Hot PASTA

Jette Petzold, Reinhard von Hanxleden
Department of Computer Science, Kiel University
jep@informatik.uni-kiel.de

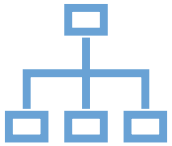
SafeComp, Sep 11th, 2025

Hazard analysis

System-Theoretic Process Analysis (STPA)

Define purpose of the analysis:

Losses • Hazards • System constraints



Model the control structure:

Responsibilities • Control structure

Identify Unsafe Control Actions (UCAs):

UCAs • Controller constraints

Identify loss scenarios:

Scenarios

Losses

First Set

L1. ROLFER was unable to execute a SAR mission (Loss of system goal)

L2. Inadequate interactions with the public during the preparation mode (Loss of public trust)

Second Set

L3: A SP dies/injured due to drowning (Loss of mission goal)

L4: People die or get injured due to a direct hit by the UAV (Loss of public trust)

L5: Loss of system equipment, i.e., UAV, SW and Ground Station. (Property loss)

Hazards

First Set

H1: ROLFER was not properly prepared for its mission → L1, L2

H2: A SP is not served adequately during the phase of preparation and handling of a SW → L2

Second Set

H3: The UAV does not approach the distressed human → L3, L5

H4: The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5

H5: The UAV approaches the SP but does not provide rescue assistance to him/her → L3

	Hazard	**SAFETY DESIGN CONSTRAINT**
1	ROLFER was not properly prepared for its mission	ROLFER must be properly prepared for its mission.
2	A SP is not served adequately during the phase of preparation and handling of a SW → L2	Every SP must be adequately served during the phase of preparation and handling of a SW
3	The UAV does not approach the distressed human → L3, L5	The UAV must approach the distressed human
4	The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5	The UAV must not violate the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level
5	The UAV approaches the SP but does not provide rescue assistance to him/her → L3	The UAV must approach the SP and must provide rescue assistance to them

UCA

Control action	Provided	not provided	Wrong timing/ order	Stopped too soon/applied too long
Give SW to user	**UCA 1**: Admin gave the SW to user, without some form of safety deposit**[H2]** **UCA 2**: Admin gave the SW to user without properly explaining the correct way of operating it. **[H2, H3]**	**UCA 3**: Admin did not give the SW to a user, even though there were available SWs. **[H2, H3]** **UCA 4**: Ο admin δεν παρείχε τα SW στους χρήστες τηρώντας προτεραιότητα προς τις ευπαθείς ομάδες. **[H2, H3]**	**UCA 5:** Admin gave the SW to the user before making sure that the UAV is ready for its mission (e.g., the battery is full, the life ring is mounted, the engine motors are working). **[H1, H3, H4, H5]** **UCA 6:** admin gave the SW to a user before checking that the SW is ready for use (e.g., it's operating correctly, the SIM card is installed) **[H1, H3]** **UCA 7:** admin gave the SW to the user before setting up the approved numbers. **[H1, H3]** **UCA 8:** Admin gave the SW to the user before setting up the supervised area borders**. [H1, H3]** **UCA 9:** Admin gave the SW to the user before checking that the ground station equipment is operating correctly (e.g. The tablet is charged, the laptop is	

Scenarios

First operational mode

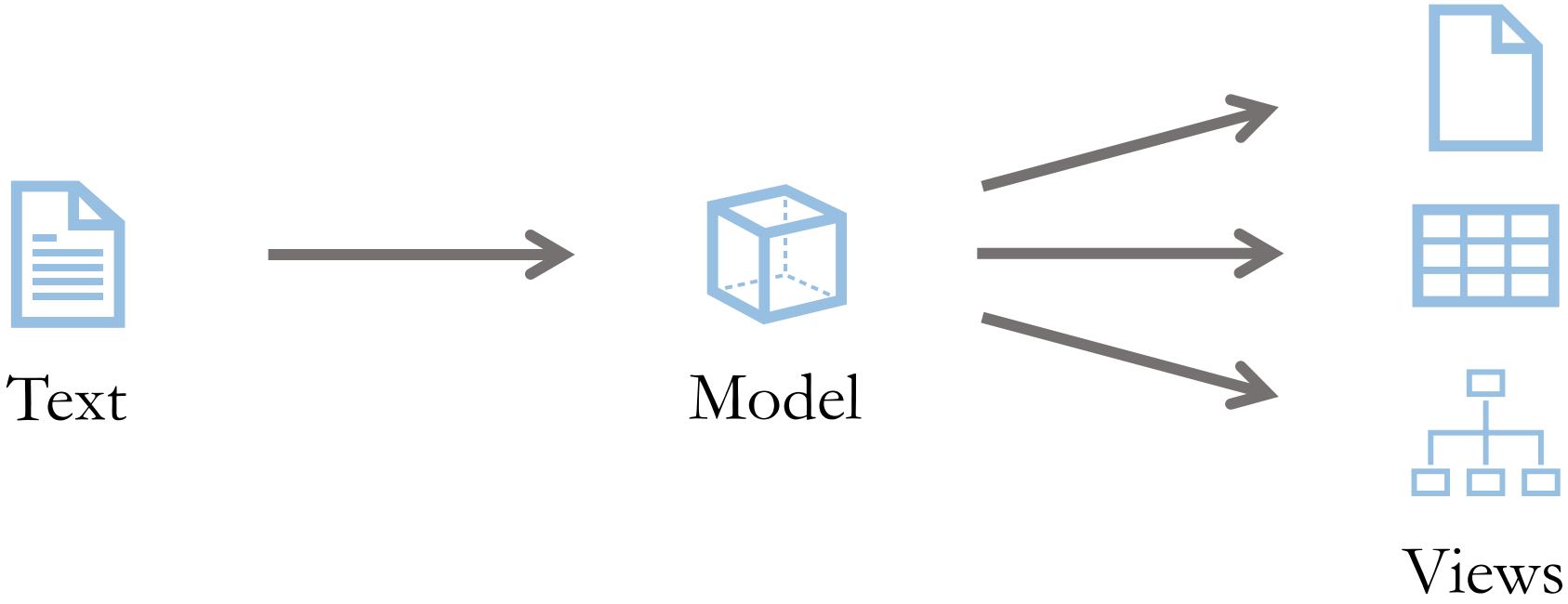
Control action: Give SW to user

UCA 1: Admin gave the SW to user, without some form of safety deposit

Σ 1: Admin gave the SW to user, without some form of safety deposit, because they did not think that having a security deposit is important.

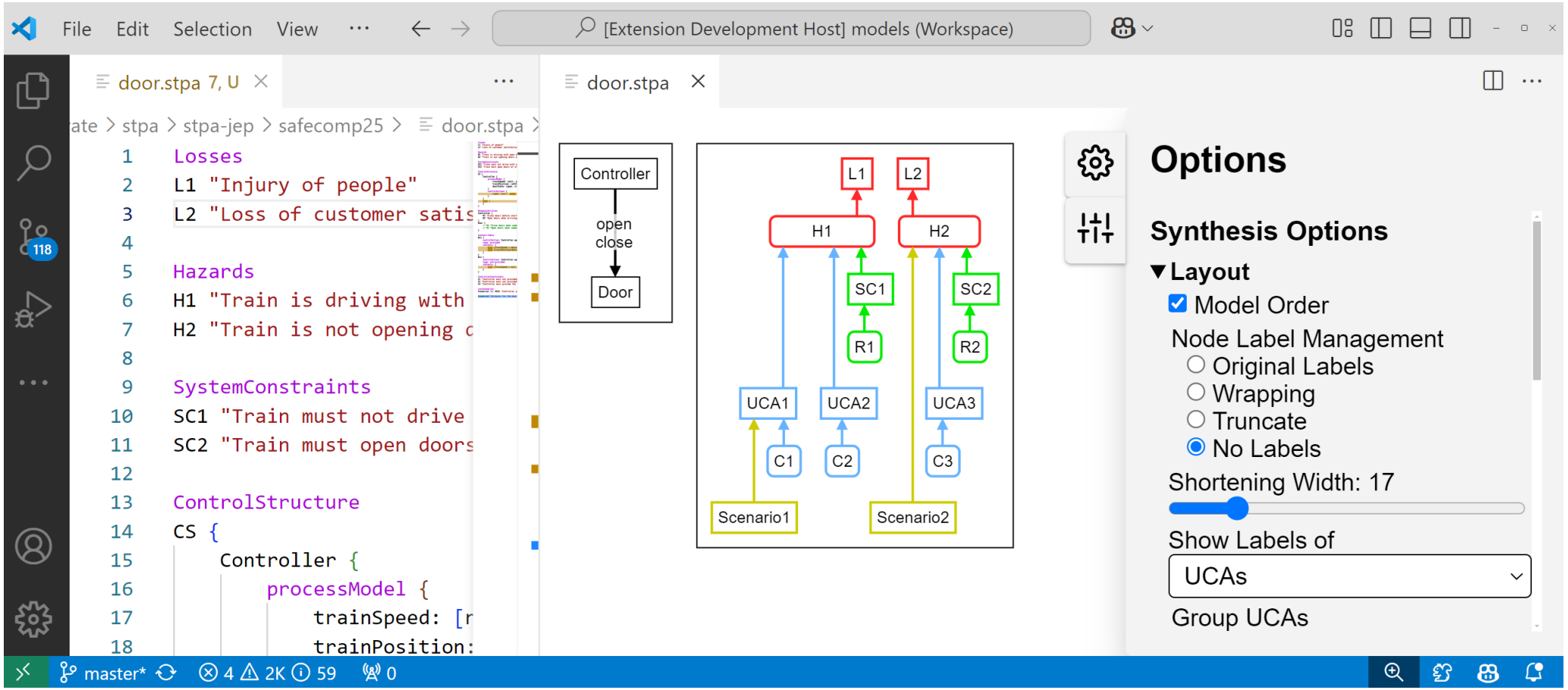
Σ 2: Admin gave the SW to user, without some form of safety deposit, because they had a lot of users to serve and did not had enough time to ask for it, or they forgot to ask for the deposit from

Combine **Textual** Descriptions with **Diagrams** in PASTA



Maximilian Kasperowski and Niklas Rentz and Sören Domrös and Reinhard von Hanxleden:
"KIELER: A Text-First Framework for Automatic Diagramming of Complex Systems."
In Proceedings of the 14th International Conference on the Theory and Application of Diagrams, DIAGRAMS '24.

Pragmatic Automated System-Theoretic Process Analysis (PASTA)



J. Petzold, J. Kreiß, R. von Hanxleden: "PASTA: Pragmatic Automated System-Theoretic Process Analysis."
2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2023.

New Features

Structural Analysis

Automation

Automatic Description Filtering

Textual-Graphical Report Generation

New Features

Structural Analysis: detect missing feedback in control structure

Automation

Automatic Description Filtering

Textual-Graphical Report Generation

New Features

Structural Analysis

Automation

Automatic Description Filtering

Textual-Graphical Report Generation

New Features

Structural Analysis

Automation: generate UCA text for scenarios

Automatic Description Filtering

Textual-Graphical Report Generation

New Features

Structural Analysis

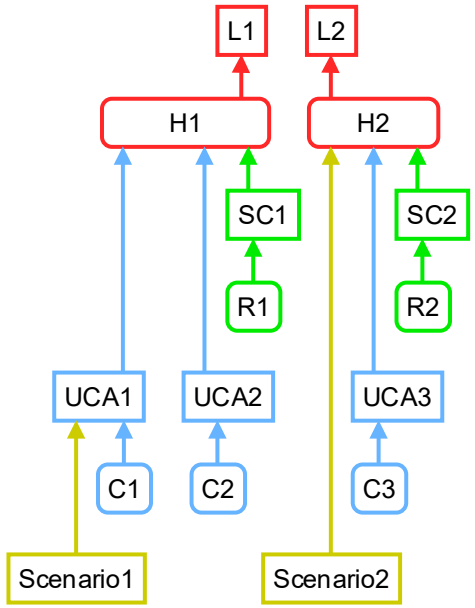
Automation

Automatic Description Filtering

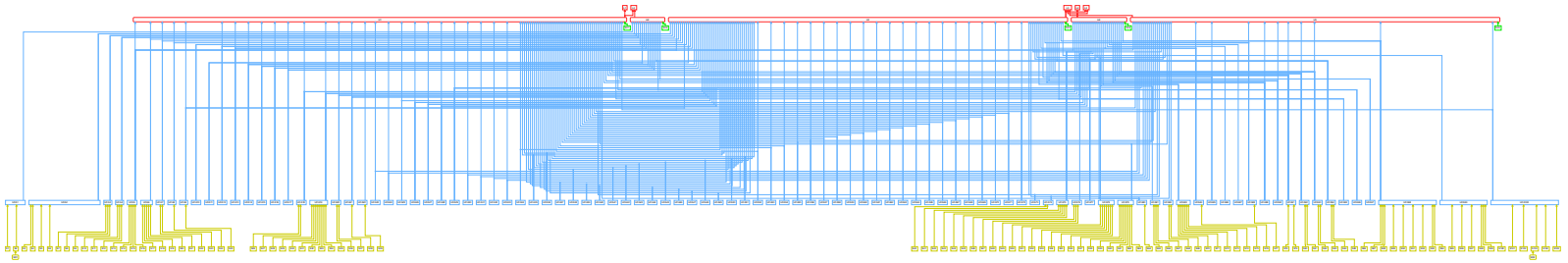
Textual-Graphical Report Generation

Problem of Diagrams

small examples clear

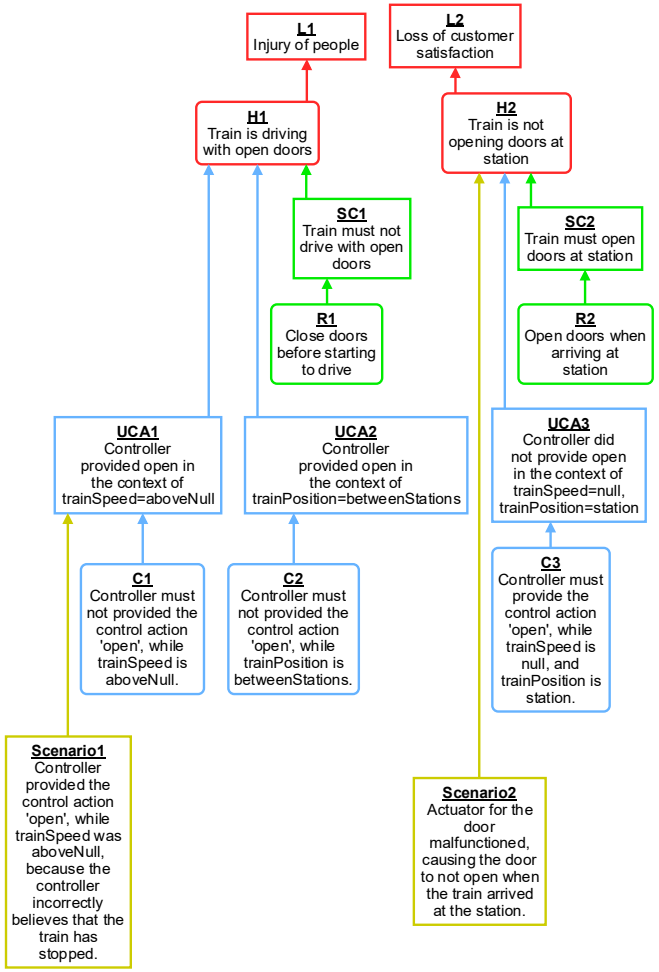


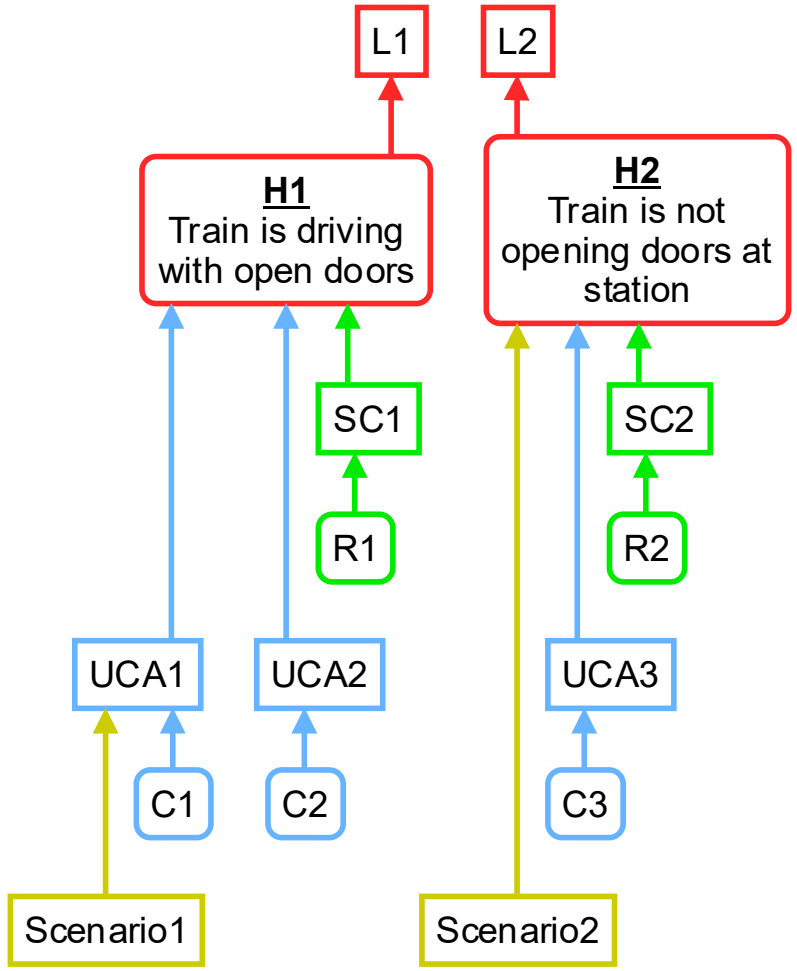
realistic analysis unclear



even more problematic when displaying descriptions

Description Filtering





door.stpa 4

models-private > stpa > stpa-jep > safecomp25 > door.stpa > ...

```
Losses
L1 "Injury of people"
L2 "Loss of customer satisfaction"

Hazards
H1 "Train is driving with open doors" [L1]
H2 "Train is not opening doors at station" [L2]

SystemConstraints
SC1 "Train must not drive with open doors" [H1]
SC2 "Train must open doors at station" [H2]

ControlStructure
CS {
    Controller {
        processModel {
            trainSpeed: [null, aboveNull]
            trainPosition: [atStation, betweenStations]
            doorState: [open, closed]
        }
        controlActions {
            [open "open", close "close"] -> Door
        }
    }
    Door {
    }
}

Responsibilities
Controller {
```

New Features

Structural Analysis

Automation

Automatic Description Filtering

Textual-Graphical Report Generation

Result Report

Losses

First Set

L1. ROLFER was unable to execute a SAR mission (Loss of system goal)

L2. Inadequate interactions with the public during the preparation mode (Loss of public trust)

Second Set

L3: A SP dies/injured due to drowning (Loss of mission goal)

L4: People die or get injured due to a direct hit by the UAV (Loss of public trust)

L5: Loss of system equipment, i.e., UAV, SW and Ground Station. (Property loss)

Hazards

First Set

H1: ROLFER was not properly prepared for its mission → L1, L2

H2: A SP is not served adequately during the phase of preparation and handling of a SW → L2

Second Set

H3: The UAV does not approach the distressed human → L3, L5

H4: The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5

H5: The UAV approaches the SP but does not provide rescue assistance to him/her → L3

	Hazard	**SAFETY DESIGN CONSTRAINT**
1	ROLFER was not properly prepared for its mission	ROLFER must be properly prepared for its mission.
2	A SP is not served adequately during the phase of preparation and handling of a SW → L2	Every SP must be adequately served during the phase of preparation and handling of a SW
3	The UAV does not approach the distressed human → L3, L5	The UAV must approach the distressed human
4	The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5	The UAV must not violate the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level
5	The UAV approaches the SP but does not provide rescue assistance to him/her → L3	The UAV must approach the SP and must provide rescue assistance to them

UCA

Control action	Provided	not provided	Wrong timing/ order	Stopped too soon/applied too long
Give SW to user	**UCA 1:** Admin gave the SW to user, without some form of safety deposit**[H2]** **UCA 2:** Admin gave the SW to user without properly explaining the correct way of operating it. **[H2, H3]**	**UCA 3:** Admin did not give the SW to a user, even though there were available SWs. **[H2, H3]** **UCA 4:** Ο admin δεν παρείχε τα SW στους χρήστες τηρώντας προτεραιότητα προς τις ευπαθείς ομάδες. **[H2, H3]**	**UCA 5:** Admin gave the SW to the user before making sure that the UAV is ready for its mission (e.g., the battery is full, the life ring is mounted, the engine motors are working). **[H1, H3, H4, H5]** **UCA 6:** admin gave the SW to a user before checking that the SW is ready for use (e.g., it's operating correctly, the SIM card is installed) **[H1, H3]** **UCA 7:** admin gave the SW to the user before setting up the approved numbers. **[H1, H3]** **UCA 8:** Admin gave the SW to the user before setting up the supervised area borders. **[H1, H3]** **UCA 9:** Admin gave the SW to the user before checking that the ground station equipment is operating correctly (e.g. The tablet is charged, the laptop is	

4

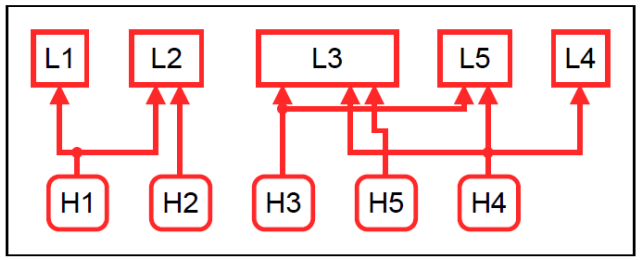
Textual-Graphical Report Generation

Losses

L1: ROLFER was unable to execute a SAR mission (Loss of system goal)
L2: Inadequate interactions with the public during the preparation mode (Loss of public trust)
L3: A SP dies/injured due to drowning (Loss of mission goal)
L4: People die or get injured due to a direct hit by the UAV (Loss of public trust)
L5: Loss of system equipment, i.e., UAV, SW and Ground Station. (Property loss)

Hazards

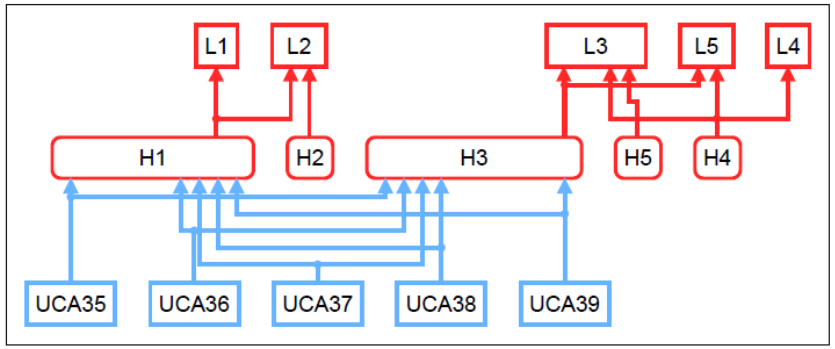
H1: ROLFER was not properly prepared for its mission [L1, L2]
H2: A SP is not served adequately during the phase of preparation and handling of a SW [L2]
H3: The UAV does not approach the distressed human [L3, L5]
H4: The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. [L3, L4, L5]
H5: The UAV approaches the SP but does not provide rescue assistance to him/her [L3]



Textual-Graphical Report Generation

Admin.UAVSafetyButton

not provided	provided	too late or too early	applied too long or stopped too soon
UCA35: in any case. [H1, H3]		**UCA36**: admin long pressed UAV safety button, after having given SW to users. [H1, H3] **UCA37**: admin longed pressed the UAVs safety button before connecting it to Mission planner. [H1, H3] **UCA38**: Admin long pressed the UAVs safety button, after running the script on Mission Planner. [H1, H3] **UCA39**: Admin long pressed the UAVs safety button, before turning on the UAVs controller. [H1, H3]	



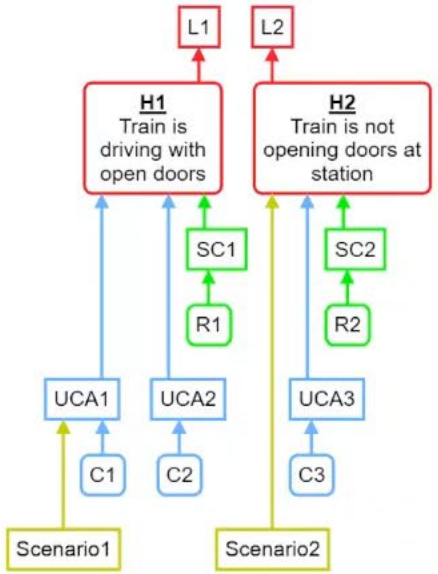
File Edit Selection View Go Run ··· [Extension Development Host] models (Workspace)

door.stpa 4

models-private > stpa > stpa-jep > safecomp25 > door.stpa > SC2

```
1   Losses
2   L1 "Injury of people"
3   L2 "Loss of customer satisfaction"
4
5   Hazards
6   H1 "Train is driving with open doors" [L1]
7   H2 "Train is not opening doors at station" [L2]
8
9   SystemConstraints
10  SC1 "Train must not drive with open doors" [H1]
11  SC2 "Train must open doors at station" [H2]
12
13  ControlStructure
14  CS {
15      Controller {
16          processModel {
17              trainSpeed: [null, aboveNull]
18              trainPosition: [atStation, betweenStations]
19              doorState: [open, closed]
20          }
21          controlActions {
22              [open "open", close "close"] -> Door
23          }
24      }
25      Door {
26      }
27  }
28
29  Responsibilities
30  Controller {
```

door.stpa



models-private master* 195 1K 65 Jette Petzold (2 months ago) Ln 11, Col 37 Spaces: 4 UTF-8 CRLF { } stpa Prettier

Pragmatic Automated System-Theoretic Process Analysis (PASTA)

GitHub Project

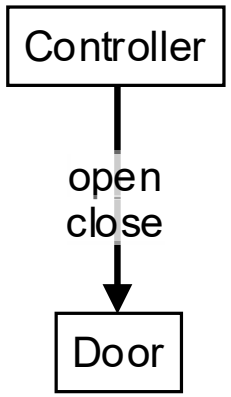
https://github.com/kieler/stpa

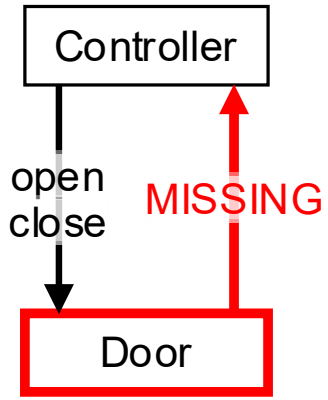
VSCode Marketplace

https://marketplace.visualstudio.com/items?itemName=kieler.pasta

Appendix

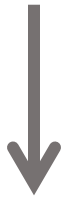
Structural Analysis





Automation – Controller Constraints

⟨*rule ID*⟩ {
controlAction: ⟨*system*⟩.⟨*controlAction*⟩
type: ⟨*UCA type*⟩
contexts: {
⟨*UCA ID*⟩ ⟨*context*⟩
}
}



CC: ⟨*system*⟩⟨*negated UCA type*⟩⟨*context*⟩

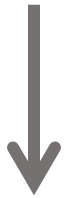
Automation – Controller Constraints

```
RL2 {
  controlAction: Controller.open
  type: not-provided
  contexts: {
    UCA3 [trainSpeed=null, trainPosition=atStation] [H2]
  }
}
```

```
ControllerConstraints
C3 "Controller must provide the control action 'open',
while trainSpeed is null, and trainPosition is atStation." [UCA3]
```

Automation - Scenarios

⟨*rule ID*⟩ {
  controlAction: ⟨*system*⟩.⟨*controlAction*⟩
  type: ⟨*UCA type*⟩
  contexts: {
    ⟨*UCA ID*⟩ ⟨*context*⟩
  }
}



⟨*Scenario ID*⟩ for ⟨*UCA ID*⟩ "⟨*system*⟩ ⟨*UCA type*⟩ ⟨*context*⟩. TODO"

Description Filtering - ROLFER