Architecture Viewpoints of STPA Analysis

2024 MIT STAMP Workshop

AGENDA:

1) *Introduction*

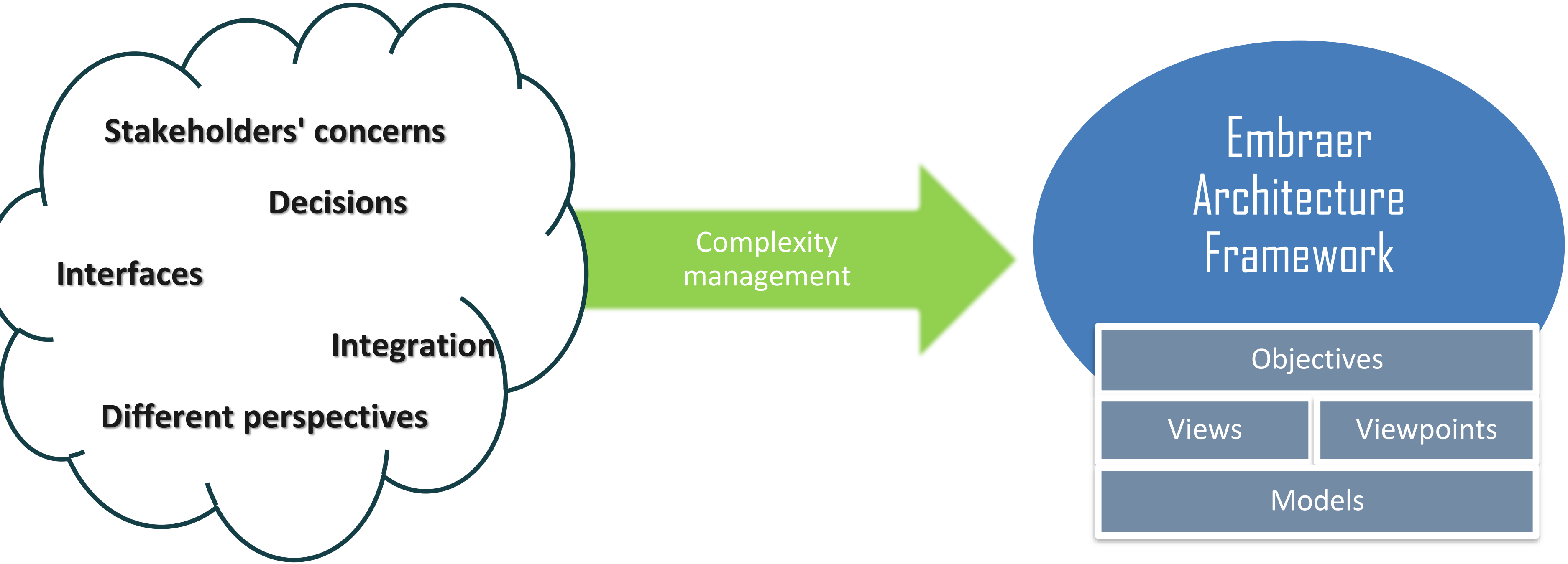
2) *Methodology*

3) *Viewpoints and views*

4) *Conclusion*

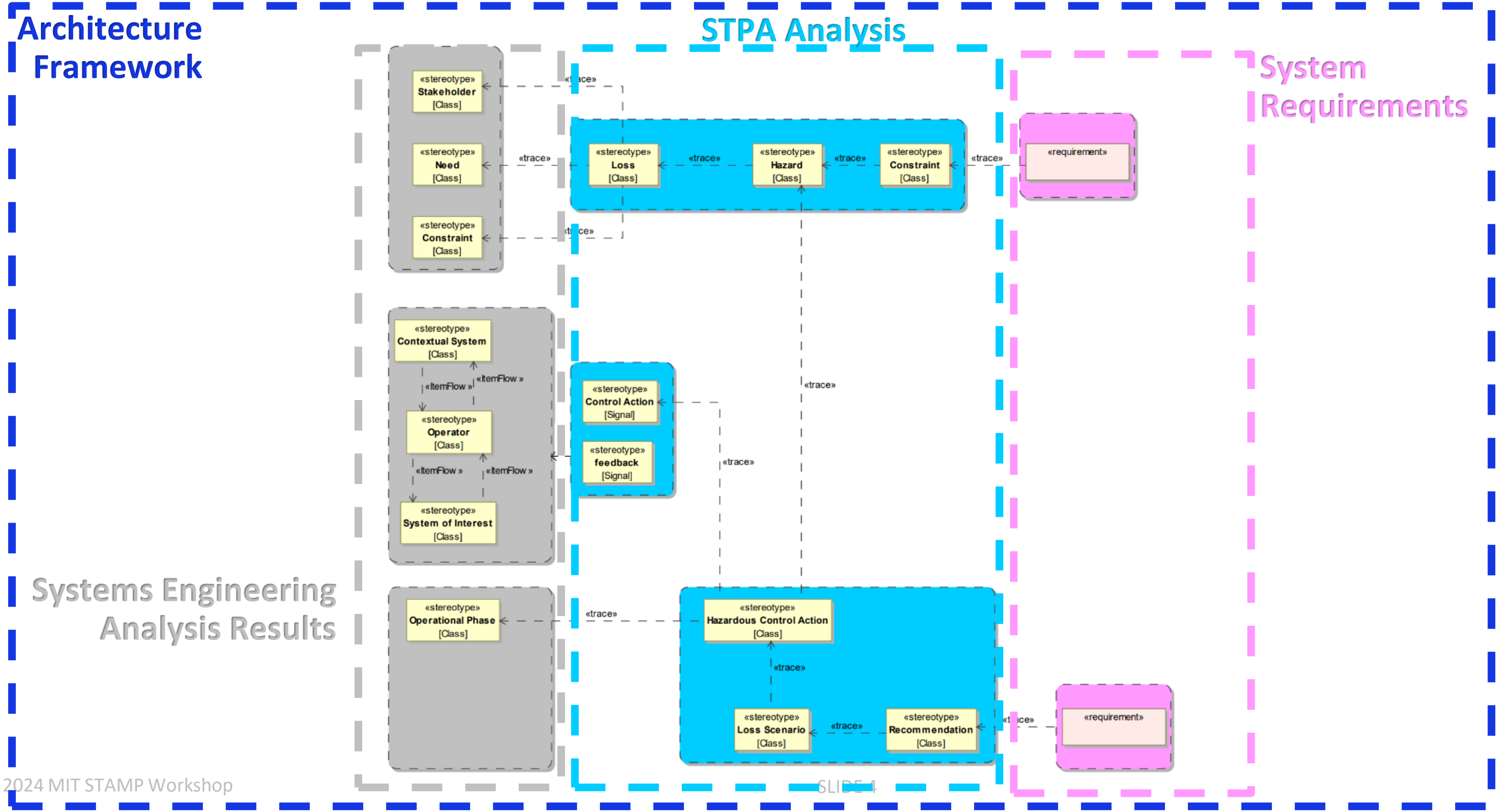
ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

Architecture frameworks establishes which results are focused on a set of objectives and integrates different perspectives for managing decisions, information, interfaces.



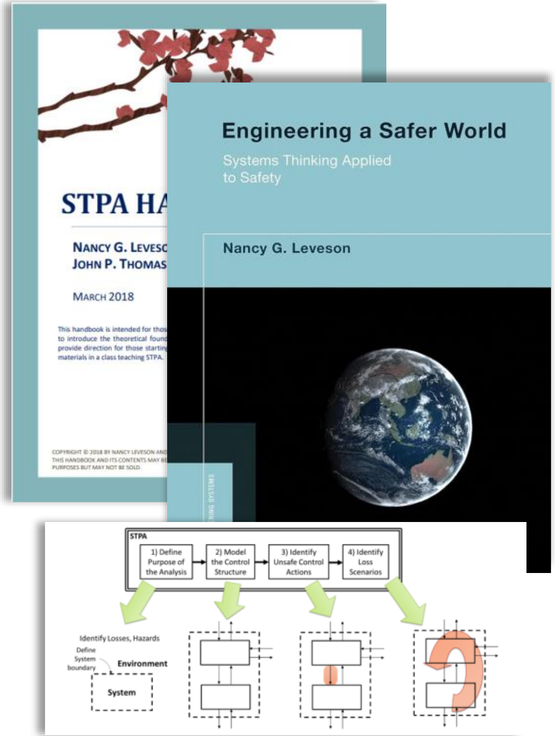
ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

The STPA should be integrated into an Architecture Framework to communicate the recommendations, requirements and scenarios to the project team and stakeholders and trace the STPA results to the respective architecture decisions.


Architecture Framework
STPA Analysis
System Requirements
Systems Engineering Analysis Results
«stereotype» Stakeholder [Class]
«stereotype» Need [Class]
«stereotype» Constraint [Class]
«stereotype» Loss [Class]
«stereotype» Hazard [Class]
«stereotype» Constraint [Class]
«requirement»
«trace»
«stereotype» Contextual System [Class]
«ItemFlow»
«stereotype» Operator [Class]
«stereotype» System of Interest [Class]
«stereotype» Control Action [Signal]
«stereotype» feedback [Signal]
«stereotype» Operational Phase [Class]
«stereotype» Hazardous Control Action [Class]
«stereotype» Loss Scenario [Class]
«stereotype» Recommendation [Class]
«requirement»

ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

Embraer methodology to construct architecture viewpoints for the STPA Analysis considers:



STPA HA

NANCY G. LEVESO
JOHN P. THOMAS

MARCH 2018

This handbook is intended for thos
to introduce the theoretical found
provide direction for those startin
materials in a class teaching STPA.

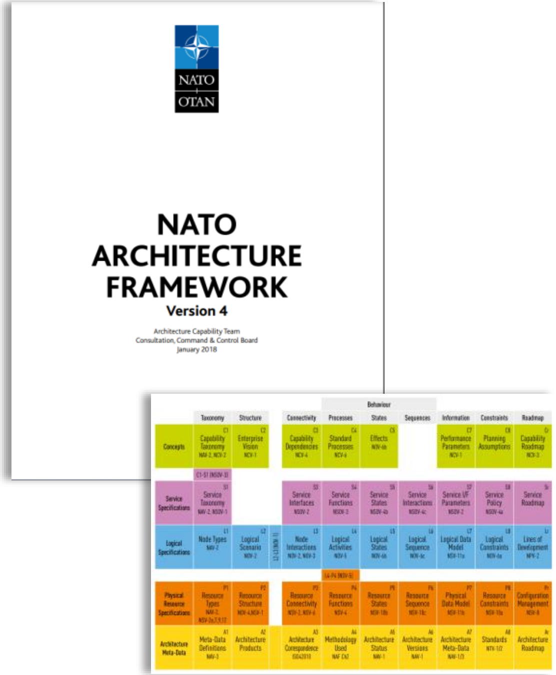
COPYRIGHT © 2018 BY NANCY LEVESON AND
THIS HANDBOOK AND ITS CONTENTS MAY BE
PURPOSES BUT MAY NOT BE SOLD.

Engineering a Safer World

Systems Thinking Applied to Safety

Nancy G. Leveson

STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System



NATO OTAN

NATO ARCHITECTURE FRAMEWORK

Version 4

Architecture Capability Team
Consultation, Command & Control Board
January 2018

					Behaviour					
	Taxonomy	Structure		Connectivity	Processes	States	Sequences	Information	Constraints	Roadmap
Concepts	C1 Capability Taxonomy NAV-2, NCV-2	C2 Enterprise Vision NCV-1		C3 Capability Dependencies NCV-4	C4 Standard Processes NCV-6	C5 Effects NOV-6b		C7 Performance Parameters NCV-1	C8 Planning Assumptions	Cr Capability Roadmap NCV-3
	C1-S1 (NSOV-3)									
Service Specifications	S1 Service Taxonomy NAV-2, NSOV-1			S3 Service Interfaces NSOV-2	S4 Service Functions NSOV-3	S5 Service States NSOV-4b	S6 Service Interactions NSOV-4c	S7 Service I/F Parameters NSOV-2	S8 Service Policy NSOV-4a	Sr Service Roadmap
Logical Specifications	L1 Node Types NAV-2	L2 Logical Scenario NOV-2	L2-L3 (NOV-1)	L3 Node Interactions NOV-2, NOV-3	L4 Logical Activities NOV-5	L5 Logical States NOV-6b	L6 Logical Sequence NOV-6c	L7 Logical Data Model NSV-11a	L8 Logical Constraints NOV-6a	Lr Lines of Development NPV-2
					L4-P4 (NSV-5)					
Physical Resource Specifications	P1 Resource Types NAV-2, NSV-2a,7,9,12	P2 Resource Structure NOV-4, NSV-1		P3 Resource Connectivity NSV-2, NSV-6	P4 Resource Functions NSV-4	P5 Resource States NSV-10b	P6 Resource Sequence NSV-10c	P7 Physical Data Model NSV-11b	P8 Resource Constraints NSV-10a	Pr Configuration Management NSV-8
Architecture Meta-Data	A1 Meta-Data Definitions NAV-3	A2 Architecture Products		A3 Architecture Correspondence ISO42010	A4 Methodology Used NAF Ch2	A5 Architecture Status NAV-1	A6 Architecture Versions NAV-1	A7 Architecture Meta-Data NAV-1/3	A8 Standards NTV-1/2	Ar Architecture Roadmap

INTERNATIONAL STANDARD

ISO/IEC/IEEE 42010

First edition
2011-12-01

Systems and software engineering — Architecture description

Ingénierie des systèmes et des logiciels — Description de l'architecture

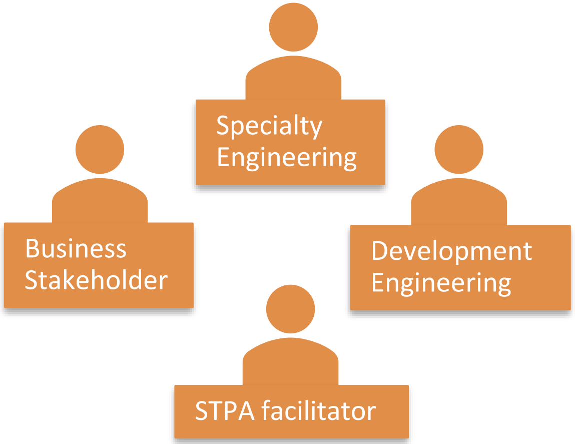
Reference number
ISO/IEC/IEEE 42010:2011(E)

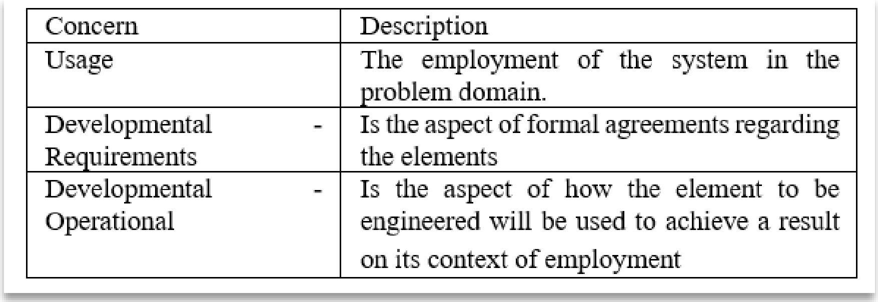
© ISO/IEC 2011
© IEEE 2011

METHODOLOGY STEPS

ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

1. **Identification of the stakeholders of the STPA Analysis;**
2. **Identification of stakeholders’ concerns;**

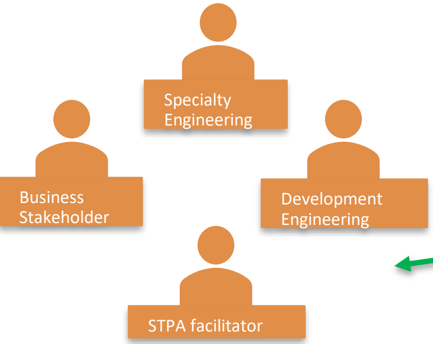


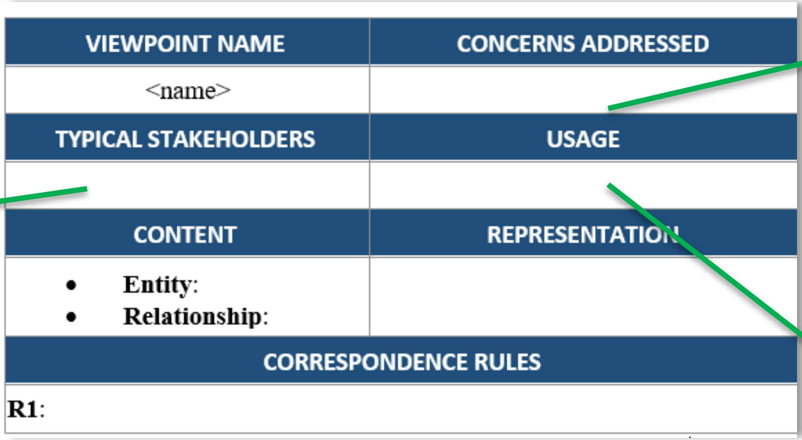


Concern	Description
Usage	The employment of the system in the problem domain.
Developmental - Requirements	Is the aspect of formal agreements regarding the elements
Developmental - Operational	Is the aspect of how the element to be engineered will be used to achieve a result on its context of employment

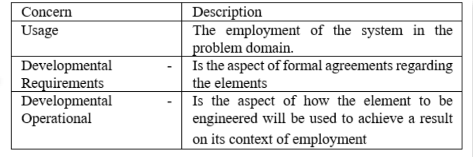
ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

3. Definition of each viewpoint identification (Viewpoint Name);
4. Relating each viewpoint to one or more concerns framed by them (Concerns addressed);
5. Relating each viewpoint to the stakeholders that have the aforementioned concerns (Typical Stakeholders);
6. Description of how the stakeholders will use the information conveyed on a view from the viewpoint (Usage);





VIEWPOINT NAME	CONCERNS ADDRESSED
<name>	
TYPICAL STAKEHOLDERS	USAGE
CONTENT	REPRESENTATION
• Entity: • Relationship:	
CORRESPONDENCE RULES	
R1:	



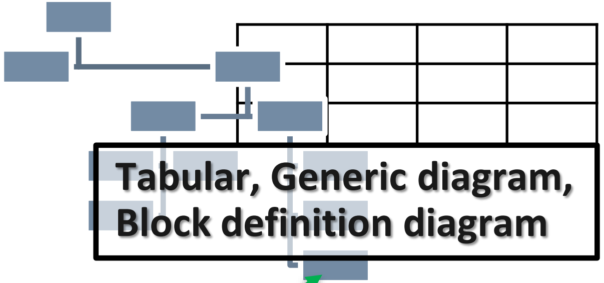
Concern		Description
Usage		The employment of the system in the problem domain.
Developmental Requirements	-	Is the aspect of formal agreements regarding the elements
Developmental Operational	-	Is the aspect of how the element to be engineered will be used to achieve a result on its context of employment

<The stakeholders will use this viewpoints to identify and validate [...]>

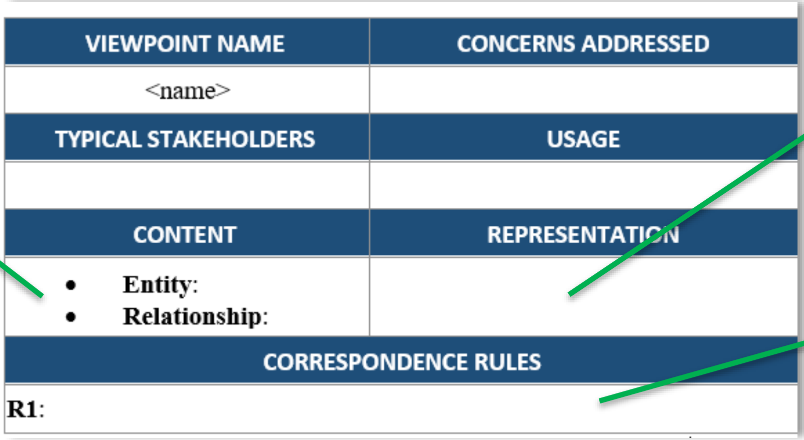
METHODOLOGY STEPS

ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

7. Definition of the content to be conveyed by the views of each viewpoint (Content)
8. Suggestion of alternative representations for each viewpoint (Representation)
9. Definition of correspondence rules for checking consistency of each viewpoint (external and internal)


Tabular, Generic diagram, Block definition diagram

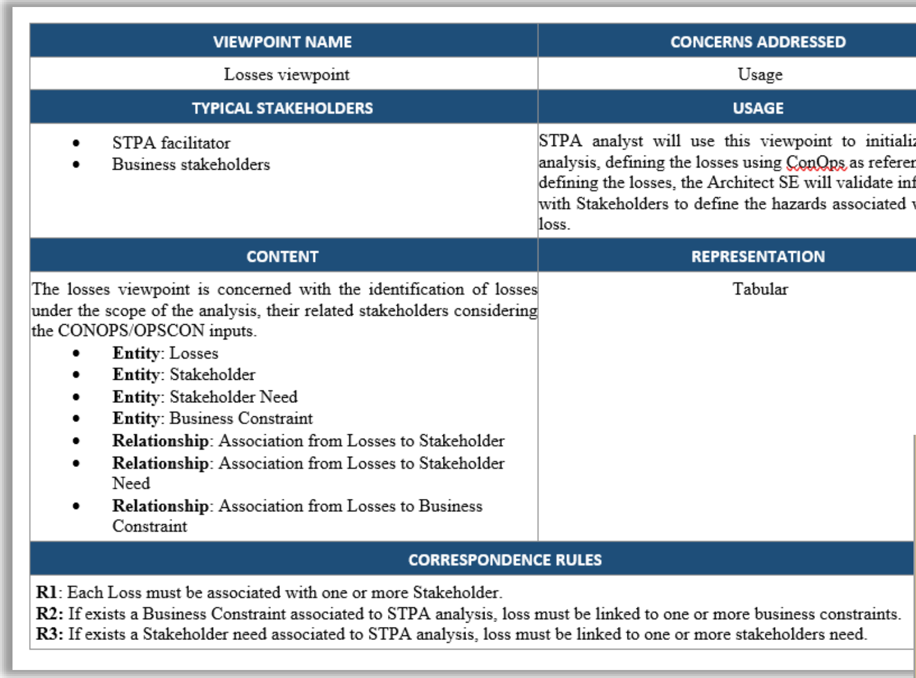
- Loss
- Hazard
- Constraint
- Control Entity
- Control Action
- Feedback
- Information
- Hazardous Control Action
- Loss Scenario
- Operational Phase
- Recommendation
- Association



VIEWPOINT NAME	CONCERNS ADDRESSED
<name>	
TYPICAL STAKEHOLDERS	USAGE
CONTENT	REPRESENTATION
• Entity: • Relationship:	
CORRESPONDENCE RULES	
R1:	

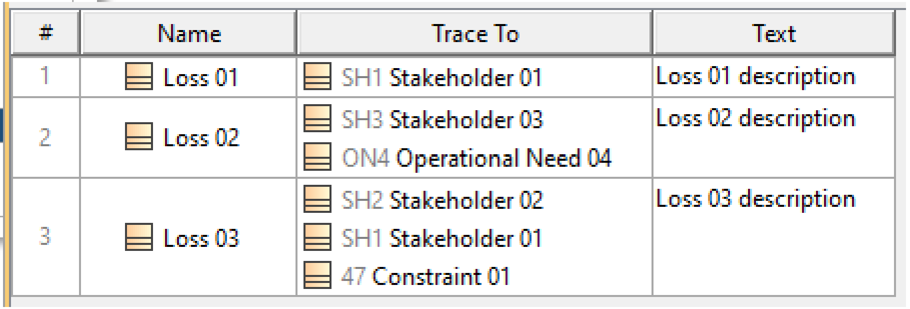
Rules to ensure consistency between the entities according to the STPA analysis

ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS



VIEWPOINT NAME	CONCERNS ADDRESSED
Losses viewpoint	Usage
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator • Business stakeholders	STPA analyst will use this viewpoint to initialize STPA analysis, defining the losses using ConOps as reference. After defining the losses, the Architect SE will validate information with Stakeholders to define the hazards associated with each loss.
CONTENT	**REPRESENTATION**
The losses viewpoint is concerned with the identification of losses under the scope of the analysis, their related stakeholders considering the CONOPS/OPSCON inputs. • **Entity**: Losses • **Entity**: Stakeholder • **Entity**: Stakeholder Need • **Entity**: Business Constraint • **Relationship**: Association from Losses to Stakeholder • **Relationship**: Association from Losses to Stakeholder Need • **Relationship**: Association from Losses to Business Constraint	Tabular
CORRESPONDENCE RULES	
R1: Each Loss must be associated with one or more Stakeholder. **R2:** If exists a Business Constraint associated to STPA analysis, loss must be linked to one or more business constraints. **R3:** If exists a Stakeholder need associated to STPA analysis, loss must be linked to one or more stakeholders need.	

LOSSES VIEWPOINT



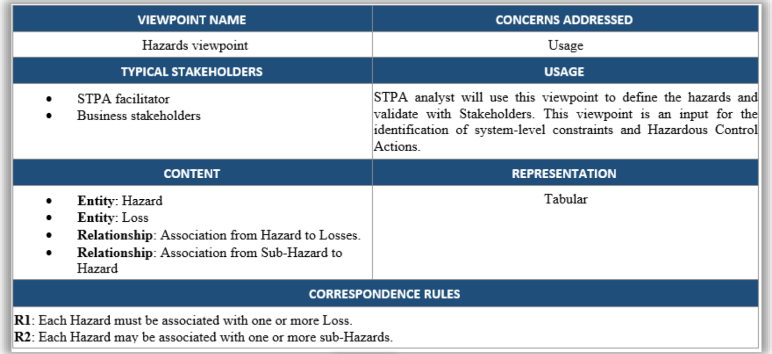
#	Name	Trace To	Text
1	Loss 01	SH1 Stakeholder 01	Loss 01 description
2	Loss 02	SH3 Stakeholder 03 ON4 Operational Need 04	Loss 02 description
3	Loss 03	SH2 Stakeholder 02 SH1 Stakeholder 01 47 Constraint 01	Loss 03 description

VIEW

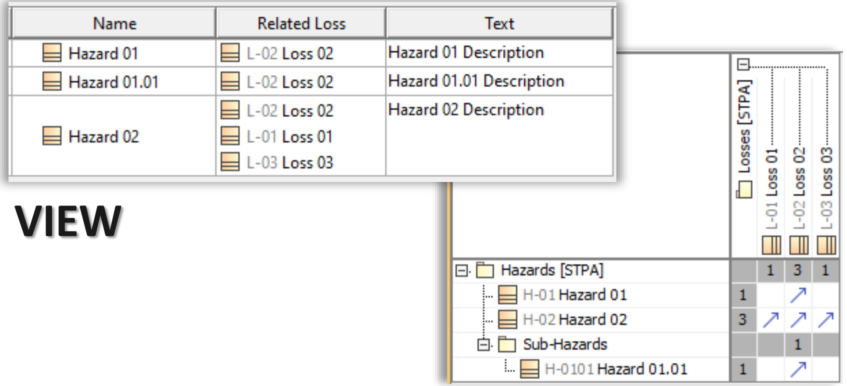
RESULTS

ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

HAZARDS VIEWPOINT



VIEWPOINT NAME	CONCERNS ADDRESSED
Hazards viewpoint	Usage
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator • Business stakeholders	STPA analyst will use this viewpoint to define the hazards and validate with Stakeholders. This viewpoint is an input for the identification of system-level constraints and Hazardous Control Actions.
CONTENT	**REPRESENTATION**
• **Entity**: Hazard • **Entity**: Loss • **Relationship**: Association from Hazard to Losses. • **Relationship**: Association from Sub-Hazard to Hazard	Tabular
CORRESPONDENCE RULES	
R1: Each Hazard must be associated with one or more Loss. **R2**: Each Hazard may be associated with one or more sub-Hazards.	



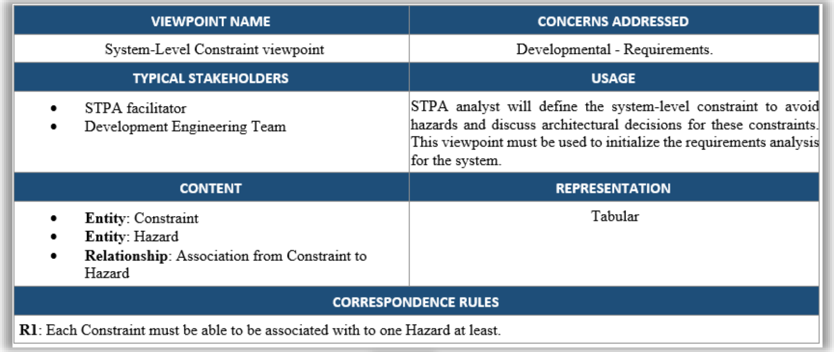
Name	Related Loss	Text
Hazard 01	L-02 Loss 02	Hazard 01 Description
Hazard 01.01	L-02 Loss 02	Hazard 01.01 Description
Hazard 02	L-02 Loss 02 L-01 Loss 01 L-03 Loss 03	Hazard 02 Description

		Losses [STPA]: L-01 Loss 01	L-02 Loss 02	L-03 Loss 03
Hazards [STPA]		1	3	1
H-01 Hazard 01	1		↗	
H-02 Hazard 02	3	↗	↗	↗
Sub-Hazards			1	
H-0101 Hazard 01.01	1		↗	

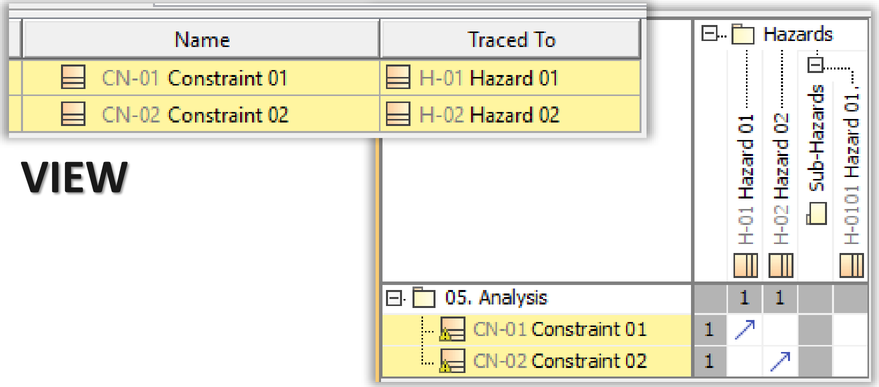
VIEW

VIEW

SYSTEM-LEVEL CONSTRAINT VIEWPOINT



VIEWPOINT NAME	CONCERNS ADDRESSED
System-Level Constraint viewpoint	Developmental - Requirements.
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator • Development Engineering Team	STPA analyst will define the system-level constraint to avoid hazards and discuss architectural decisions for these constraints. This viewpoint must be used to initialize the requirements analysis for the system.
CONTENT	**REPRESENTATION**
• **Entity**: Constraint • **Entity**: Hazard • **Relationship**: Association from Constraint to Hazard	Tabular
CORRESPONDENCE RULES	
R1: Each Constraint must be able to be associated with to one Hazard at least.	



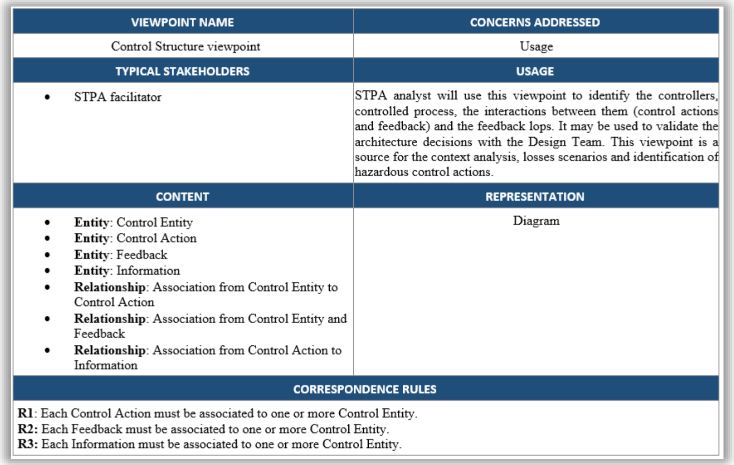
Name	Traced To
CN-01 Constraint 01	H-01 Hazard 01
CN-02 Constraint 02	H-02 Hazard 02

		Hazards: H-01 Hazard 01	H-02 Hazard 02	Sub-Hazards	H-0101 Hazard 01.01
05. Analysis		1	1		
CN-01 Constraint 01	1	↗			
CN-02 Constraint 02	1		↗		

VIEW

VIEW

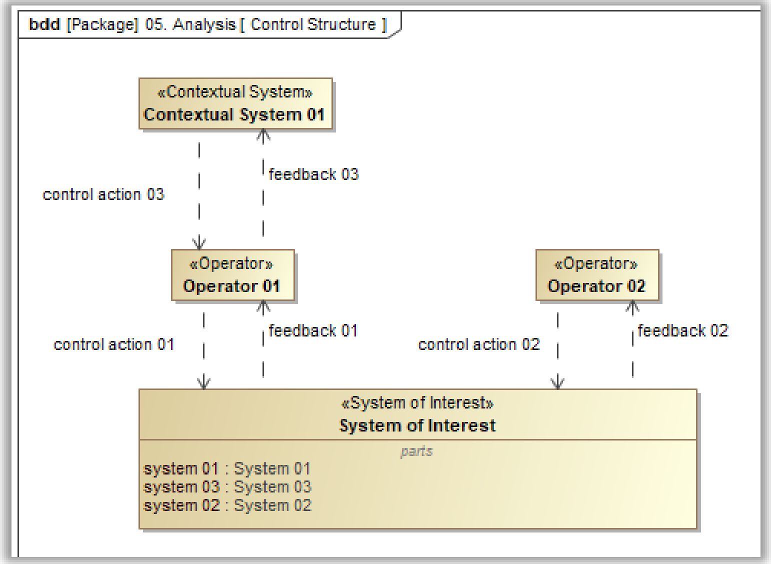
ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS



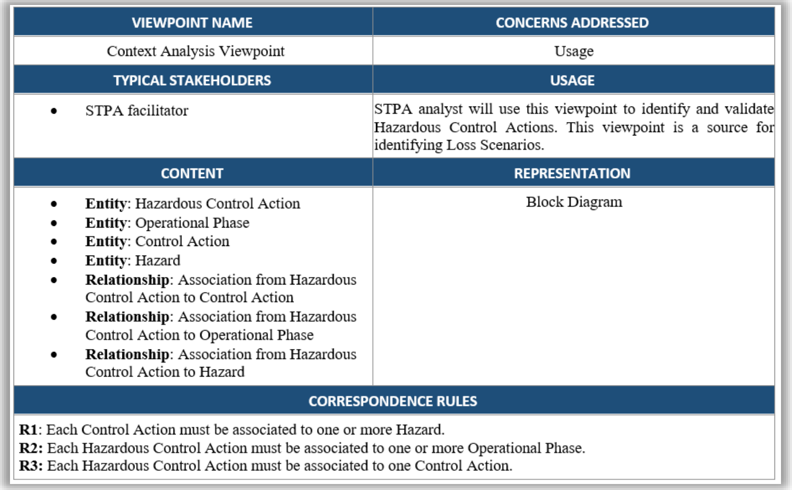
VIEWPOINT NAME	CONCERNS ADDRESSED
Control Structure viewpoint	Usage
TYPICAL STAKEHOLDERS	**USAGE**
- STPA facilitator	STPA analyst will use this viewpoint to identify the controllers, controlled process, the interactions between them (control actions and feedback) and the feedback lops. It may be used to validate the architecture decisions with the Design Team. This viewpoint is a source for the context analysis, losses scenarios and identification of hazardous control actions.
CONTENT	**REPRESENTATION**
- **Entity**: Control Entity - **Entity**: Control Action - **Entity**: Feedback - **Entity**: Information - **Relationship**: Association from Control Entity to Control Action - **Relationship**: Association from Control Entity and Feedback - **Relationship**: Association from Control Action to Information	Diagram
CORRESPONDENCE RULES	
R1: Each Control Action must be associated to one or more Control Entity. **R2:** Each Feedback must be associated to one or more Control Entity. **R3:** Each Information must be associated to one or more Control Entity.	

CONTROL STRUCTURE VIEWPOINT

VIEW

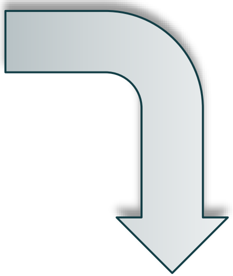


ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

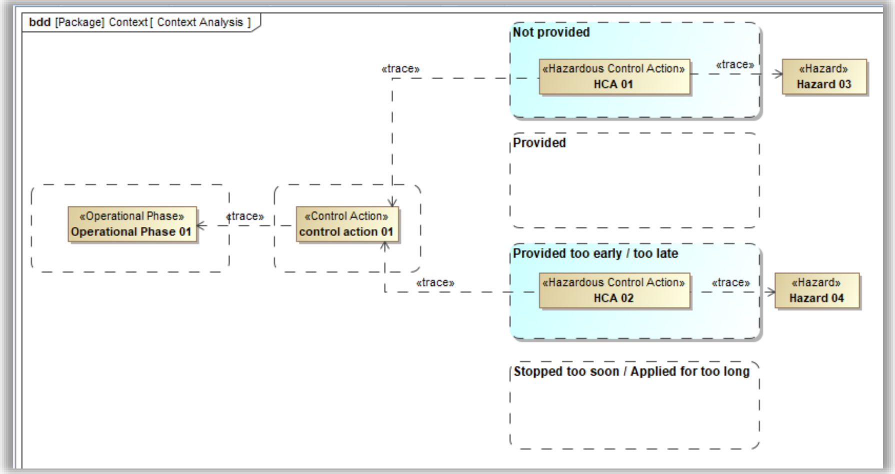


VIEWPOINT NAME	CONCERNS ADDRESSED
Context Analysis Viewpoint	Usage
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator	STPA analyst will use this viewpoint to identify and validate Hazardous Control Actions. This viewpoint is a source for identifying Loss Scenarios.
CONTENT	**REPRESENTATION**
• **Entity**: Hazardous Control Action • **Entity**: Operational Phase • **Entity**: Control Action • **Entity**: Hazard • **Relationship**: Association from Hazardous Control Action to Control Action • **Relationship**: Association from Hazardous Control Action to Operational Phase • **Relationship**: Association from Hazardous Control Action to Hazard	Block Diagram
CORRESPONDENCE RULES	
R1: Each Control Action must be associated to one or more Hazard. **R2:** Each Hazardous Control Action must be associated to one or more Operational Phase. **R3:** Each Hazardous Control Action must be associated to one Control Action.	

CONTEXT ANALYSIS VIEWPOINT



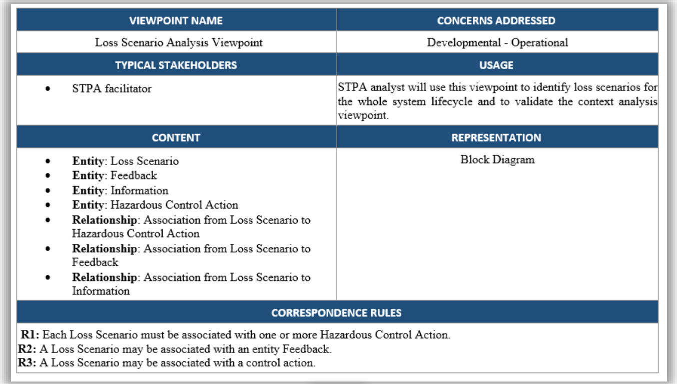
VIEW



RESULTS

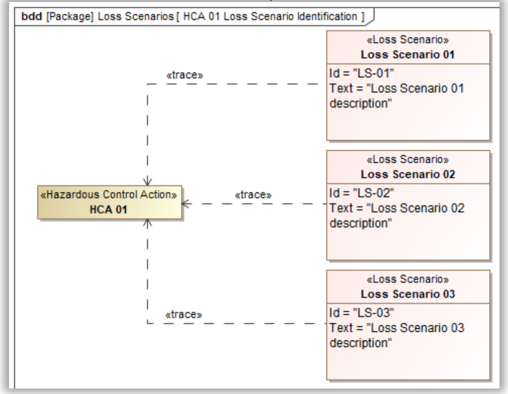
ARCHITECTURE VIEWPOINTS OF STPA ANALYSIS

LOSS SCENARIO ANALYSIS VIEWPOINT

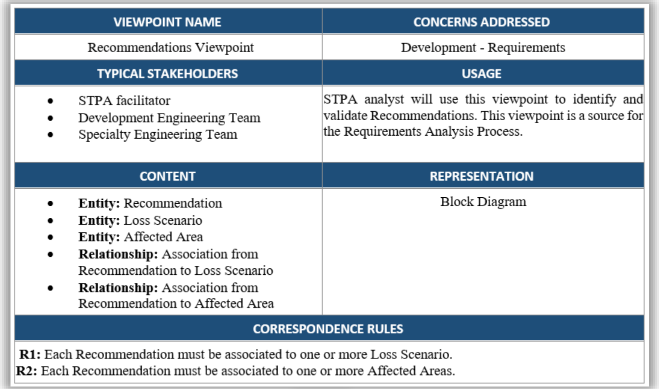


VIEWPOINT NAME	CONCERNS ADDRESSED
Loss Scenario Analysis Viewpoint	Developmental - Operational
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator	STPA analyst will use this viewpoint to identify loss scenarios for the whole system lifecycle and to validate the context analysis viewpoint.
CONTENT	**REPRESENTATION**
• **Entity**: Loss Scenario • **Entity**: Feedback • **Entity**: Information • **Entity**: Hazardous Control Action • **Relationship**: Association from Loss Scenario to Hazardous Control Action • **Relationship**: Association from Loss Scenario to Feedback • **Relationship**: Association from Loss Scenario to Information	Block Diagram
CORRESPONDENCE RULES	
R1: Each Loss Scenario must be associated with one or more Hazardous Control Action. **R2:** A Loss Scenario may be associated with an entity Feedback. **R3:** A Loss Scenario may be associated with a control action.	

VIEW

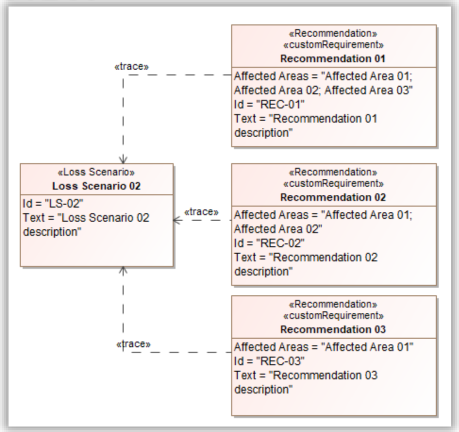

bdd [Package] Loss Scenarios [HCA 01 Loss Scenario Identification]
«Loss Scenario»
Loss Scenario 01
Id = "LS-01"
Text = "Loss Scenario 01 description"
«Loss Scenario»
Loss Scenario 02
Id = "LS-02"
Text = "Loss Scenario 02 description"
«Loss Scenario»
Loss Scenario 03
Id = "LS-03"
Text = "Loss Scenario 03 description"
«Hazardous Control Action»
HCA 01
«trace»
«trace»
«trace»

RECOMMENDATIONS VIEWPOINT



VIEWPOINT NAME	CONCERNS ADDRESSED
Recommendations Viewpoint	Development - Requirements
TYPICAL STAKEHOLDERS	**USAGE**
• STPA facilitator • Development Engineering Team • Specialty Engineering Team	STPA analyst will use this viewpoint to identify and validate Recommendations. This viewpoint is a source for the Requirements Analysis Process.
CONTENT	**REPRESENTATION**
• **Entity:** Recommendation • **Entity:** Loss Scenario • **Entity:** Affected Area • **Relationship:** Association from Recommendation to Loss Scenario • **Relationship:** Association from Recommendation to Affected Area	Block Diagram
CORRESPONDENCE RULES	
R1: Each Recommendation must be associated to one or more Loss Scenario. **R2:** Each Recommendation must be associated to one or more Affected Areas.	

VIEW


«Recommendation»
«customRequirement»
Recommendation 01
Affected Areas = "Affected Area 01; Affected Area 02; Affected Area 03"
Id = "REC-01"
Text = "Recommendation 01 description"
«Loss Scenario»
Loss Scenario 02
Id = "LS-02"
Text = "Loss Scenario 02 description"
«Recommendation»
«customRequirement»
Recommendation 02
Affected Areas = "Affected Area 01; Affected Area 02"
Id = "REC-02"
Text = "Recommendation 02 description"
«Recommendation»
«customRequirement»
Recommendation 03
Affected Areas = "Affected Area 01"
Id = "REC-03"
Text = "Recommendation 03 description"
«trace»
«trace»
«trace»

EMBRAER

Conclusion:

- Architecture views are a useful tool to manage complex developments
- Architecture views applied to STPA analysis is an effective way for integration of complex system development
- Architecture views integrated to an architecture framework to develop a complex product system

Architecture Viewpoints of STPA Analysis

Bruna Silva Queiroz
Chief Engineer Office
EMBRAER
São José dos Campos, Brazil
bruna.queiroz@embraer.com.br

Carina Carla Silva
Chief Engineer Office
EMBRAER
São José dos Campos, Brazil
carina.silva@embraer.com.br

Thiago Rodrigues da Costa
Chief Engineer Office
EMBRAER
São José dos Campos, Brazil
thiago.rodrigues@embraer.com.br

Architecture Viewpoints of STPA Analysis

[1] Leveson, Nancy G. Engineering a safer world: Systems thinking applied to safety. The MIT Press, 2016.

[2] Leveson, Nancy G., and John P. Thomas. "STPA handbook." Cambridge, MA, USA (2018).

[3] ISO, IEC. "IEEE: 42010: 2011 systems and software engineering, architecture description." International Standard (2011).

[4] NATO. “NATO Architecture Framework” v. 4. 2018.