IAMP Safety Critical Systems Working Papers

Towards a modeling language for Systems-Theoretic Process Analysis (STPA)

Proposal for a domain specific language (DSL) for model driven Systems-Theoretic Process Analysis (STPA) based on UML

Issue: 1
Date: 03.11.2016
Authors: Sven Stefan Krauss, Martin Rejzek, Monika Reif, Christian Hilbes

Authors
Sven Stefan Krauss svenstefan.krauss@zhaw.ch
Martin Rejzek martin.rejzek@zhaw.ch

Peer Review
Dr. Monika Reif monika.reif@zhaw.ch

Editor
Dr. Christian Hilbes christian.hilbes@zhaw.ch

Quality Assurance
Responsible for IAMP Safety Critical Systems open access publications
Sven Stefan Krauss svenstefan.krauss@zhaw.ch

Internal ID
259885

Table of Content

1 Introduction

Systems-Theoretic Process Analysis (STPA) is a modern safety analysis technique developed by Leveson [1] which is based on the accident model Systems-Theoretic Accident Model and Processes (STAMP) [2].

In order to minimize the gap typically existing between system development and safety analysis we integrate the STPA methodology directly with an UML/SysML environment, promoting the paradigm of safety-guided design [3]. UML (Unified Modeling Language) [4] and SysML (System Modeling Language) [5] are visual modeling languages used for model based software and systems engineering. For people who are not familiar with UML and SysML we recommend [6-8]. To understand the STAMP/STPA modeling concepts reading of [3], [9], and [10] is recommended.

We developed an extension called SAHRA (STPA based Hazard and Risk Analysis) [11] for Sparx Systems Enterprise Architect (EA) [12] (Figure 1). EA is a popular commercial UML/SysML modeling tool which can be used for requirements engineering, system and software design. The corporate edition of EA provides multi user support with security permission system, scripting and automation API, SQL searches, configuration management integration, report generation and modeling functionality.

SAHRA includes a domain specific language (DSL) profile for STPA based on EA's MDG technology [13] to provide additional diagram types, toolboxes, UML profiles, patterns and templates for STPA modeling, further called MDG Profile for STPA. The SAHRA extension provides a context sensitive object browser for comfortable editing and special editors for performing STPA Step 1 and Step 2.

This document formalizes the concepts of safety-guided design with STPA mentioned in [3] by providing an overview of the diagrams, elements and connectors that are defined in the MDG Profile for STPA. While the implementation of the MDG profile itself is specific to EA, the concepts and the approach to extend UML with a specific profile for STPA is generic. The purpose of this document is therefore twofold:

1. This document seeks to provide a comprehensive definition towards a domain specific modeling language for System-Theoretic Process Analysis (STPA), including the definition of terms, elements and graphical representation;
2. It aims to document best practices with STPA and software tool SAHRA.

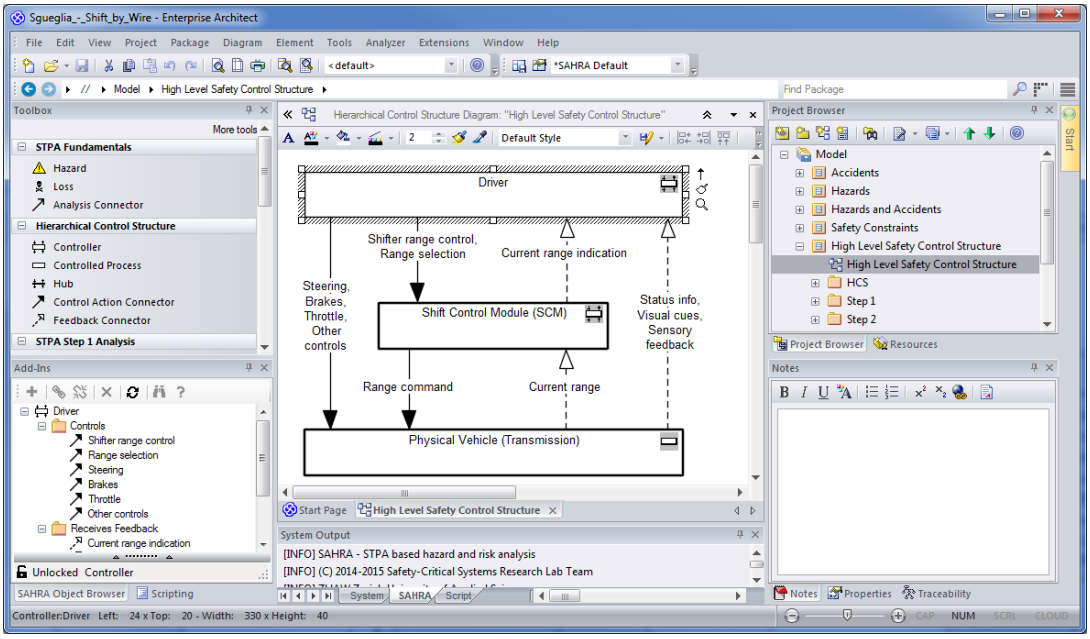


Figure 1: SAHRA – STPA based Hazard and Risk Analysis: an extension for Sparx Systems Enterprise Architect[1] to integrate STPA with a UML/SysML modeling environment. The example diagram shown is adapted from [14].

[1] Sparx Systems, Enterprise Architect, MDG Integration, and MDG Technology are trademarks or registered trademarks of Sparx Systems Pty Ltd., Creswick, Australia.

2 MDG Profile for STPA

2.1 Overview

The MDG Profile for STPA tailors UML to STPA with new diagram types, new element types and new connector types. A model (in this context) is a set of diagrams with elements which are connected by connectors. Connectors define a relationship between two elements. A connector has a source element and a target element. The visual style of a connector defines its meaning which can be altered by applying stereotypes.

To provide the possibility to extend the MDG Profile for STPA, extensions can be used. We included in this document the extensions which were usefull in our case studies. To document the items which are available in the MDG Profile for STPA, a table according to table 1 is used in this document.

Figure 2 provides an overview of all diagrams, connectors, elements and extensions which are available in the MDG Profile for STPA, which are further documented in this document.

Table 1: Item's documentation scheme used in this document.

Property	Description
Metatype	Name of the item
Purpose	Purpose of item
Extends	UML item on which the new item is based on
Stereotype	Stereotype of the item
Alternative Name(s)	Alternative names which can be found in STAMP/STPA related documents and presentations
Visual Representation	Graphical example of the new item

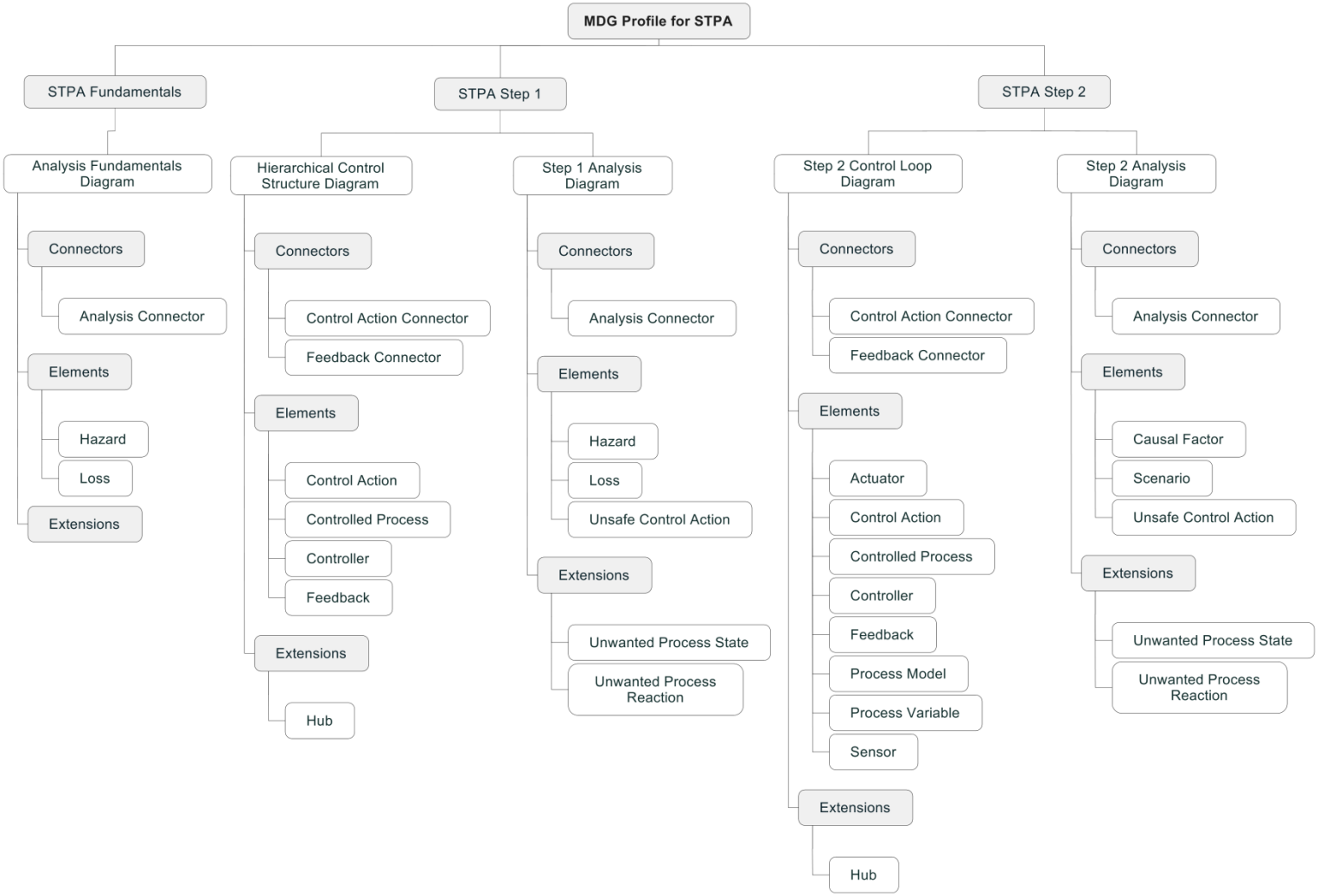


Figure 2: MDG Profile for STPA - Overview of available Diagrams, Connectors, Elements and Extensions.

2.2 Analysis Fundamentals Diagram

2.2.1 Purpose

The Analysis Fundamentals Diagram is used to define analysis fundamentals like losses (accidents), hazards and their relationships (Figure 3). Valid links for Analysis Connector and related elements are defined in chapter 2.7.1.

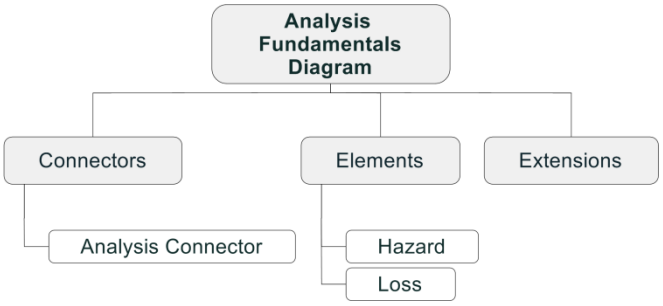


Figure 3: STPA Analysis Fundamentals Diagram Overview.

2.2.2 Example Diagram

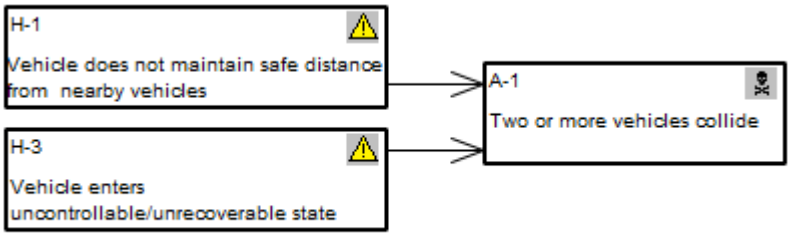


Figure 4: Example Analysis Fundamentals Diagram (adapted from [14] based on [3]).

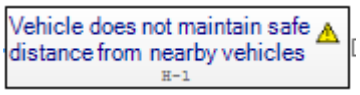
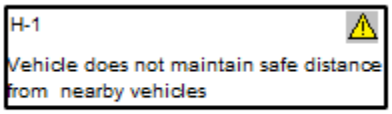
2.2.3 Connectors

2.2.3.1 Analysis Connector

Property	Description
Metatype	Analysis Connector
Purpose	Defines the relationship between two analysis elements. The direction of the connector defines the relationship, normally a potential path from cause to consequence.
Extends	UML::Association
Stereotype	STPA_AnalysisConnector
Alternative Name(s)	n/a
Allowed Connections	See 2.7.1
Visual Representation	

2.2.4 Elements

2.2.4.1 Hazard

Property	Description
Metatype	Hazard
Purpose	Represents “System state / set of conditions that together with particular set of worst-case environmental conditions will lead to accident” [1, p. 183]
Extends	UML::Class
Stereotype	STPA_Hazard
Alternative Name(s)	System Level Hazard
Visual Representation	SAHRA Analysis View  Other diagrams 

2.2.4.2 Loss

Property	Description
Metatype	Loss
Purpose	Represents “an unplanned / undesired loss event” [1, p. 181]
Extends	UML::Class
Stereotype	STPA_Loss
Alternative Name(s)	System Level Loss, System Level Accident
Visual Representation	SAHRA Analysis View 
	Other diagrams 

2.3 Hierarchical Control Structure Diagram

2.3.1 Purpose

The Hierarchical Control Structure Diagram is used to create a functional, hierarchical model of the system under consideration with Controllers, Controlled Processes, Control Actions and Feedback (Figure 5) as a foundation for the consequent analysis steps (Step 1 and Step 2) of STPA.

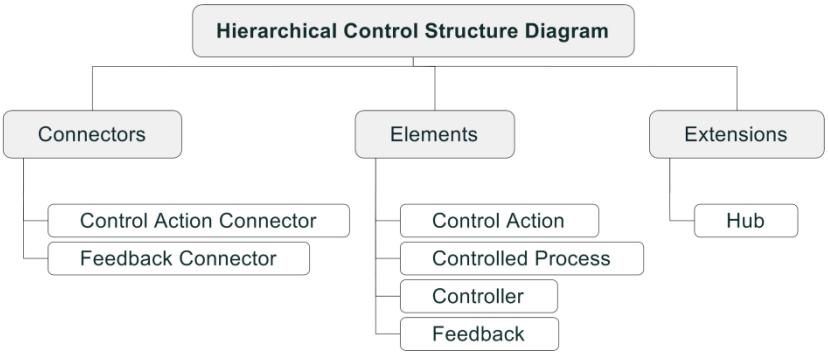


Figure 5: Hierarchical Control Structure Diagram Overview.

2.3.2 Example Diagram

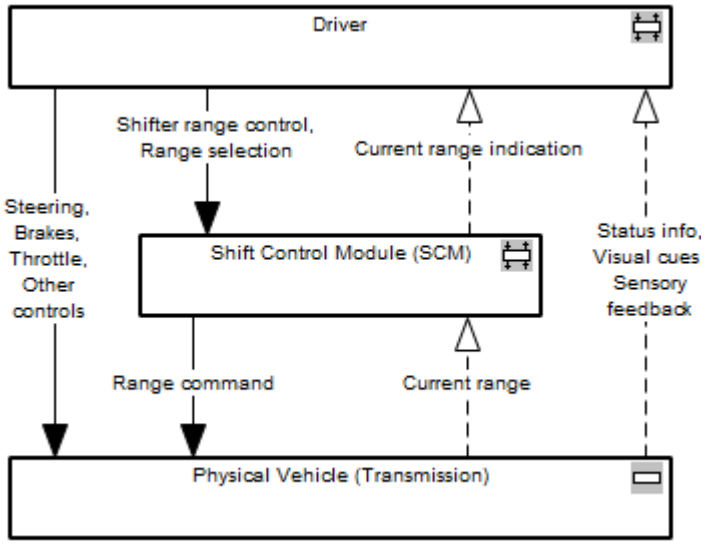


Figure 6: Example Hierarchical Control Structure (adapted from [14, p. 103]).

2.3.3 Connectors

2.3.3.1 Control Action Connector

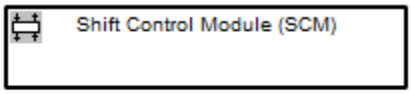
Property	Description
Metatype	Control Action Connector
Purpose	Provides a route for Control Actions. A Control Action Connector can host a number of Control Actions as conveyed items.
Extends	UML::InformationFlow
Stereotype	STPA_ControlActionConnector
Alternative Name(s)	n/a
Valid connections	See 2.7.2
Visual Representation	

2.3.3.2 Feedback Connector

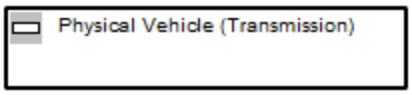
Property	Description
Metatype	Feedback Connector
Purpose	Provides a route for Feedback. A Feedback Connector can host a number of Feedback items as conveyed items.
Extends	UML::InformationFlow
Stereotype	STPA_FeedbackConnector
Alternative Name(s)	n/a
Valid connections	See 2.7.3
Visual Representation	

2.3.4 Elements

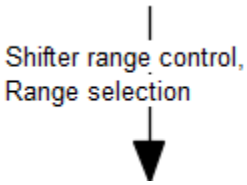
2.3.4.1 Controller

Property	Description
Metatype	Controller
Purpose	A controller affects the state of the system by providing control actions based on process model and feedback. A controller can be an automated controller or a human controller. A controller can provide and receive control actions and provide and receive feedback.
Extends	UML::Class
Stereotype	STPA_Controller
Alternative Name(s)	n/a
Visual Representation	

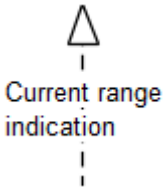
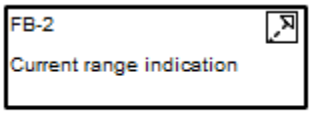
2.3.4.2 Controlled Process

Property	Description
Metatype	Controlled Process
Purpose	Represent the controlled process of the system under consideration. A controlled process can receive control actions and provide feedback.
Extends	UML::Class
Stereotype	STPA_ControlledProcess
Alternative Name(s)	Dynamic System State
Visual Representation	

2.3.4.3 Control Action

Property	Description
Metatype	Control Action
Purpose	Represents a control action to change the state of the system.
Extends	UML::Class
Stereotype	STPA_ControlAction
Alternative Name(s)	Control Action
Remarks	Control Actions can only be linked with a Control Action Connector. When multiple Control Actions are linked with the same Control Action Connector they are shown separated by commas. In EA, Control Actions shown on the connector are realized as conveyed items on an information flow connector.
Visual Representation	Hierarchical Control Structure Diagram and Step 2 Control Loop Diagram 
	other diagrams 

2.3.4.4 Feedback

Property	Description
Metatype	Feedback
Purpose	Represents a system information.
Extends	UML::Class
Stereotype	STPA_Feedback
Alternative Name(s)	Feedback, Control Feedback
Remarks	Feedback can only be linked with a Feedback Connector. When multiple Feedback items are linked with the same Feedback Connector they are shown separated by commas. In EA, Feedback elements shown on connectors are realized as conveyed items on an information flow connector.
Visual Representation	Hierarchical Control Structure Diagram and Step 2 Control Loop Diagram 
	other diagrams 

2.3.5 Extensions

2.3.5.1 Hub

Property	Description
Metatype	Hub
Purpose	The hub element is an auxiliary element to route Control Actions and Feedback. It can be used: • to split Control Action Connectors into a number of Control Action Connectors, • to split Feedback Connectors into a number of Feedback Connectors, • to join Control Action Connectors, • to join Feedback Connectors, • to maintain the consistency of Control Actions and Feedback between different diagram representations of one HCS
Extends	UML::Fork/Join
Stereotype	STPA_Hub
Alternative Name(s)	Bus, Node
Visual Representation	[redacted]

2.4 Step 1 Analysis Diagram

2.4.1 Purpose

The Step 1 Analysis Diagram defines links between Control Action, Keyword, Unsafe Control Action and effects like Unwanted Process State, Unwanted Process Reaction, Hazards and Losses (Figure 7) [3].

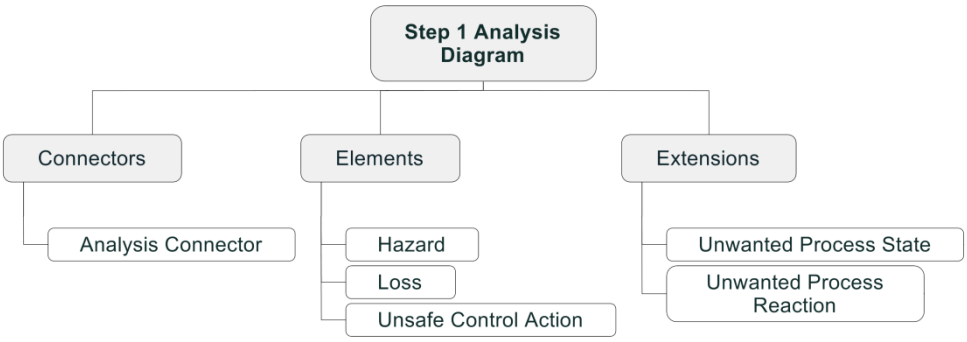


Figure 7: Step 1 Analysis Diagram Overview.

2.4.2 Example Diagram

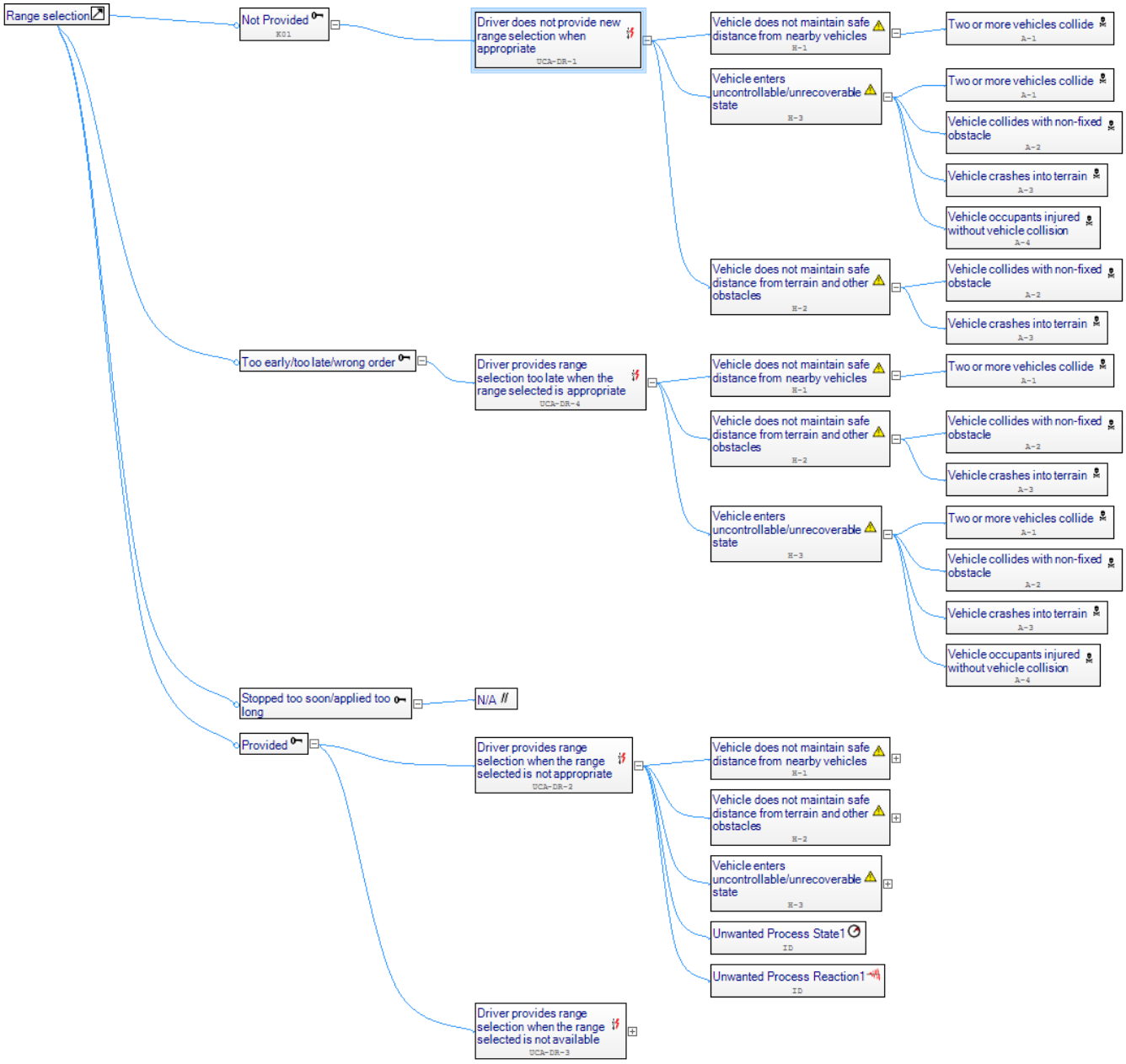


Figure 8: Example Step 1 Analysis Diagram (adapted from [14] based on [3]) as shown in SAHRA's Analysis View.

2.4.3 Connectors

The diagram uses the Analysis Connector as defined in chapter 2.2.3.

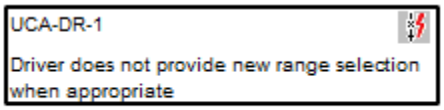
2.4.4 Elements

The diagram uses also Hazard and Loss elements as defined in chapter 2.2.4.

2.4.4.1 Keyword

Property	Description
Metatype	Keyword
Purpose	Provides guidance to find Unsafe Control Actions
Extends	UML::Class
Stereotype	STPA_Keyword
Alternative Name(s)	n/a
Visual Representation	SAHRA Analysis View 
	Other diagrams 

2.4.4.2 Unsafe Control Action

Property	Description
Metatype	Unsafe Control Action
Purpose	Represents a (potential) Unsafe Control Action, which typically leads to Unsafe Process State, Unsafe Process Reaction or Hazard.
Extends	UML::Class
Stereotype	STPA_UnsafeControlAction
Alternative Name(s)	n/a
Visual Representation	SAHRA Analysis View 
	Other diagrams 

2.4.5 Extensions

2.4.5.1 Unwanted Process State

Property	Description
Metatype	Unwanted Process State
Purpose	Represents an unwanted (undesired) process or system state which might lead to an Unsafe Process Reaction or Hazard.
Extends	UML::Class
Stereotype	STPA_UnwantedProcessState
Alternative Name(s)	Undesired System State
Visual Representation	SAHRA Analysis View 
	Other diagrams 

2.4.5.2 Unwanted Process Reaction

Property	Description
Metatype	Unwanted Process Reaction
Purpose	Represents an unwanted (undesired) process reaction or undesired system reaction which might lead to Hazard.
Extends	UML::Class
Stereotype	STPA_UnwantedProcessReaction
Alternative Name(s)	Undesired System Reaction
Visual Representation	SAHRA Analysis View 
	

2.5 Step 2 Control Loop Diagram

2.5.1 Purpose

The Step 2 control loop represents that part of the Hierarchical Control Structure which is of relevance for a specific control action and extends the HCS with Actuators and Sensors. The Step 2 Control Loop Diagram is a foundation for the STPA Step 2 analysis (Figure 9). Optionally the diagram may show the controller's process model and its process variables (Figure 10).

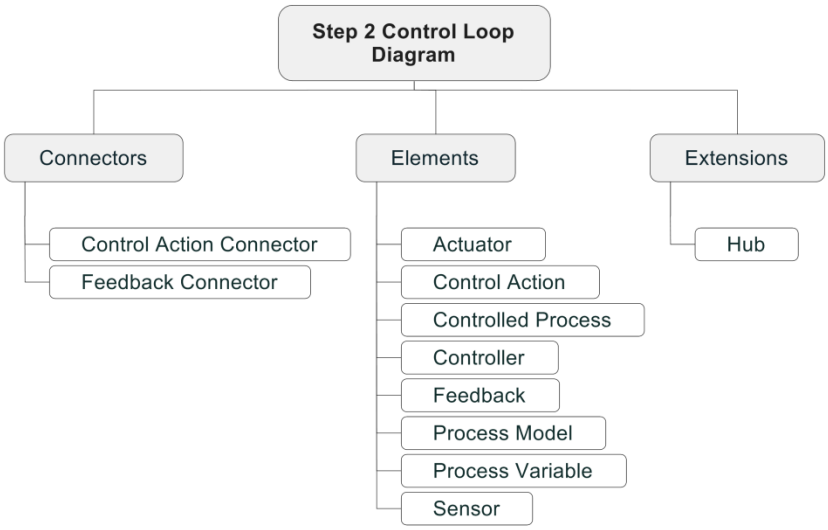


Figure 9: Step 2 Control Loop Diagram Overview.

2.5.2 Example Diagram

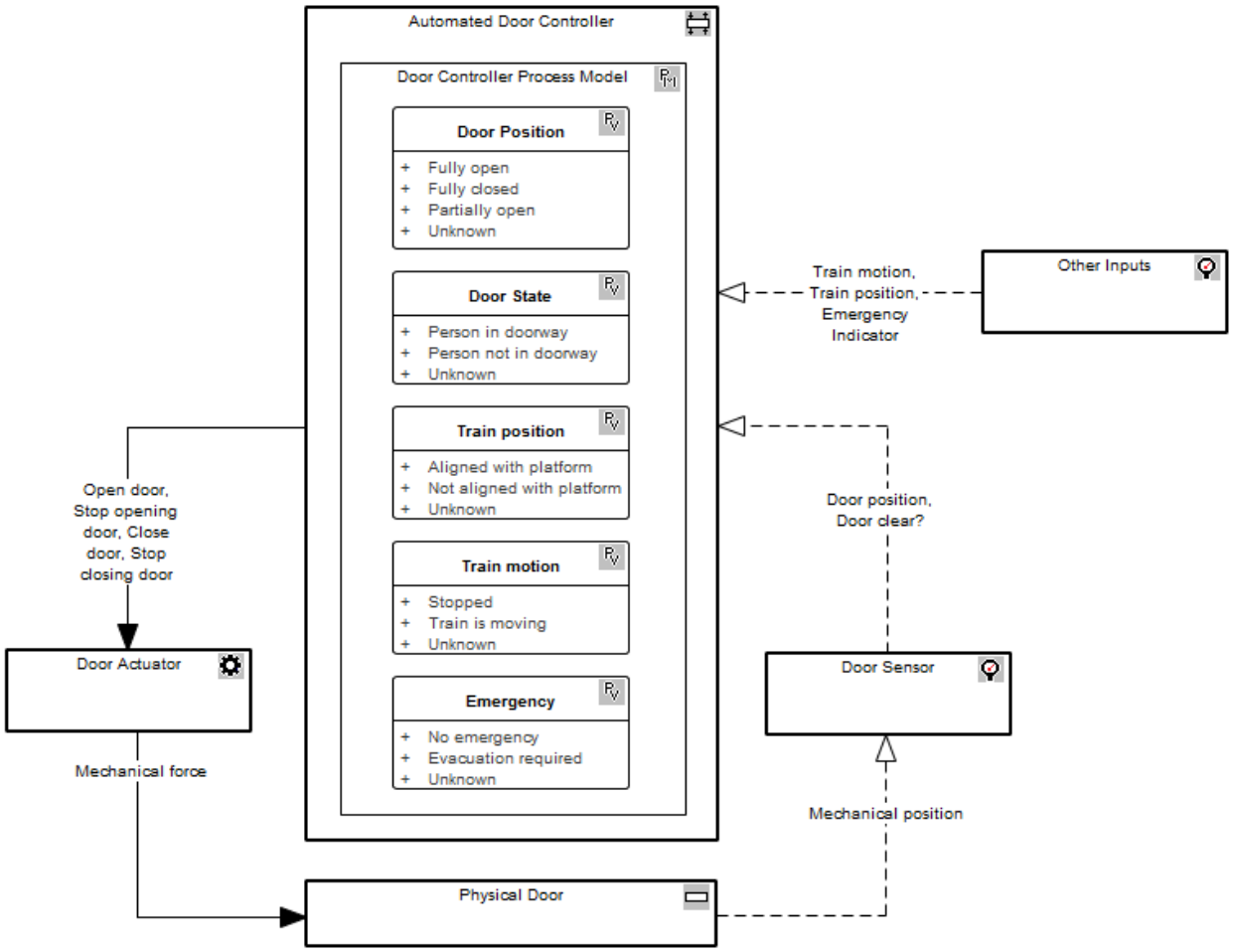


Figure 10: Example Step 2 Control Loop Diagram (adapted from [15, p. 82]).

2.5.3 Connectors

The diagram uses the Control Action Connector and Feedback Connector as defined in chapter 2.2.3.

2.5.4 Elements

The Step 2 Control Loop Diagram uses also the elements of the Hierarchical Control Structure diagram (Controller, Controlled Process, Control Action, Feedback, Hub) as defined in chapter 2.3.4.

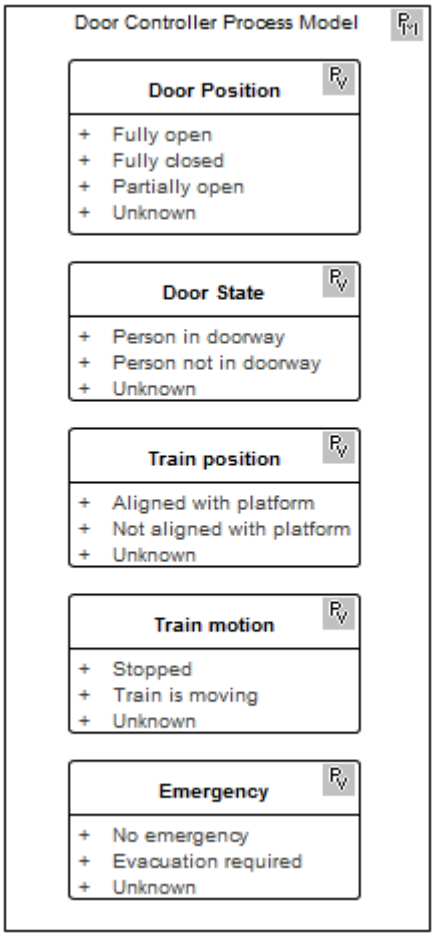
2.5.4.1 Actuator

Property	Description
Metatype	Actuator
Purpose	Represents an actuator
Extends	UML::Class
Stereotype	STPA_Actuator
Alternative Name(s)	n/a
Visual Representation	

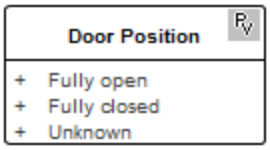
2.5.4.2 Sensor

Property	Description
Metatype	Sensor
Purpose	Represents a sensor
Extends	UML::Class
Stereotype	STPA_Sensor
Alternative Name(s)	n/a
Visual Representation	

2.5.4.3 Process Model

Property	Description
Metatype	Process Model
Purpose	Represents process model of a Controller. A Process Model can contain a number of Process Variables.
Extends	UML::Class
Stereotype	STPA_ProcessModel
Alternative Name(s)	n/a
Visual Representation	

2.5.4.4 Process Variable

Property	Description
Metatype	Process Variable
Purpose	Represents a process variable of a process model
Extends	UML::Class
Stereotype	STPA_ProcessVariable
Alternative Name(s)	System State Variable
Visual Representation	

2.6 Step 2 Analysis Diagram

2.6.1 Purpose

The Step 2 Analysis Diagram defines links between Unsafe Control Actions, Scenarios and Causal Factors (Figure 11) [3].

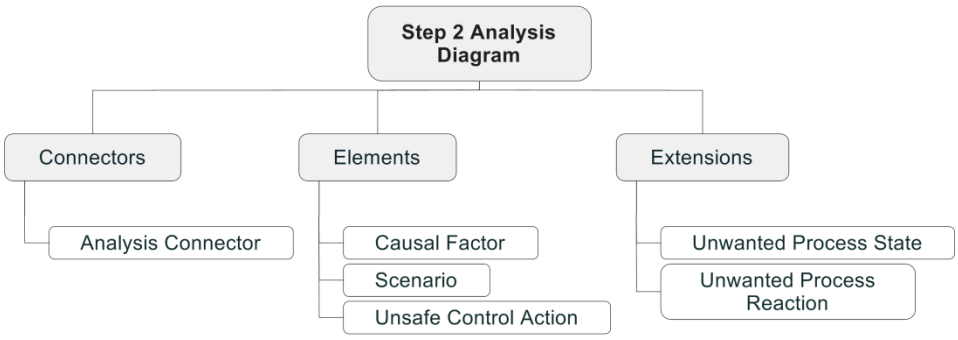


Figure 11: Step 2 Analysis Diagram Overview.

2.6.2 Example Diagram

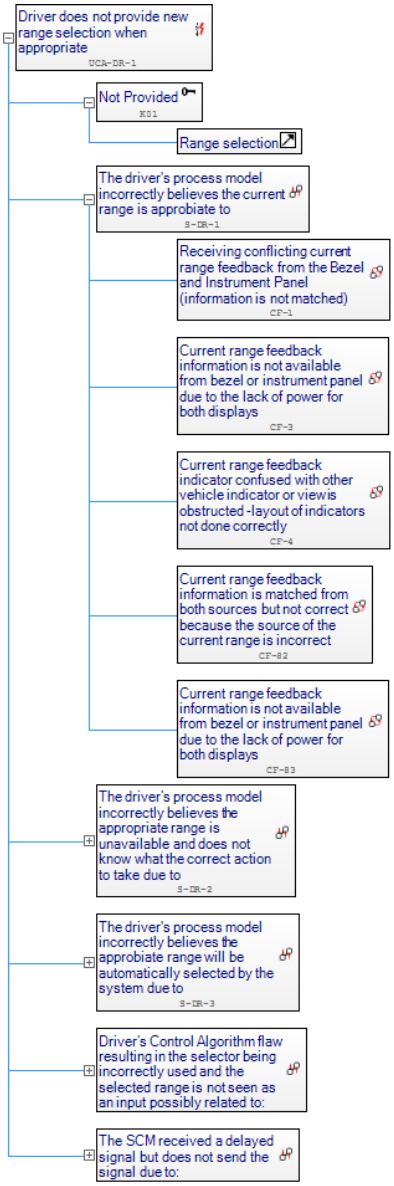


Figure 12: Example for Step 2 Analysis Diagram (adapted from [14] based on [3]) as shown in SAHRA's analysis editor.

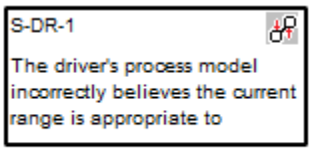
2.6.3 Connectors

The diagram uses the Analysis Connector as defined in chapter 2.2.3.1.

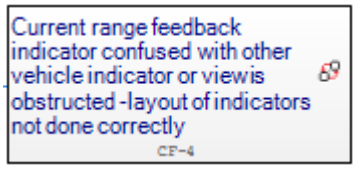
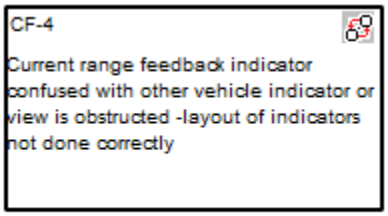
2.6.4 Elements

The Step 2 Analysis Diagram uses also the elements of the Step 1 Analysis Diagram as defined in chapter 2.4.4.

2.6.4.1 Scenario

Property	Description
Metatype	Scenario
Purpose	Represents a scenario to group Causal Factor
Extends	UML::Class
Stereotype	STPA_Scenario
Alternative Name(s)	Accident Scenario
Visual Representation	SAHRA Analysis Editor  Other diagrams 

2.6.4.2 Causal Factor

Property	Description
Metatype	Causal Factor
Purpose	Represents a causal factor
Extends	UML::Class
Stereotype	STPA_Scenario
Alternative Name(s)	Causal Flaws, Control Flaws
Visual Representation	SAHRA Analysis Editor 
	Other diagrams 

2.7 Rule Sets

2.7.1 Analysis Connector Rule Set

Valid connections for Analysis Connector										
		Target								
		Causal Factor	Scenario	Keyword	Control Action	Unsafe Control Action	Unwanted Process State	Unwanted Process Reaction	Hazard	Loss
Source	Causal Factor	✗	✓	✓	✗	✗	✗	✗	✗	✗
	Scenario	✗	✓	✗	✗	✓	✓	✓	✗	✗
	Keyword	✗	✗	✗	✓	✗	✗	✗	✗	✗
	Control Action	✗	✗	✗	✗	✓	✗	✗	✗	✗
	Unsafe Control Action	✗	✗	✗	✗	✗	✓	✓	✓	✗
	Unwanted Process State	✗	✗	✗	✗	✗	✓	✓	✓	✗
	Unwanted Process Reaction	✗	✗	✗	✗	✗	✗	✓	✓	✗
	Hazard	✗	✗	✗	✗	✗	✗	✗	✓	✓
	Loss	✗	✗	✗	✗	✗	✗	✗	✗	✓

2.7.2 Control Action Connector Rule Set

Valid connections for Control Action Connector						
		Target				
		Controller	Controlled Process	Hub	Actuator	Sensor
Source	Controller	✓	✓	✓	✓	✗
	Controlled Process	✗	✗	✗	✗	✗
	Hub	✓	✓	✓	✓	✓
	Actuator	✗	✓	✗	✓	✗
	Sensor	✗	✗	✗	✗	✓

2.7.3 Feedback Connector Rule Set

Valid connections for Feedback Connector						
		Target				
		Controller	Controlled Process	Hub	Actuator	Sensor
Source	Controller	✓	✗	✓	✗	✗
	Controlled Process	✓	✗	✓	✗	✓
	Hub	✓	✓	✓	✗	✓
	Actuator	✗	✗	✗	✗	✗
	Sensor	✓	✓	✓	✗	✓

3 Using MDG Profile for STPA

3.1 Installation

The MDG profile for STPA is automatically installed when the SAHRA [11] extension is installed. For more information, please refer to the SAHRA documentation.

To check if the profile is loaded navigate to `Extensions` | `MDG Technologies…` . The MDG Technologies dialog should have an entry `STPA` (Figure 13).

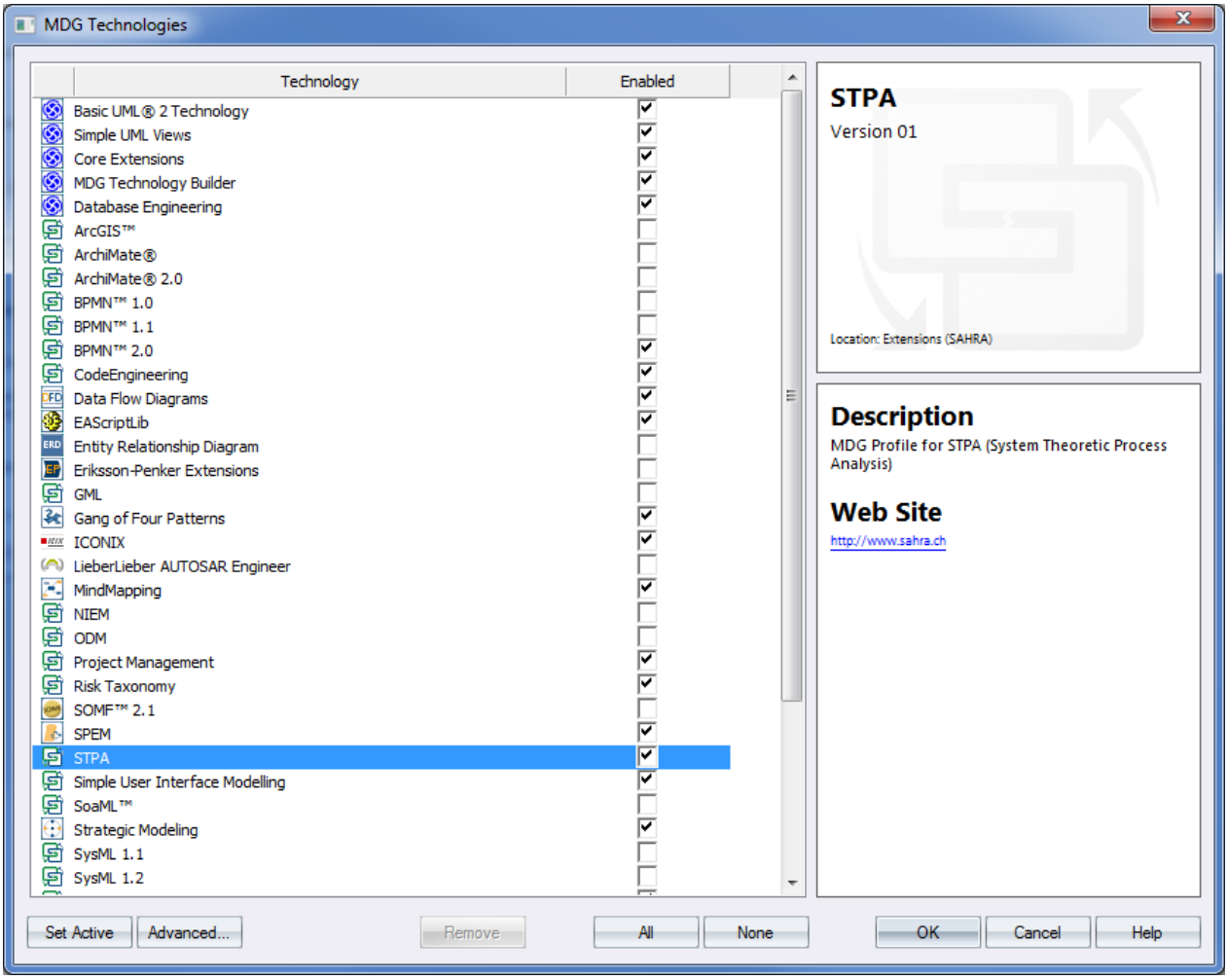


Figure 13: MDG Technologies Dialog.

3.2 Diagrams

The MDG Profile for STPA provides four new diagram types:

- STPA Analysis Fundamentals
- STPA Hierarchical Control Structure
- STPA Step 1 Analysis*)
- STPA Step 2 Analysis*)

*) These diagrams are only required when the MDG Profile for STPA is used without the SAHRA extension. The diagrams are not needed by the SAHRA extension editors for Step 1 and Step 2.

To create a new STPA diagram, select `STPA` in the New Diagram dialog and select `STPA` under `Select From:` and the diagram type for the new diagram under `Diagram Types:`

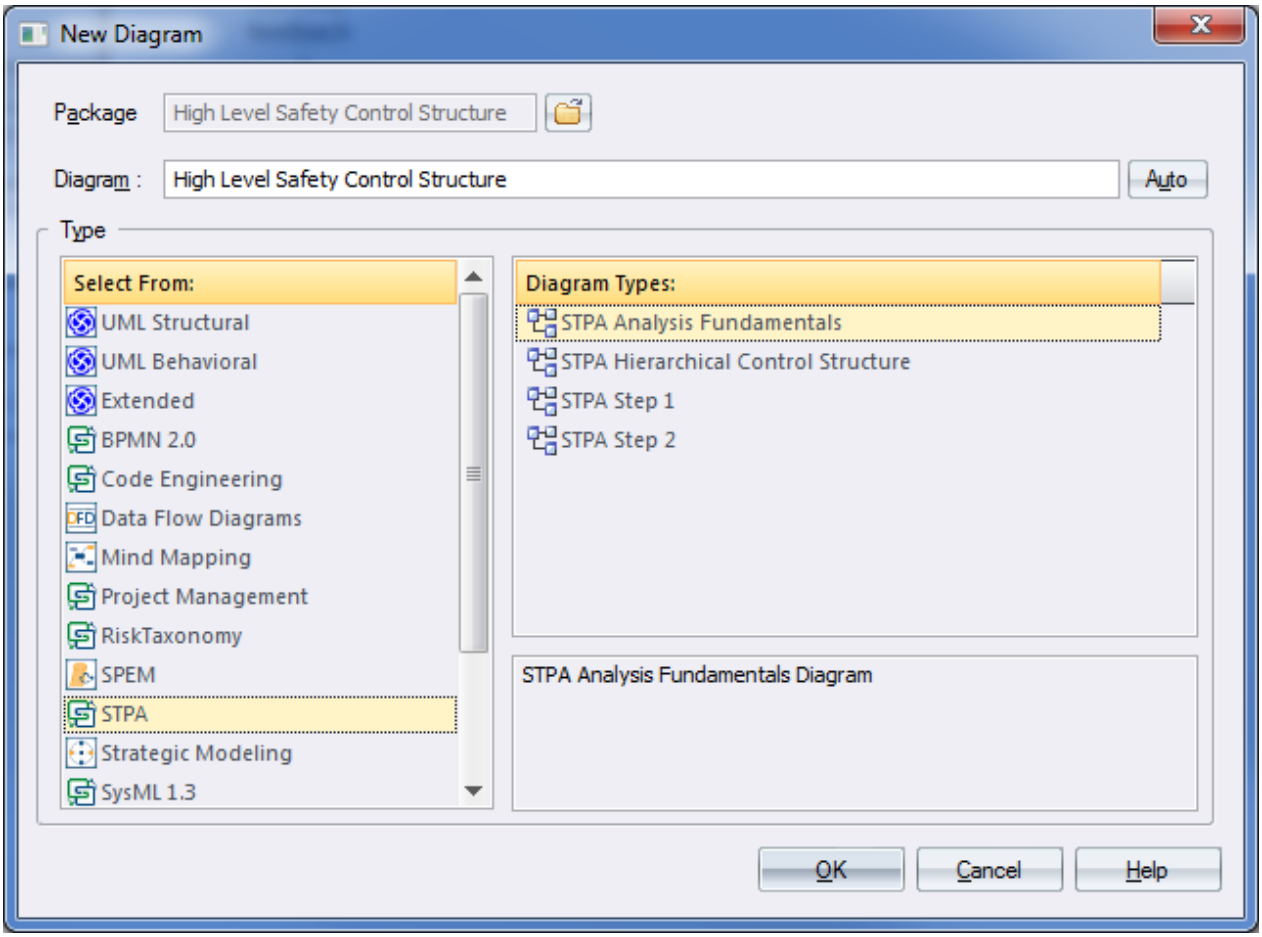


Figure 14: New Diagram Dialog.

3.3 Toolbox

When a STPA diagram is created, the STPA toolbox is shown (Figure 15). In case it is not shown, please click on `More tools…` and select `STPA` from the list.

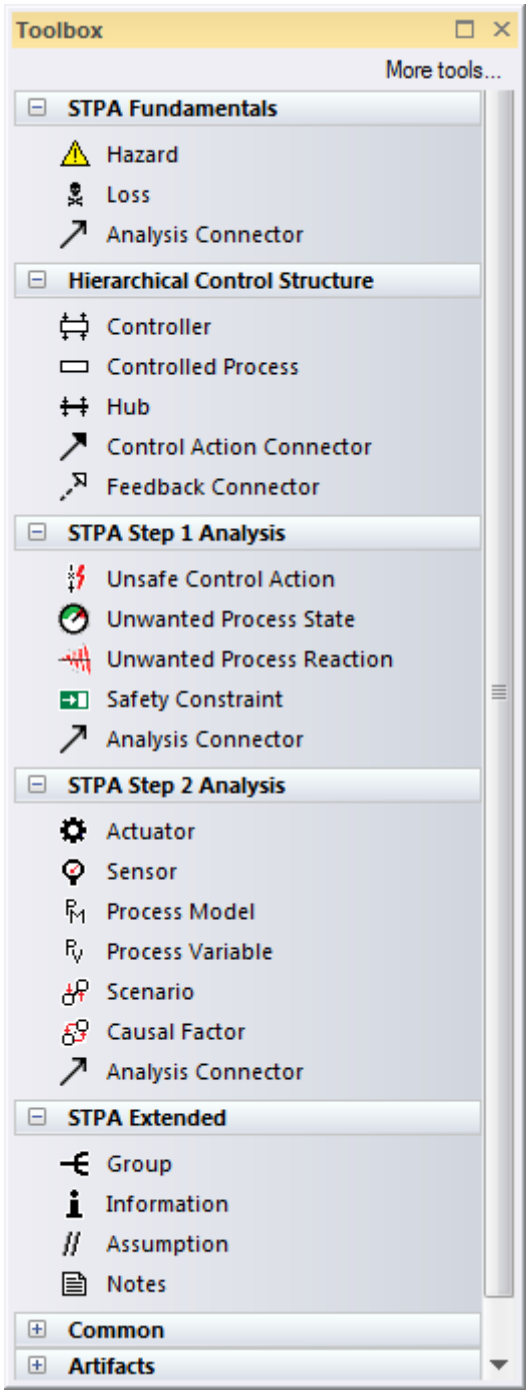


Figure 15: STPA Toolbox.

3.4 Properties Dialog

All elements in the MDG Profile for STPA have these standard properties[2] which can be edited with the properties dialog:

- Name – name of the element;
- Notes – long description of the element;
- Stereotype – Type of the element.

The properties dialog can be opened with a double click on an element or with `Properties…` from a context menu. The user can enter name, notes as a long description and can edit other properties (Figure 16).

All elements in the MDG Profile for STPA have additional properties (realized as tagged values):

- ID – user defined text to identify the element;
- Context – user defined text to document the context of the element, for example diagram detail level;
- ParentID – user defined text to specify the parent element ID.

To show special tagged values for the element, tab `STPA` must be selected on the right hand side (Figure 17).

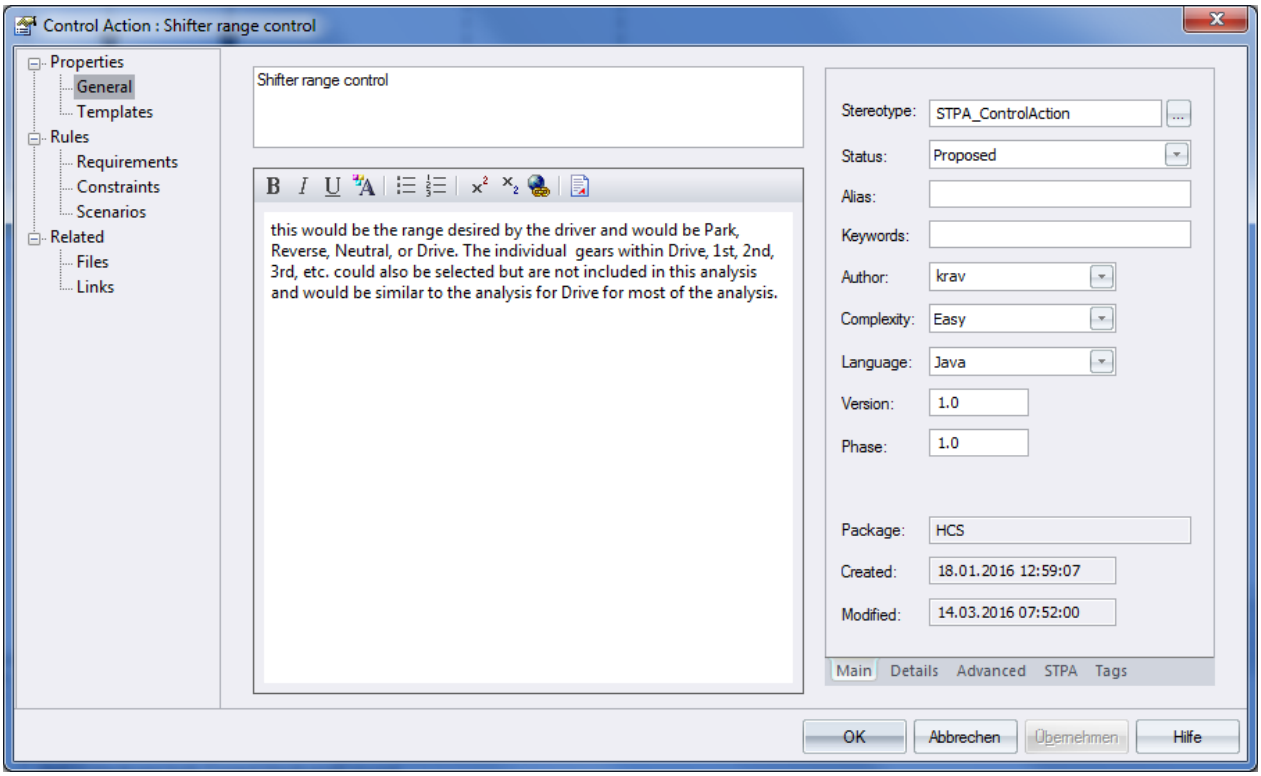


Figure 16: Properties dialog for a Control Action showing general properties like Name, Notes, Stereotype and other metadata.

[2] There are more properties available, but are not further used in this document.

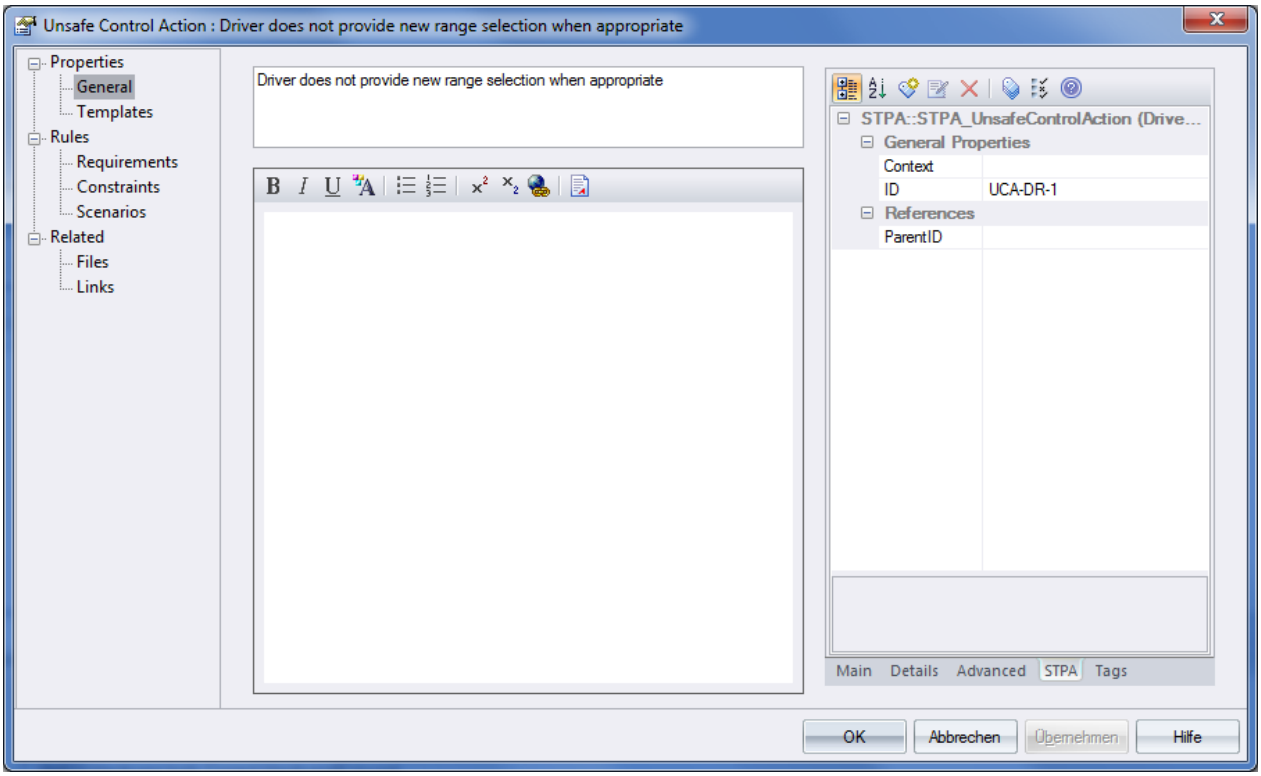


Figure 17: Properties dialog for an Unsafe Control Action. Notes field is empty. Tab STPA is selected to show special tagged values for STPA.

4 Appendix

4.1 References

1. Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety*. 2012, Cambridge MA, USA: MIT Press.
2. Leveson, N.G., *A new accident model for engineering safer systems.* Safety Science, 2004. **42**(4): p. 237-270.
3. Rejzek, M., C. Hilbes, and S.S. Krauss, *Safety Driven Design with UML and STPA*, in *STAMP Workshop 2015*. 2015: MIT, Boston.
4. Object Management Group, *OMG Unified Modeling Language (OMG UML™) Version 2.5. OMG Document Number: formal/15-03-01.* 2015.
5. Object Management Group, *OMG Systems Modeling Language (OMG SysML™) Version 1.4. OMG Document Number: formal/2015-06–03*. 2015.
6. Seidl, M., et al., *UML@classroom: An introduction to object-oriented modeling*. 2015: Springer International Publishing.
7. Weilkiens, T., *Systems engineering with SysML/UML: modeling, analysis, design*. 2011: Morgan Kaufmann.
8. Holt, J. and S. Perry, *SysML for Systems Engineering: A Model-Based Approach*. 2013: Institution of Engineering and Technology.
9. Wieringa, R., *Design methods for reactive systems : Yourdon, Statemate and the UML*. 2003: San Francisco : Morgan Kaufmann.
10. Antoine, B., *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry*. 2013, Massachusetts Institute of Technology.
11. Krauss, S.S., et al., *SAHRA - An integrated software tool for STPA: Poster*, in *4th European STAMP Workshop (September, 13-15)*. 2016, Zurich University of Applied Sciences (ZHAW): Zurich, Switzerland.
12. Sparx Systems Pty Ltd. *Enterprise Architect - UML Modeling and Lifecycle Tool Suite*. 2015 [cited 2015 01.08.2015]; Available from: http://www.sparxsystems.com/.
13. Sparx Systems Pty Ltd. *Model Driven Generation (MDG) Technologies*. 2015 27.07.2015]; Available from: http://www.sparxsystems.com.au/resources/mdg_tech/.
14. Sgueglia, J., *Managing Design Changes using Safety-Guided Design for a Safety-Critical Automotive System. MIT Master's Thesis, June 2015*. 2015: MIT, Boston.
15. Thomas, J., *Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis*, in *PhD Thesis, Engineering Systems Division*. 2013: MIT, Boston.