International Journal of Safety Science
Vo 02, No. 01, (2018), pp. 94-103
DOI:10.24900/ijss/020194103.2018.0301

Special Issue Article: The 5th European STAMP Workshop (ESW) 2017, Chief Editor: Svana Helen Björnsdottir, Reykjavik University

Modelling Multiple Levels of Abstraction in Hierarchical Control Structures

Martin Rejzek[1*], Svana Helen Björnsdóttir[2], Sven Stefan Krauss[1]

[1] *Safety-Critical Systems Research Lab, Zurich University of Applied Sciences; Technikumstrasse 9; 8401 Winterthur; Switzerland; www.zhaw.ch/iamp/sks*

[2] *Stiki - Information Security; Laugavegur 178; 105 Reykjavík; Iceland; www.stiki.eu*

[*] *Corresponding author: martin.rejzek@zhaw.ch*

Abstract

The hazard analysis method "Systems Theoretic Process Analysis" (STPA) makes use of a functional system representation in the form of a Hierarchical Control Structure and uses this model as the starting point for the analysis process. The development of the Hierarchical Control Structure typically involves multiple iterations and starts at a rather abstract view, which is refined during the modelling process. Usually, no differentiation is made between the Hierarchical Control Structure model and its representation as a diagram. In addition, the representation is typically restricted to a single diagram. This paper addresses the opportunities of explicitly differentiating between model and views and introduces a concept encouraging use of multiple diagrams representing one model. This paper also discusses the rulesets and consistency considerations necessary to ensure the analysis is complete and the Hierarchical Control Structure representations are consistent with the model and with each other.

Keywords: *STAMP, STPA, model, modelling, abstraction, diagrams, views*

1. Introduction

Systems Theoretic Process Analysis (STPA) is an analysis method understanding safety and security as emergent properties of a system [1].

The typical analysis process of STPA, depicted in **Figure 1**, can be summarized as following:

- The system to be analyzed, first, needs to be described as a Hierarchical Control Structure (HCS) through the identification of controlling units (controllers), the controlled process, and the flow of control actions and feedback among them. The HCS represents a model of the system under analysis. Development of the Hierarchical Control Structure can be seen as preparation work before performing the STPA.
- In the first step of the analysis, referred to as "STPA Step 1", inadequate control actions are systematically identified and described, and an assessment made about whether they can potentially result in a hazard, making them "unsafe control actions".

- In the second step of the analysis, "STPA Step 2", the reasons are systematically analyzed for why inadequate control actions that result in unwanted process outcomes can occur, and the corresponding scenarios are identfied.

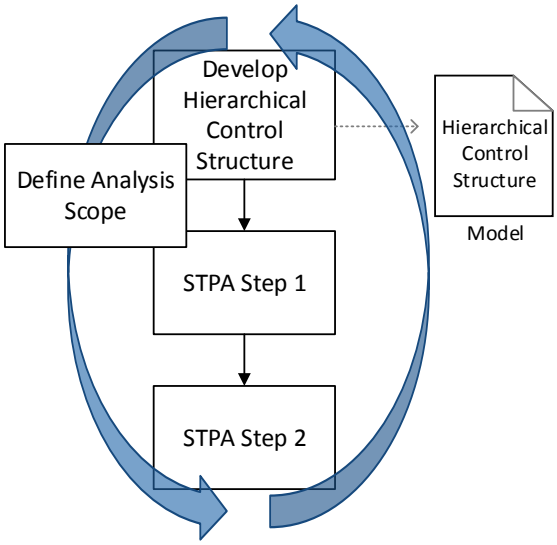

Figure 1: The STPA process is an iterative process (depicted by the blue arrows). The definition of the analysis scope takes place while developing the Hierarchical Control Structure (preparatory step of STPA), but also through STPA Step 1 and Step 2.

1.1. Problem Statement

Typically, the first HCS draft models the system to be analyzed, at a rather abstract level, in the form of a single diagram and refrains from establishing system details.

Such an abstract representation may feature, for example, "traffic control" as single controller, while not modelling the internals of the traffic control system individually. (Further examples of different levels of abstractions can be seen in [2, 3]). Some reasons for starting at an abstract level are as follows (non-exhaustive list):

a) As with every hazard analysis method and also for STPA, the analysis scope needs to be determined. Development of the HCS covers one aspect of this "scope definition". Starting the modelling process at an abstract level allows for establishing a rough scope early in the process. While progressing through the analysis and refining the abstract representation, the scope will gradually become refined.

b) When a system is used in different applications, an analysis based on an abstract representation may serve as a common starting point for individual, application specific analyses, and refinements. Consider a robotic arm used to weld metal plates, but also used for exchanging tools of a milling machine. STPA can be performed for the robotic arm itself, not taking into account the specific application. This analysis can be used as starting point for further, application specific, analyses such as for the welding or tool exchange.

c) An abstract representation may even be valid for various types of systems. For example, the same abstract representation may be used to model cancer treatment with proton radiation beams [4-6] and brachytherapy [3]. This means existing models may be re-used and again serve as starting point for more concrete analyses.

d) Finally, starting the modelling process at an abstract level allows for quick identification of those parts of a system for which further clarification activities are

necessary. This is relevant, since such activities typically require time. The sooner the clarifications are initiated the better.

While progressing with the analysis the original abstract representation is typically "discarded", i.e. it is no longer actively considered for STPA but instead more detailed, refined representations are used. Although the initial abstract representation might be kept as an informative resource (in the simplest form the analyst may keep a printout of the HCS diagram), STPA currently foresees no formal way of maintaining multiple levels of abstraction. This is considered a drawback of the methodology and frames the research objective of this paper.

1.2. Research Objective

This paper promotes making use of multiple diagrams to model the complete HCS. Furthermore, the paper shows what modelling rulesets and constraints need to apply in order to keep the diagrams, and subsequent STPA Step 1 and 2, consistent. In particular, the dependencies between the modelling elements appearing on the HCS diagrams as well as the dependencies of these elements to STPA Step 1 and 2 must be well traced and under control. Otherwise, model and analysis tend to become incomplete and inconsistent.

2. Proposed Concept and Use Cases

The concept described in this paper:

- Explicitly differentiates between the HCS "model" and it's "views";
- Provides the necessary ruleset for modelling HCS with multiple diagrams;
- Shows the influence on the process steps STPA Step 1 and 2 when using multiple diagrams.

As it turns out, the proposed concept doesn't only enable modelling and analyzing multiple levels of abstraction as introduced in chapter 1, but it is also beneficial in other cases:

- <u>Complementing Views:</u> An analyst may use multiple diagrams to model different phases or characteristics of a system, for example, the phases *design*, *operation*, and *decommissioning,* or the characteristics *dose control* and *position control* of a cancer radiation treatment system[1]. Principally the analyst can choose between the following options:
    - The phases or characteristics can be analyzed individually. However, this would result in neglecting the interactions between the phases/characteristics and be against the paradigm of STPA, as the holistic viewpoint would not be followed.
    - All phases or characteristics can be modelled by means of one HCS diagram. Depending on the size and complexity, the result could be a large and confusing representation.
    - Following the concept proposed in this paper: Multiple diagrams can be used to model the phases/characteristics where certain elements (controllers, control actions, etc.) could appear on multiple diagrams. All diagrams are part of the same model. Although multiple

[1] The instrumentation and control system in cancer radiation treatment systems for dose control may be quite different from the system for position control. Therefore, a desire may exist to handle dose control and position control individually from an analysis viewpoint.

diagrams represent the model, the analysis would see the system as a whole and would not handle the diagrams on an individual basis.

- Intelligent Actuators and Sensors: Once the analyst performs STPA Step 2, it can become clear that an element, which has been considered to be a simple actuator or sensor (therefore omitted on the HCS diagram), fulfills all the attributes of a STPA controller. For example, when an actuator configurable (e.g. an actuator which is programmable) and/or has the power to make decisions about the controlled process on its own.
    - The analyst can now go back to the original HCS diagram and add the intelligent actuator (where it would appear as "controller") including the relevant control actions and feedback. (The resulting model would still contain only a single HCS diagram.)
    - Alternatively, the analyst can model the actuator and its control flow on a second HCS diagram. (The resulting model would then contain two HCS diagrams.)
- Functional Redundancies: Some systems make use of functional redundancies. An example of this is two ground based control centers for satellite control. While the control centers could be identical and impose the same strengths and weaknesses, their interconnectivity could lead to additional hazards.
    - The analyst can model the details of the identical ground centers on one diagram and use a second HCS diagram to model the control flow between the ground centers and the satellite.

3. Concept Development Process

The key factors stimulating HCS modelling by means of multiple diagrams are simple to state:

- Allow representation of a HCS by means of multiple diagrams (views);
- Allow using the same element in multiple diagrams;
- Allow parent-child relationship among elements.

However, as mentioned above, keeping the diagrams consistent and ensuring the STPA Step 1 and 2 match the model and are complete is not a trivial objective. The three diagrams in Figure 2 give an illustrative example of this complexity.

Diagram 1 in Figure 2 shows a hierarchical control structure with three controllers (labelled *A*, *B*, and *C*) and a *Controlled Process*. For the sake of this example only two control actions are explicitly shown: *CA1* and *CA2*. *Diagram 2* shows controllers *A*, *B* and the *Controlled Process* again. This diagram does not show *Controller C* and consequently control action *CA1* which is received by *Controller C*. *Diagram 3* shows a third view of the same model focusing on the internals of *Controller B*. Note that *CA1* appears on the first but does not appear on the second and third diagram. Furthermore, the source of *CA2* is *Controller B* in the first and second diagram while it is *Controller B.1* in the third diagram.

This brings up a couple of modelling and analysis questions. How is the analyst made aware of the fact that *Controller B* issues *CA1* when working with *Diagram 2*? Could the analyst show *CA1* on *Diagram 2* even though *Controller C* is not represented? Is it inconsistent to have *CA2* appearing on *Diagram 2* and *3* with different sources? How does *CA2* need to be handled in STPA Step 1 and 2?

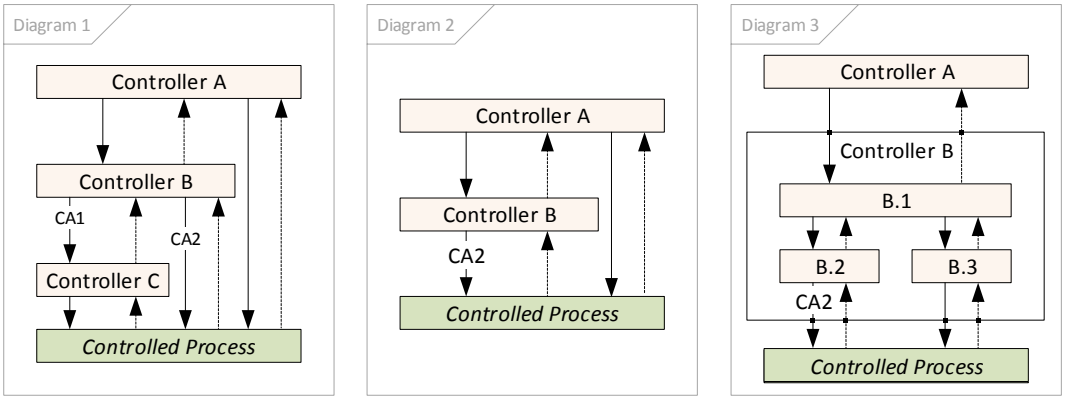

Figure 2: Representation of a Hierarchical Control Structure by means of three diagrams. In order to keep the diagrams consistent and making sure the analysis matches the model and is complete, a ruleset and consistency considerations are indispensable.

To ensure the diagrams are consistent and the analysis is complete, a set of rules and consistency considerations are indispensable - addressing not only the modelling aspect, but also STPA Step 1 and 2. The "divide and conquer strategy" illustrated in Figure 3 was used to derive rulesets and consistency considerations for the individual use cases and consolidate them into one set.

Identify Use Cases: As a first step, use cases have been identified, where using multiple HCS diagrams describing the same model will benefit the analysis. Some of these use cases have already been mentioned in chapter 2.

In a second step the use cases were mentally played through and analyzed with the help of knowledge gained from previous projects [4, 5, 7-10], literature and a constructed example. The aim of the constructed example was to analyze situations, which did not occur in previous projects nor the literature we looked at, but were principally possible.

For each use case the set of rules was derived that is necessary to enable the use case. The ruleset contains specifics about modelling and consistency considerations, as well as, rules influencing STPA Step 1 and 2.

Previous projects, literature, and additional examples where used to preliminary verify the applicability and correctness of the derived ruleset. (A proper verification is yet to be done.)

The individual rulesets where consolidated into one basic ruleset, with the rules and consistency considerations refined. This last step is still a work in progress.

The following two chapters discuss the two use cases "complementing views" and "levels of abstraction".

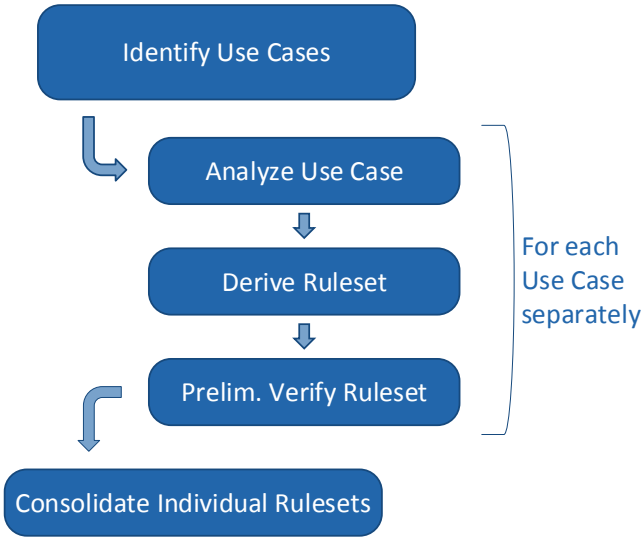

Figure 3: First, use cases were identified that benefited from using multiple Hierarchical Control Structure diagrams. Each use case was separately analyzed, a ruleset derived, and the ruleset preliminary verified. Finally, the individual rulesets where consolidated into one.

4. Complementing Views

4.1. Introduction to Complementing Views

Figure 4 provides an abstract example of complementing views. *Diagram 4a* and *4b* together represent the exact same model as *Diagram 4*, just in two separate diagrams.

Controller Q issues control action *CA1* that is received by *Controller R*. *Controller R* issues control action *CA2* that is received by *Process S*. Additionally, *Controller Q* influences the *Process S* directly by the means of control actions *CA3* and *CA4*. Feedback is not explicitly modelled in this example.

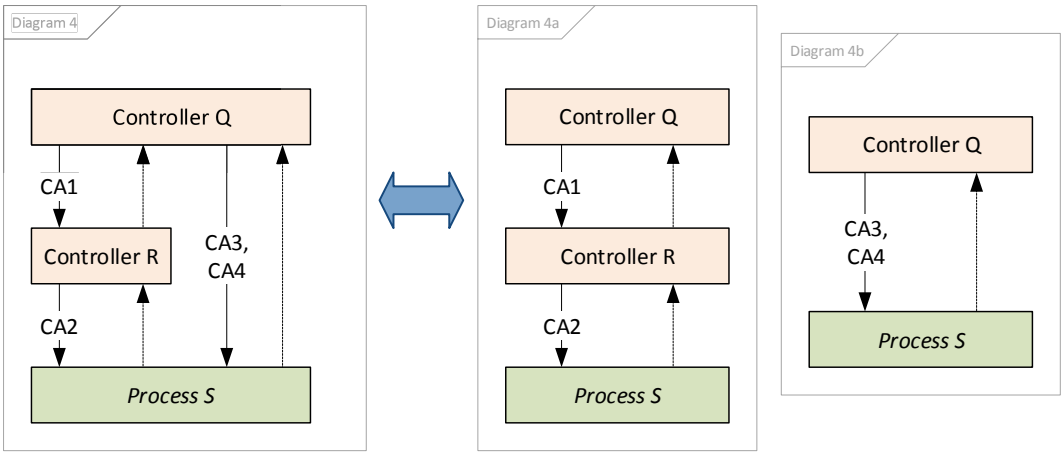

Figure 4: Diagram 4a and 4b together describe exactly the same model as Diagram 4 on the left side.

Table 1 lists the appearance of elements on *Diagram 4*, *4a*, and *4b* from Figure 4.

Element	Appearance in Figure 4		
	Diagram 4	Diagram 4a	Diagram 4b
Controllers:			
Controller Q	Yes	Yes	**Yes**
Controller R	Yes	Yes	**No**
Controlled Processes:			
Process S	Yes	Yes	**Yes**
Control Actions:			
CA1	Yes	Yes	**No**
CA2	Yes	Yes	**No**
CA3	Yes	No	**Yes**
CA4	Yes	No	**Yes**
Feedback:			

Table 1: Appearance of elements on Diagram 4, 4a, and 4b of Figure 4.

4.2. Ruleset for Complementing Views

The rules identified for this use case are simple and straight forward. A subset of those rules is provided in the following list:

- The same controller may appear on multiple diagrams.
- A diagram may show only a subset of the control actions generated/received by a controller.
- STPA Step 1 shall be performed for all control actions regardless of which diagram they are shown on.
- Every element (controller, controlled process, control action, or feedback) shall appear on one diagram at least.
- …

While this rather basic use case can be beneficial to the analyst in certain circumstances, it is also a pre-requisite for all other use cases such as "levels of abstraction" addressed in the following chapter.

5. Levels of Abstraction

5.1. Introduction to Levels of Abstraction

The motivation to support different levels of abstraction when modelling the Hierarchical Control Structure has already been laid out in chapter 1. This use case is based on the premises that two visual representations of a controller exist:

- A representation that shows the controllers interaction with its environment. This view doesn't show any internals of the controller, but it is represented as a black

frame from the hierarchical control structure viewpoint[2]. We refer to this type as D0-representation. (Figure 5, controllers shown on the left diagram)

- A representation that shows the internals of the controller, referred to as D1-representation. In this representation, the decomposed controller is visualized as a frame, which allows refining it with new elements and their control flow. (Figure 5 "Treatment Delivery" on the right)

The example shown in Figure 5 is based on [4-6]. The example shows the D0- and D1-representations of the controller *Treatment Delivery*.

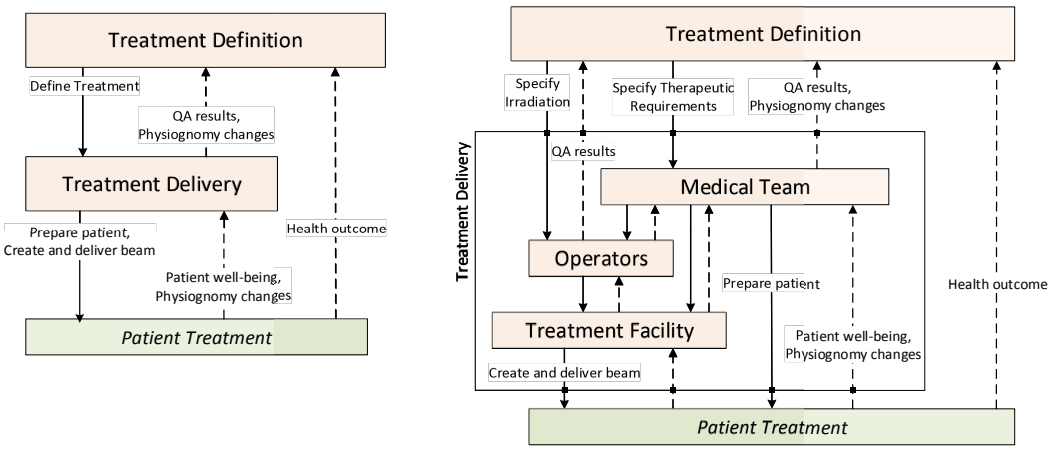

Figure 5: An example based on [4-6] showing two levels of abstraction of the controller "Treatment Delivery" and the control action "Define Treatment". The structure shown on the right shows the internals of "Treatment Delivery". Furthermore, on this side the control action "Define Treatment" is refined into "Specify Irradiation" and "Specify Therapeutic Requirements".

While the left diagram of Figure 5 displays the controller *Treatment Delivery* as a single unit (D0-representation), the right diagram displays the internal details of the *Treatment Delivery* (D1-representation)." These internals are: *Medical Team*, *Operators*, and *Treatment Facility*. While the control actions *Prepare patient,* and *Create and deliver beam* are issued by the controller *Treatment Delivery* on the left, they are issued by *Treatment Facility*, respectively by the *Medical Team* on the right.

The concept of refinement does not only apply to controllers, but also to control actions and feedback. For example, the left diagram of Figure 5 shows the control action *Define Treatment*. This control action is not shown in the right diagram, but it is represented by *Specify Irradiation* and *Specify Therapeutic Requirements*. An overview about the refinement and relationship between controllers, control actions, and feedback is given below in Table 2.

[2] Internals like the process model, which the controller naturally contain are typically not shown graphically on the hierarchical control structure diagram.

Element		Appearance on Figure 5	
Parent element	Child element	Left diagram	Right diagram
Controllers:			
Treatment Definition		Yes	Yes
Treatment Delivery		Yes	As frame
	Medical Team	No	Yes
	Operators	No	Yes
	Treatment Facility	No	Yes
Controlled Processes:			
Patient Treatment		Yes	Yes
Control Actions:			
Define Treatment		Yes	No
	Specify Irradiation	No	Yes
	Specify Therapeutic Requirements	No	Yes
Prepare patient		Yes	Yes
Create and deliver beam		Yes	Yes
Feedback:			
QA results		Yes	Yes*
Physiognomy changes		Yes	Yes
Patient well-being		Yes	Yes
Physiognomy changes		Yes	Yes
Health outcome		Yes	Yes

* Feedback appears twice on the right diagram. Once linked to the Operators, once to the Medical Team.

Table 2: Appearance of elements in Figure 5.

5.2. Ruleset for Levels of Abstraction

Also for the use case "Levels of Abstraction", a set of rules has been identified. For example, the following pair of rules:

- A feedback may have multiple sinks.
- If a feedback has multiple sinks, they must be related to each other by a parent-child relationship.

These two rules apply to the feedback *Patient well-being* of Figure 5. The sink of this feedback is the controller *Treatment Delivery* (left diagram) respectively, but more precisely, the controller *Medical Team* (right diagram) is related by a parent-child relationship with *Treatment Delivery*.

6. Conclusion and Outlook

While the rulesets for the individual use cases have been derived and a successful preliminary verification of them was conducted, the consolidation of the rules is still work in progress.

We believe the concept described in this paper is especially useful when an analysis shall dive into the details of a system. Making sure to comply with the ruleset and

constraints involves some effort; however, we believe this effort is highly automatable through software tools and does therefore not necessarily result in substantial additional workload for the analyst. Nevertheless, the analyst has to understand the basic concept of modelling HCS with multiple diagrams.

The ruleset and constraints allowing complementing views have successfully been implemented in a STPA software tool [11]. In a next step, the proposed concept will be applied from the start of an analysis project with STPA.

Acknowledgments

This work was conducted within research projects supported by the Swiss Commission for Technology and Innovation (project grant number 15822.1 PFIW-IW; [12]) and by Eurostars (project ID 10 663; [13]). The concept described in this paper formed a talk presented at the 5th European STAMP/STPA Workshop and Conference in Reykjavík, Iceland in September 2017. [14, 15]

References

[1] Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety*. 2012, Cambridge MA, USA: MIT Press.

[2] Adesina, A.A., et al., *Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management.* Pharmaceutical Medicine, 2017. **31**(4): p. 267-278.

[3] Pawlicki, T., et al., *Application of systems and control theory-based hazard analysis to radiation oncology*. Medical physics, 2016. **43**(3): p. 1514-1530.

[4] Rejzek, M., *Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System*, in *STAMP Workshop 2012*. 2012: MIT, Boston.

[5] Rejzek, M., *Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System ... a Review*, in *1st European STAMP Workshop*. 2012: Braunschweig.

[6] 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.

[7] Rejzek, M., *Use of STPA in digital instrumentation and control systems of nuclear power plants*, in *2nd European STAMP Workshop*. 2014: Stuttgart.

[8] Rejzek, M., C. Hilbes, and S.S. Krauss, *Safety Driven Design with UML and STPA*, in *STAMP Workshop 2015*. 2015: MIT, Boston.

[9] Krauss, S.S., M. Rejzek, and C. Hilbes, *Tool Qualification Considerations for Tools Supporting STPA.* Procedia Engineering, 2015. **128**: p. 15-24.

[10] Krauss, S.S., M. Reif, and M. Moser, *CAST Analysis of a Railroad Accident in Switzerland*, in *5th European STAMP/STPA Workshop and Conference*. 2017: Reykjavik, Iceland.

[11] *Risk Management studio (RM Studio)*. Available from: http://www.riskmanagementstudio.com/.

[12] *Swiss Confederation - Commission for Technology and Innovation CTI*. Available from: https://www.kti.admin.ch/kti/en/home.html.

[13] *European Commission - Eurostars*. Available from: https://www.eurostars-eureka.eu/.

[14] *5th European STAMP/STPA Workshop and Conference*. Available from: https://en.ru.is/stamp.

[15] *ESW: European STAMP Workshop*. Available from: http://www.stamp-workshop.eu/.