

The Challenges of Supporting STPA with a Software Tool

Svana Helen Björnsdóttir

Christopher Brown

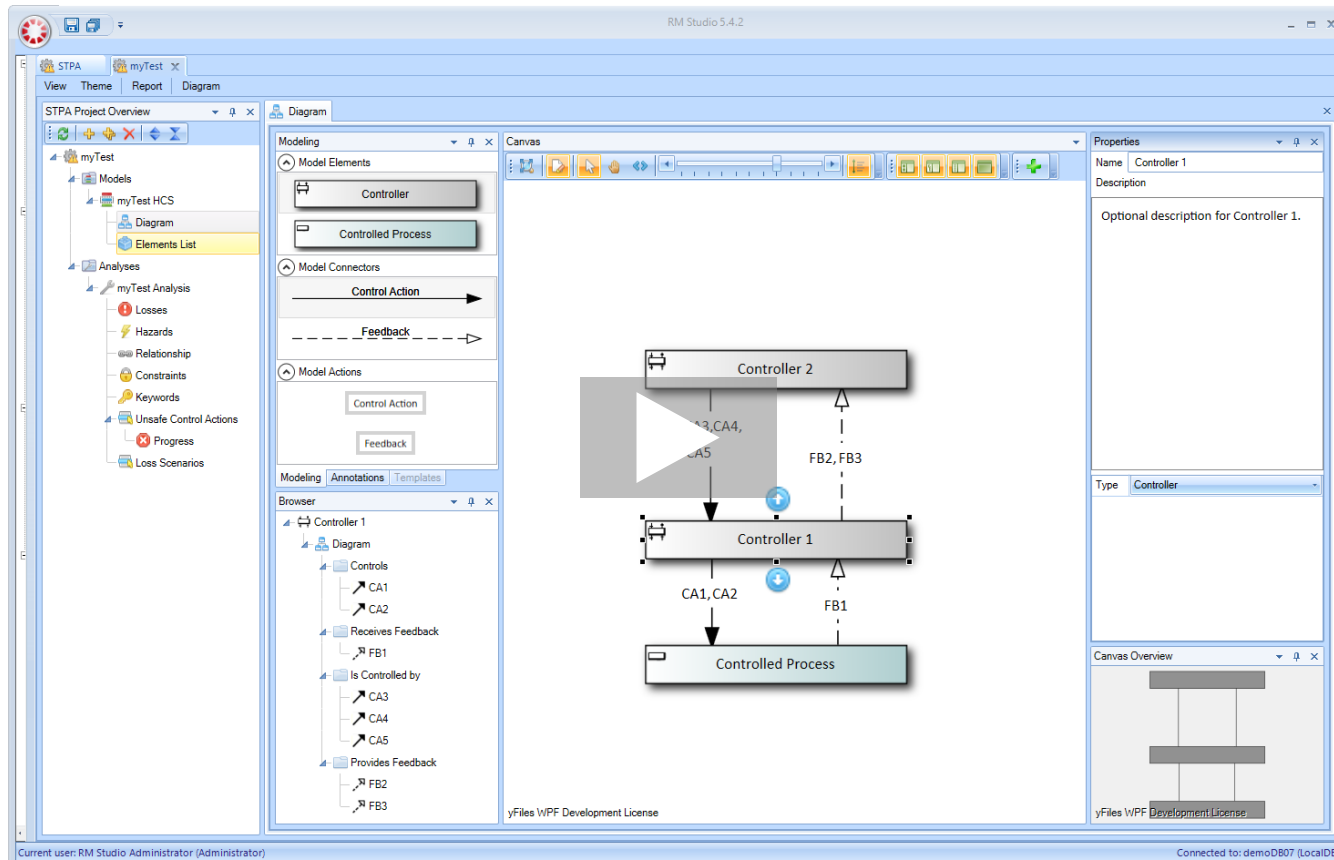
Martin Rejzek

- STPA is applied in different Industry Domains
 - Systematically analyzed our own research projects
 - Screened a lot of STPA literature
 - Spent a lot of time on terminology
- Diverse stakeholders
 - Provide specific reports for analysts/managers/board
 - Account for STPA knowledge and experience
- Best practice in working with STPA is an iterative approach
 - Allow to start Step 1 and 2 while still working on HCS
 - Support identifying items needing reevaluation
 - Ensure traceability is established and maintained

- Making the Diagramming sophisticated and flexible enough
 - Make capturing diagrams easy
 - Provide advanced functions for adaptability
 - feature meta-data for all elements
 - Choosing the optimal third party graphics library
- Support refinement (zooming in) of HCS
 - Support having multiple diagrams
 - Allow re-using elements on diagrams
 - Ensure consistency and completeness
 - Manage all the dependencies between HCS and Step 1, 2

(See recently published paper on this referenced at end of slide deck)

- Aligning the diagramming with the analysis process
 - Use minimal constraints on diagramming process
 - Progress measuring no parts are missing
- People tend to use «Constraints» very differently
 - Keep the constraints as flexible as possible
 - Allow to categorize by user definable categories
- STPA is often applied collaboratively by teams
 - Store data in a database which allows check-in/out
 - Support multi-screens
 - Support annotations requesting reviews or input from team members



Video demonstration and further information on the software module:
<https://www.riskmanagementstudio.com/features/stpa>

Contact:

Svana Helen Björnsdóttir

svana@stiki.eu

<https://stiki.eu/>

Christopher Brown

chris@stiki.eu

<https://stiki.eu/>

Martin Rejzek

martin.rejzek@zhaw.ch

<http://zhaw.ch/iamp/sks>

This project is supported by:

Eurostars

Technology Development Fund, Iceland

Swiss Confederation, Federal Department of
Economic Affairs, State Secretariat for Education,
Research and Innovation SERI



Video demonstration and further information on the software module:
<https://www.riskmanagementstudio.com/features/stpa>

Tool Qualification Considerations



Stiki is certified by:



We also looked into (see references at end of slide deck):



Industrial / Generic

- IEC 61508 Part 3
- IEC 61508 Part 4



Railway

- EN 50128



Aerospace & Defense

- DO-178C
- DO-330



Automotive

- ISO 26262 Part 8

Modelling Multiple Levels of Abstraction in Hierarchical Control Structures

- Talk at [European STAMP Workshop and Conference 2017](#)
- Paper in [International Journal of Safety Science](#)

Tool Qualification Considerations for (Software) Tools Supporting STPA

- Talk at [3rd European STAMP Workshop](#)
- Paper in [Elsevier Procedia Engineering](#)

RM Studio STPA Module

- <https://www.riskmanagementstudio.com/features/stpa>

Stiki Information Security

- <https://stiki.eu/>

Safety-Critical Systems Research Lab, Zurich University of Applied Sciences

- <http://zhaw.ch/iamp/sks>