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



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

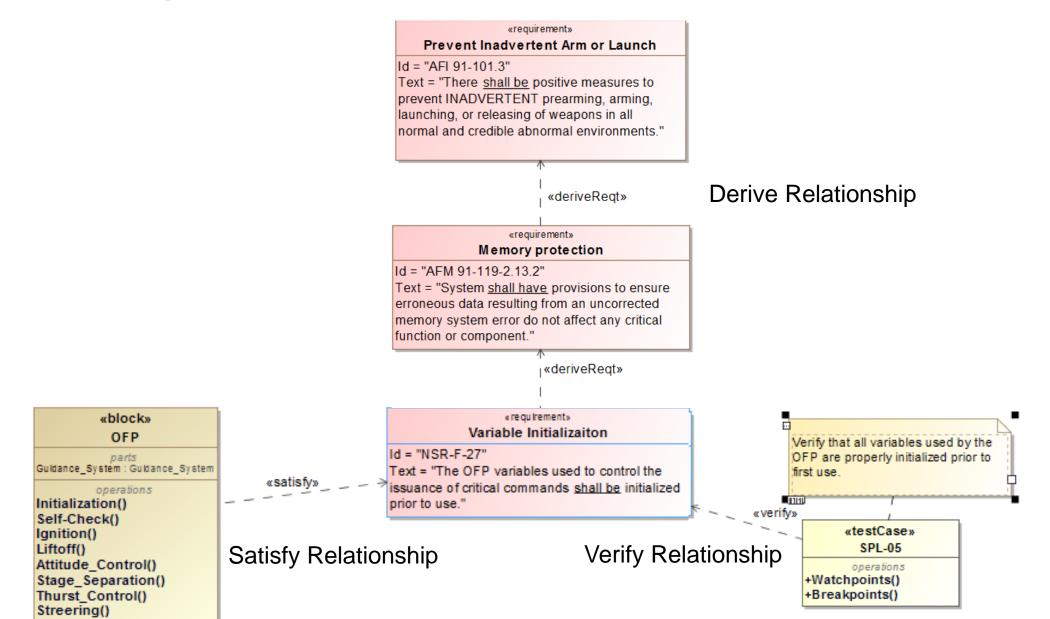
#	Id	△ Name	Text
188	119.2.3.c	R 119.2.3.cHigher Order Language (HOL) 3	Use of Assembly or Machine Language <u>shall be</u> justified in the NCIS in accordance with AFI 63-125, paragraph 3.2.2. Otherwise, a request for deviation <u>shall be</u> submitted.
189	119.2.3.d	R 119.2.3.d Higher Order Language (HOL) 4	The original language <u>shall be</u> used when modifying critical software.
190	119.2.5.a	R 119.2.5.a Fault Tolerance 1	Software <u>shall be</u> 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 <u>shall be</u> 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 <u>shall be</u> 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

- E / Relations
- E Authorized/Unique Signals Transmitted Unaltered() : VerdictKind
- E Critical Command Transmissions() : VerdictKind
- E Critical Function Areas SW Access() : VerdictKind
- E Critical Function HW Installation and Shutdown() : VerdictKind
- E CSCI Contains Only Bit Patterns() : VerdictKind
- Documentation of Scheduling() : VerdictKind
- Erasure of Clear-Text Secure Codes() : VerdictKind
- Error Will Notify Operator and Not Perform Any Critical Function. Operator Can Can
- E Tailure Modes of Hardware are Recognized() : VerdictKind
- FPGA Memory Evaluation() : VerdictKind
- Handling of Deadlock() : VerdictKind
- High Level Nuclear Surety Requirements() : VerdictKind
- E Identify Unauthorized Entries Prior to a Nuclear Function() : VerdictKind
- 🗄 🔂 No Global Variables Used() : VerdictKind
- 🗄 🔁 No Unused Code() : VerdictKind
- 🗄 🔁 Nuclear Permission or Enable Codes Error Correction() : VerdictKind
- E Operator Input Errors Detected/Software Notifes Operator() : VerdictKind
- 🗄 🔁 Prearm Unique Signal Storage() : VerdictKind
- E Routines Initiated through Crewmember Action() : VerdictKind

Verification Criteria from Section 3 of AFMAN 91-119

Allocation of Requirements and Verification Methods



Requirements Allocation Matrix

Legend → Satisfy																								
Satisfy (Implied)																								
	od 3	RV			S	ys	ste	en	n I	ΕI	er	n	en	nts	3									
	Sec	tion			Ξ-		Forv	vard	Secti	ion														
E CONTRACTOR OF CONTRACTOR	Body	/ Sec	tion			-	-	Armi	ng a	nd F	uzing	g As	semb	ly [A	FA]					Ξ		Forw	ard	:
	Icy St			ectrical				10.0	Armi	ng a	nd F	1.1	g Ass		ly [A	_					on As	Trans		
	Radio Frequency	W5RA Cable	Warhead	Warhead Elect				BAT/RSVR Asse		CPC ASSY-	(MPACT EL 0	HIT Connector	auch Safety [PTP Assembly		Radar Ther	Receiver As pi	Iransmitter Stat	Video Proc. a		Forward Section	High Impulse	Nosetip	VIK-21 Mod 3-
	58	31	10	97			207	22	40	17	19	36	94	18	114	25	82	46	26	123	4	13	6	124
D AFMAN 91-118	58	31	10	97			207	22	40	17	19	36	94	18	114	25	82	46	26	123	4	13	6	124
- R 118.2.2.2.1.1.a Critical Functions - Authorization - Device Or	\checkmark			\checkmark	6	5	4						\checkmark		kerer.		\checkmark			K.				K.,
R 118.2.2.2.1.1.b Critical Functions - Authorization - Informatio	2			\checkmark	6	5	4						2		Lerer.		2			K.				<
- R 118.2.2.2.1.2.a Critical Functions - Authorization - Positive D	2			\checkmark	6	5	4						\checkmark		L.		<			×.				<
R 118.2.2.2.1.2.b Critical Functions - Authorization - Protection	\checkmark			\checkmark	6	5	4						\checkmark		kerer.		\checkmark			kerer.				\leq
- R 118.2.2.2.1.2.c Critical Functions - Authorization - Attack/By	\checkmark			\checkmark	7	6	4						\checkmark		kerer.		<	\checkmark		kerer.				< <u> </u>
- R 118.2.2.2.1.2.d Critical Functions - Authorization - Attack/By	\checkmark			\checkmark	7	6	4						\checkmark		Le***		\checkmark	\checkmark		<~				\checkmark
- R 118.2.2.2.1.2.e Critical Functions - Authorization - Latching	\checkmark			\checkmark	7	6	4						\checkmark		14. C		\checkmark	\checkmark		<~				\checkmark
R 118.2.2.2.1.2.f Critical Functions - Authorization - Safing/Rel	\checkmark			\checkmark	7	6	4						\checkmark		Reader.		\checkmark	\checkmark		K.				\swarrow
R 118.2.2.2.1.a Critical Functions - Authorization - Control Dev	\checkmark			\checkmark	6	5	4						\checkmark		Read		\checkmark			<				<
- R 118.2.2.2.1.b Critical Functions - Authorization - Devices to I	1			1	6	5	1						1		lerer.		1			L				

Requirements

Tables showing Requirements and Verification Objectives for Each Component

Component	Allocated Requirements	Related Verification Objectives
	118.2.2.2.1.1.a Critical Functions - Authorization - Device Operation	6
Arming and Fuzing Assembly [AFA]	118.2.2.2.1.1.b Critical Functions - Authorization - Information Control Concept	A&F system chemical compatibility
System Structure::MMIII CBM::Post Boost Vehicle	118.2.2.2.1.2.a Critical Functions - Authorization - Positive Design Features	AMAC and release systems independence
PBV]::Reentry System RS]::Reentry Vehicle	<i>118.2.2.2.1.2.b</i> Critical Functions - Authorization - Protection Against Inadvertent Operation	
RV]::MK-21 Mod 3 V::Forward ection::Forward Section]	118.2.2.2.1.2.c Critical Functions - Authorization - Attack/Bypass of Device	Authorized/Unique Signals Transmitted Unaltered
	118.2.2.2.1.2.d Critical Functions - Authorization - Attack/Bypass Indication	Certification evidence for embedded software and firmware
	118.2.2.2.1.2.e Critical Functions - Authorization - Latching and Protection	Certification evidence for non-specialized COTS equipment
	118.2.2.2.1.2.f Critical Functions - Authorization - Safing/Relocking	6
	Function 118.2.2.2.1.a Critical Functions - Authorization - Control Devices	Certification evidence for specialized COTS equipment
	118.2.2.2.1.6 Critical Functions - Authorization - Control Devices 118.2.2.2.1.6 Critical Functions - Authorization - Devices to Prevent Prearming/Arming	
	118.2.2.2.2.1.a Critical Functions - Prearming - Uniquely Coded Signal	8
	118.2.2.2.2.1.b Critical Functions - Prearming - Command Signal Unavailable	Conformance to MIL-STD- 461 and MIL-STD-464
	118.2.2.2.2.2 Critical Functions - Prearming - Isolation from Circuits	Critical circuit isolation
	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	Design criteria for EMR protection
	<i>118.2.2.2.2.b</i> Critical Functions - Prearming - Separation from Authorization Function	8
	118.2.2.2.2.c Critical Functions - Prearming - Preclusion	Device authorization through command and control channels
	118.2.2.2.3.a Critical Functions - Launching - Control	8

Requirement	Components	Verification Objectives
) 19.2.10.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]]	でしていたのでは、 CSCI Contains Only Bit Patterns
I 19.2.10.b Idle Operations 2	MIL-STD-1750A CPU [System Structure::MIIII ICBM::Post Boost Vehicle [PBV]::Missile Guidance Set [MGS]::N550 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
R 119.2.12.6 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]]	B Identify Unauthorized Entries Prior to a Nuclear Function
R 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]::N550 MGS::Missile Guidance Computer [MGC]::Missile Guidance Computer [MGC]::Computer Memory Module [CMM]]	B Failure Modes of Hardware are Recognized
R 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	원 SW Wait, Stop, and Halt States

Generation of the Certification Plan from the Model using a Template

Table of Contents	Certification Pla
Date: July 16, 2018	Revision: 0.

Table of Contents

Revision	n History	
Table of	Contents	i
Table of	Figures	iv
Executiv	/e Summary	
1. Intro	oduction	1
1.1.	Purpose	1
1.2.	Scope	1
1.3.	Overview	
1.4.	Notes	1
2. Rol	les and Responsibilities	
3. Cer	rtification Requirements and Conformance Verification	6
3.1.	Requirement Allocation Matrices	6
3.1.	.1. MGC Requirements	6
3.1.	.2. Mk21 Mod 3 RV Requirements	
3.1.	.3. Satisfied Requirements [All]	
3.2.	Requirement Verification Matrices	
3.2.	.1. Verification Methods [All]	
3.3.	Components and Verification Objectives	
3.4.	Requirements and Verification Objectives	
3.5.	Structural Diagrams	192
3.5.	.1. AFA BDD	192
3.5.	.2. AFA Requirements BDD	

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

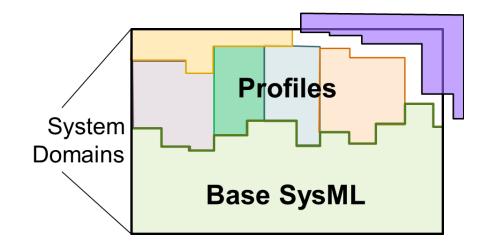
Use of a Profile to Extend SysML to a Specific Domain

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

13

- Pre-configured **diagrams and tables**, for displaying the new information
- Templates for Exported Artifacts
 - Templates for external **documents and reports**, for extracting profile information

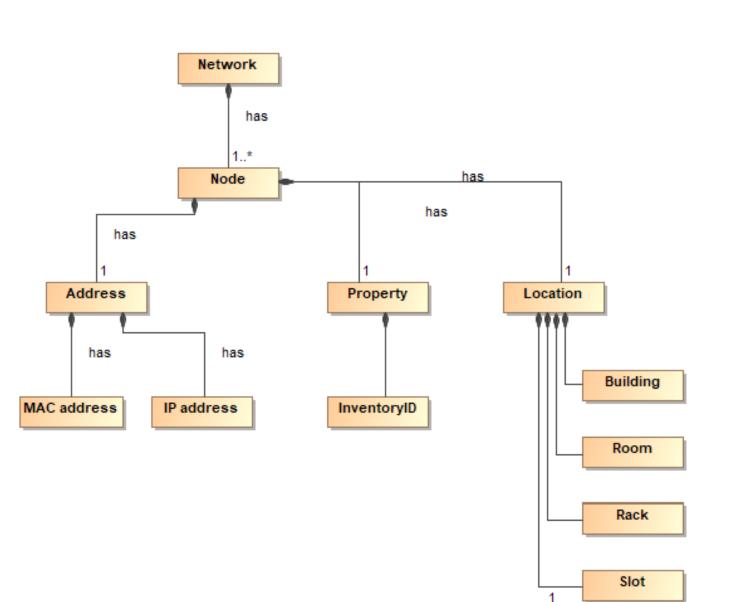


What does a Profile Consist Of?

- 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)

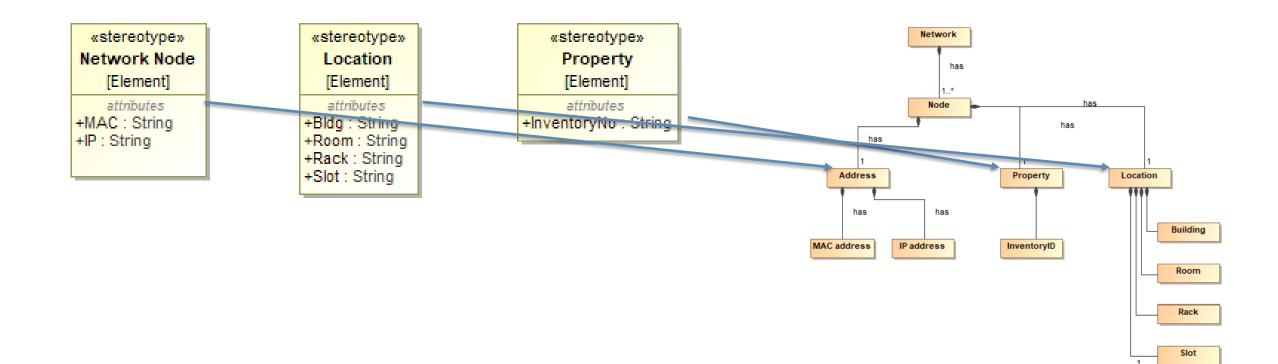
- Meta-Models describe the relationships between profile concepts
- A profile begins with a concept, translated into the modeling language and refined
 - For example, define the concepts for a local area computer network (LAN)



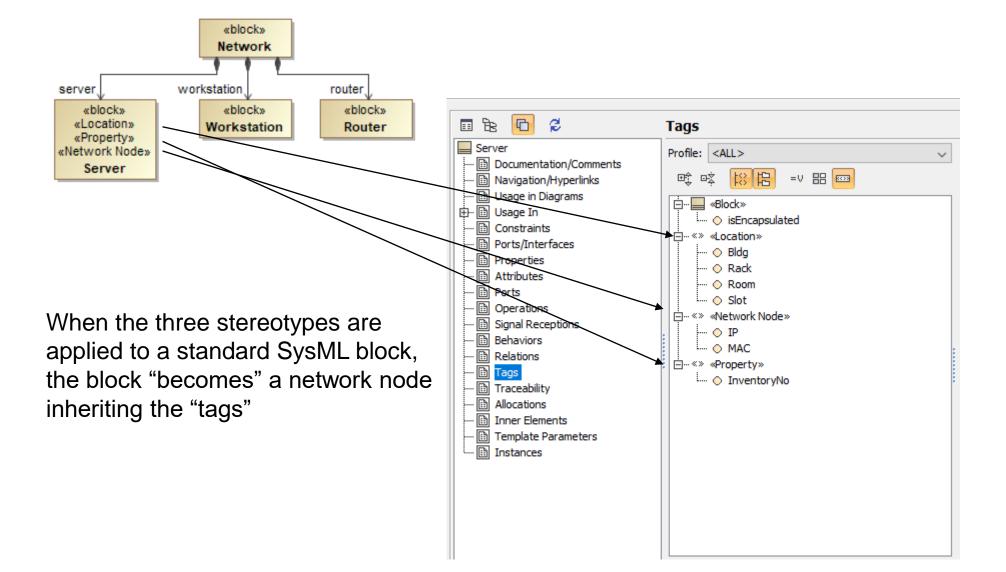
Stereotypes for the LAN Meta-Model

Animated

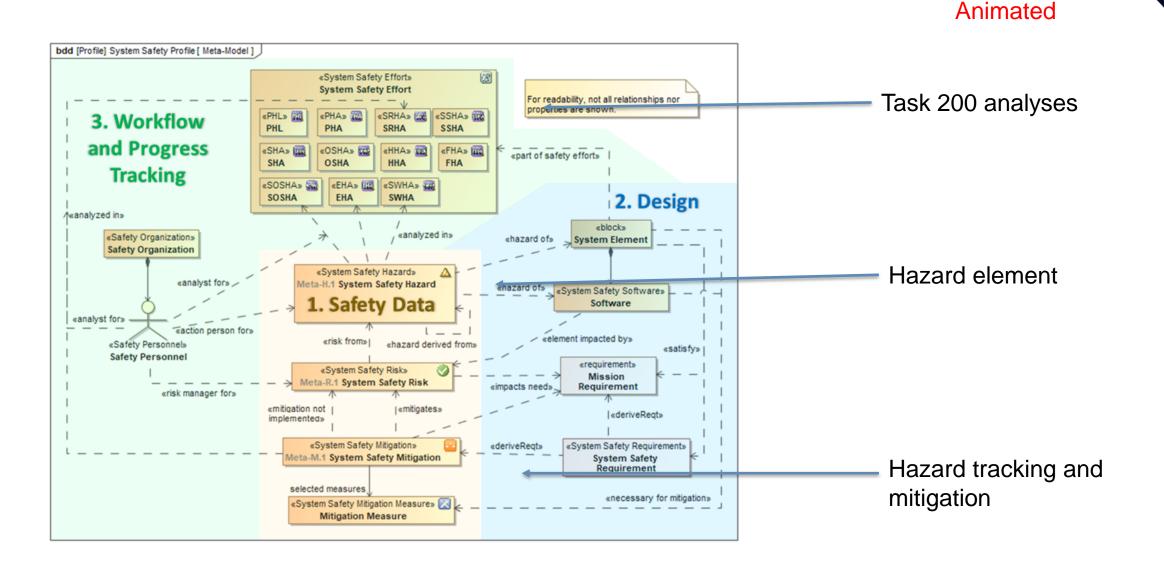
Using the LAN meta-model, we define a simple profile that consists of 3 stereotypes



Applying the LAN Stereotypes



System Safety Profile Meta-Model



Tables produced from Queries in the Profile

H	AZARDS	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 		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	A Ex-H.3 Example 3 Safety H	Example System	ℜ PHL Example

F	RIS	SKS	Name	Hazards	Mitigations	Risk Status	Initial Risk Assessment Code	Target Risk Assessment Code	Final Risk Assessment Code
				A Ex-H.1 Example 1 Safety Hazar					-
1		Ex-R.1	🕜 Example 1 Safety Risk		Ex-M.5 Example 1 Safety Mi		▲ 1A	1F	1E
					Ex-M.6 Example 1 Safety Mi				
2		Ex-R.2	Example 2 Safety Risk	A Ex-H.2 Example 2 Safety Hazar	😨 Ex-M.2 Example 2 Safety Mi	Realized	1A 1A		<u>∧</u> 28

N	ITIGATIO	NS Name	△ Hazards	Impacted Needs	Mitigation Description	Mitigation Measures List	Derived Requirements	Mitigation Status
1	Ex-M.1	Example 1 Safety Mitigation	A Ex-H.1 Example 1 Safety Hazard	R Ex-SysReq.1 Example 1 Requirement	Mitigation through software fix	 Example 1 Mitigation Measure Example 2 Mitigation Measure 		Not Implemented
2	Ex-M.2	😌 Example 2 Safety Mitigation		R 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		R Ex-SysReq.3 Example 3 Requirement R Ex-SysReq.4 Example 4 Requirement				Not Implemented

P	ROGRESS	△ Stereotype	Name	Safety Hazard Analysis	Analysis Start Date	Analysis Completion Date	Analyst	Comments	o actualCompletionDate
-	1 10201 03	🔬 System Safety Hazard [Cla	A 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 [Cla	A 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 [Cla	A 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 Mitigatio	🔁 SRHA Example	7/9/18	11/15/19			8/20/19
5	Mitigations	😨 System Safety Mitigation	Ex-M.2 Example 2 Safety Mitigation	SRHA Example	7/9/18	11/15/19	♀ Safety Analyst 2		

Implemented using generic table capability of Cameo Systems Modeler

Model Exports: Risk Matrix

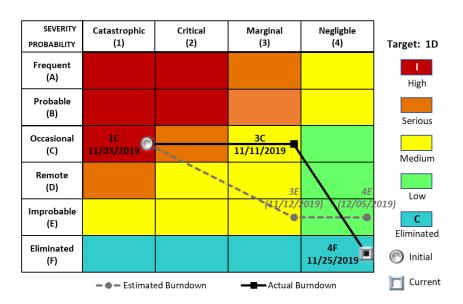
System Safety Risk Matrix (template)

- 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

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



2/ww.incose.org/symp2022

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

Program	: Name of	the safety	effort o	or similar con	struc	t in w	hich I	Hazard: //	azard ID	Name of t	he		
-		g analyzed.			ourae			hazard ele	-	indine of a			
	DPEN/CLO	· · ·		comma-sepa	arated	l list o	of the type	of hazard	(e.g. elec	trical therm	al etc.)		
				-									
		-		st of the failu				-	_				
PHL	PHA	SSHA	SHA	O&SHA	н	A	FHA	SOSHA	EHA	SwHA	SRHA		
CMPLT	IP	N/A											
	-			affected by th	ne	Hea	lth Conditi	ions: The	condition	s impacting			
-	-	-	-	by comma.			onnel hea		-				
•				hase of the						of the syste			
mission when the hazard could be encountered. affected by the hazard, separated by comma.													
System Operation Description: A description of the environmental Components: The components of the													
nominal operation of the system environment affected by the hazard, separated by comma.													
						com	ima.						
	escription	-											
	iled descri f Hazard:	ption of th	e hazaro	l, including a			ise statem	ent of the	condition	1.			
	т наzага: lleted list c			Effects o					4h - h		L		
- A bu	lieted list o	of causes								d, along wit	n		
					lileteo		of the diffe				,		
	te: The da d or discov		he hazar	d was first		1				person in ch	arge of		
							or managing the hazard						
INITIAL R		nitial Risk		TARGET RAC		Target Risk <u>FINAL</u> RAC: Final, accepted Risk							
Severity:	1	4		Severity:		1-4		Seve	rity:	1-4			
Probabili	ity: A	- F		Probability:		A - F Probability: A - F							
Multiple	mitigation	s, each wit	h their c	own measure	s, ma	y be a	ssociated	with a sing	gle hazard	. Hence, the	ere may		
be severa	al mitigatio	on sections	-										
Mitigatio	on Approa	<u>ch</u> :											
The over	all descrip	tion of the	mitigati	on.									
Recomm	ended Act	tion:											
1. (Nan	ne of Meas	<i>ure)</i> Numb	ered list	t of actions fr	om as	ssocia	ited measu	ires and o	rdered by	measure ty	pe.		
		•		zard Frequen	icy Da	ita:							
		nded Actio											
Status an	id impact o	of recomm	ended o	r other hazar	d con	trols.							
Date of A	Analysis:					Ana	lyst:						
Commen	ts:												
Supporti	ng Docum	entation:											
List of lin	ks to or na	mes of do	cumenta	ation support	ing th	e info	ormation a	bove.					

- 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

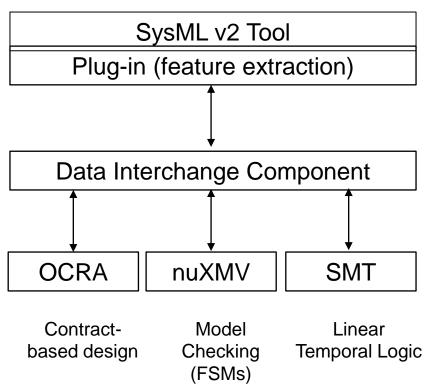
- Advantages
 - Combines program- and domain-specific information with the system design model
 - Allows relevant certification data to be entered directly into the primary architecture model
 - Allows allocation and tracking of certification requirements conformance
 - Allows data to be retrieved into 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 to 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 wellestablished formal methods tools to be connected to the model and used for analysis



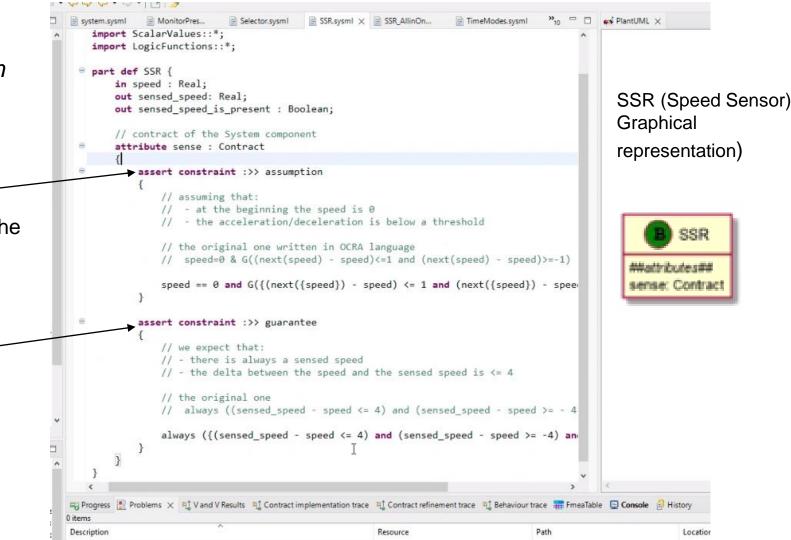
Example: SysML Block Definition with Assumption-Guarantee Contract

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

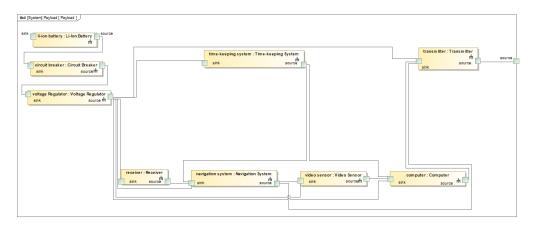
Guarantee attribute

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



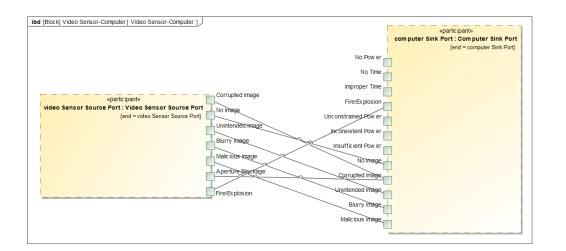
SysML v2 example from model developed by Stefano Tonetta and Luca Cristoforetti, FBK Institute, Italy, 2024

Automated Generation of FMEAs from SysML Models

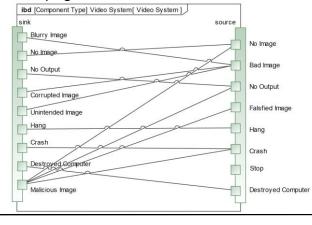


1. Identify Failure Propagation Paths with IBDs

3. Define Inter-Component Failure Propagation and Transformation



2. Define Internal Component Failure Propagation and Transformation



4. Generate Output

				and the second second	Teller Block		and the second se		in the second		the second se		and the second	and the second second		
	Hardware		No Time				and Chiefs Consideration		A LAND COMPANY	Unknown Mitigation			22	Accessing at Lawrence b.		
hardware	Cornel	_	No Time				0 <u>1</u>		6 Unknown Detection			-	0 0	4 9		
system Contro		1.18	No Time				3 3			Unknown Mitigation		-	0 0			
system Contro		-	Peorine				n		Mouraiswa Passesson	Interioran semilarities I	concernment in the second s	91	0 0	an Arra Million Cost Physics	the second second	
system Contro	1						Mission									
hardware					kernel: No Ti											
kernel				Unspecified			Terminatio						Unknown	Unknown Unknown		
System Contro	2 Hardwar	e	No Time	Cause	system Contr	rol: Bad Time	Computer Result		1 Unknown Detectio	in Unknown Mitigat	ion Unknown Protection	ń.	4 Detection	Mitigation Protection		
Bardware				and the second second	and the second second		Informediate Effects	Test Common	Initellier Se	and the second second second	Include And Uncertaintie			mentions First Detection	A 1 8 8 1 1 1 1 1 1	
kernel			A DESIGNATION				video System: Malicious									
comm System																
System Contro					Malicious	Unspecified								Reasonability		
video System			62 kernel	Kernel	Image		video System: Crash	Computer	Loss of Data	3 Unknown Del	tection Unknown Mitiga	ition Unknown	Protection	3 Check	Restart	Input Validat
hardware	3 Haroware						video System: Corrupted									
kernel					Corrupted	Unspecified	Image;							Reasonability		
Comm System			63 kernel	Kernel	Image	Cause	video System: Bad Image	Computer	Bad Image	2 Reasonability	Check	Input Vali	dation	3 Check		Input Validat
system Contre							video System: Unintended		1.							
Video System					Unintended	Unspecified	Imane							Reasonability		
	4 Hardwar		64 kernel	Kernel	Image		video System: Bad Image	Computer	Bad Image	2 Reasonability	Check	input Vali	dation	3 Check		Input Validat
kernel			and Manager	NAULURI .	or office	Unspecified	annen sästene nan midde	Composes	and scored a	a measurations	Collect.	ingres you		a contra		
video System				10000			100000 and a 10000 and a 1000	2010020	10.001223000	100000000000000000000000000000000000000			2012 (22)		la series de la se	Unknown
hardware		- 1	65 kernel	Kernel	Hang		comm System: Hang	Computer	Loss of Data	5 Unknown Del	tection Unknown Mitiga	tion Unknown	Protection	2 Timer Expiration	Restart	Protection
kernel						Unspecified										Unknown
video System			66 kernel	Kernel	Hang	Cause	system Control: Hang	Computer	Loss of Data	3 Unknown Del	tection Unknown Mitiga	tion Unknown	Protection	2 Timer Expiration	Restart	Protection
video System	5 Hardwan	e				Unspecified										
hardware			67 kernel	Kernel	Hang	Cause	video System: Hang	Computer	No Image	2 Reasonability	Check	input Vali	dation	2 Timer Expiration	Restart	Input Validati
kernel						Unspecified										Unknown
Video System			68 kernel	Kernel	Hang	Cause	video System: Hang	Computer	Loss of Data	3 Unknown Det	tection Unknown Mitiga	dion Unknown	Protection	2 Timer Expiration	Restart	Protection
video System						Unspecified										Unknown
video System	6 Hardwan		se kernel	Kernel	Crash		comm System: Crash	Computer	Loss of Data	2 Hoknown Del	tection Unknown Mitiga	tion Heknown	Destaction	2 Timer Expiration	Restart	Protection
hardware			and Marriel	NULL PAGE	Crazii	Unspecified	contra spacette crush	comparer	0000000000	2 011010111 00	interest conservation interests	and an and an	Protection.	2 Thinks Coperation	merinis	Unknown
3 kernel			21 0000000	Xernal	1000000		system Control: Crash	Gamman (providence.	1211200/0725	1	577 1378 TAVA	1000000000	2222000	2722	
ĺ			70 kernel	Kernel	Crash		system control: crash	Computer	Loss of Data	3 Unknown Del	tection Unknown Mitiga	tion Unknown	Protection	2 Timer Expiration	Restart	Protection
						Unspecified										
			71 kernel	Kernel	Crash		video System: Crash	Computer	No Image	2 Reasonability	Check	Input Vali	dation	2 Timer Expiration	Restart	Input Validati
	7 Hardwan	e				Unspecified										Unknown
			72 kernel	Kernel	Crash	Cause	video System: Crash	Computer	Loss of Data	3 Unknown Det	tection Unknown Mitiga	ition Unknown	Protection	2 Timer Expiration	Restart	Protection
					Destroyed	Unspecified	comm System: Destroyed		Destroyed					Unknown	Unknown	Unknown
	8 Hardwar		73 kernel	Kernel	Computer	Cause	Computer	Computer	Computer	1 Unknown Det	tection Unknown Mitiga	tion Unknown	Protection	2 Detection	Mitigation	Protection
		-			Destroyed	Unsperified	comm System: Destroyed							Unknown	Unknown	Unknown
			74 kernel	Kernel	Computer		Computer	Computer	Comm Failure	2 Linknown Del	tection Unknown Mitiga	tion linknown	Drotection	2 Detection		Protection
			and second		computer	cause	Construction of the second sec		Mission	a orangem pe	and the model of the second se	Contra Contra Contra		* 0-10000	anagation	
	9 Hardwan	6			10 South States	12233								10000000	12112	202000
				15 97	Destroyed		system Control: Destroyed		Terminating	72.07 23	SAN 1973 3224			Unknown	Unknown	
		-	75 kernel	Kernel	Computer		Computer	Computer	Result	1 Unknown Det	tection Unknown Mitiga	ition Unknown	Protection	2 Detection		Protection
					Destroyed		system Control: Destroyed		Destroyed					Unknown		Unknown
			76 kernel	Kernel	Computer	Cause	Computer	Computer	Computer	1 Unknown Det	tection Unknown Mitiga	ition Unknown	Protection	2 Detection	Mitigation	Protection

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
 - $\circ~$ Development process based on SysML
 - o 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
 - $\circ~$ Model analysis capabilities, methods, and tools
 - Evaluation process
- Model Based Certification Plan
 - $\circ~$ Artifacts and evidence to be provided
 - Acceptance criteria
 - Evaluation process
 - $\circ~$ 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 <u>www.omg.org</u>)
- Ross Raymond and Myron Hecht, "A SysML Profile for MIL-STD-882E (System Safety)", 32nd Annual INCOSE International Symposium, June, 2022