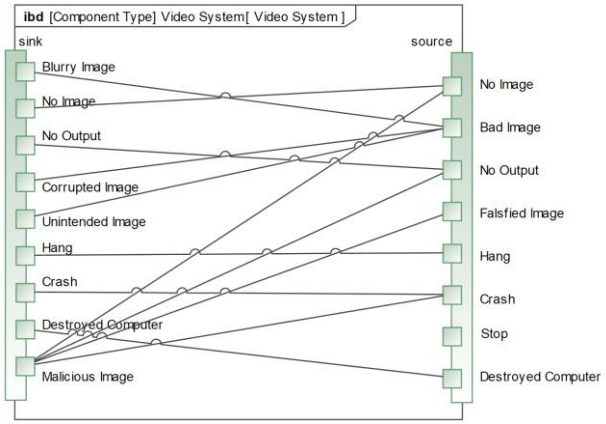
SysML v2 example from model developed by Stefano Tonetta and Luca Cristoforetti, FBK Institute, Italy, 2024

Automated Generation of FMEAs from SysML Models

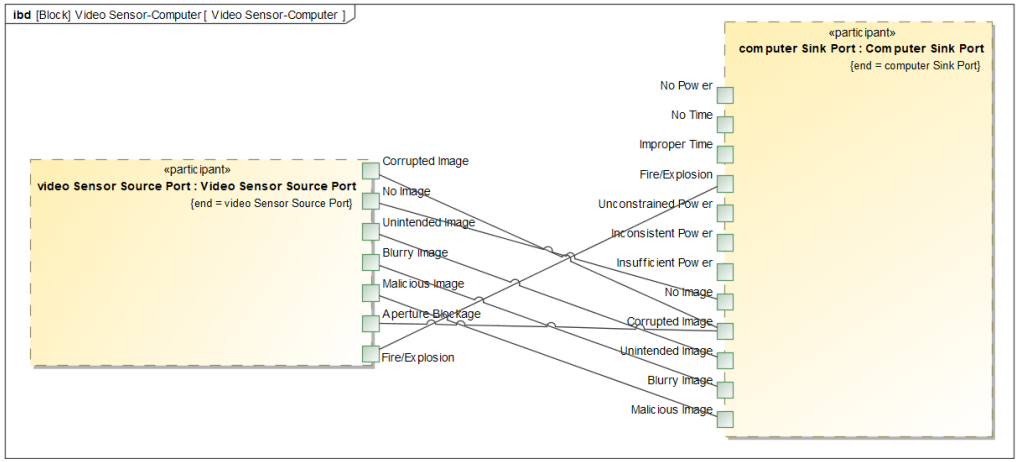
1. Identify Failure Propagation Paths with IBDs



2. Define Internal Component Failure Propagation and Transformation



3. Define Inter-Component Failure Propagation and Transformation



4. Generate Output

Discussion

- Advantages
  - Certification can be performed on the model
  - Allows allocation and tracking of certification requirements conformance
    - Allows data to be retrieved into views and reports
  - Enables the system modelers to more easily communicate with domain experts
  - Presents up-to-date system information on certification status in common, pre-configured formats
  - Generates Certification Authority specific artifacts on demand
- Disadvantages
  - Model-based certification methods are at the research stage
  - SysML v2 has not yet been formally approved and released
  - Requires substantial expertise
  - Agreement with the Certification Authority must be reached on acceptance criteria for formal methods
  - Certification of the model is not the same as certification of the system

Conclusions

Conditions for Successful Certification Using SysML

- Applicant capabilities
  - Capabilities in MBSE
  - Development process based on SysML
  - Inclusion of certification requirements, verification methods in the Model Development Plan
  - Production of Certification Artifacts in the form expected by the Certification Authority
- Certification authority capabilities
  - Development of model acceptance regulatory guidance
  - Model analysis capabilities, methods, and tools
  - Evaluation process
- Model Based Certification Plan
  - Artifacts and evidence to be provided
  - Acceptance criteria
  - Evaluation process
  - Process for modifying the plan

Closing Remark

- Which project will be the first to undergo Model-based Certification?

References

- Stefano Tenotta and Luca Cristoforetti, “Formal verification and safety analysis for SysML v2 with nXmv, OCRA, and xSAP”, presentation at the OMG Systems Modeling Community, February 22, 2024 (available online at www.omg.org)
- Ross Raymond and Myron Hecht, “A SysML Profile for MIL-STD-882E (System Safety)”, 32nd Annual INCOSE International Symposium, June, 2022