Zurich University
of Applied Sciences

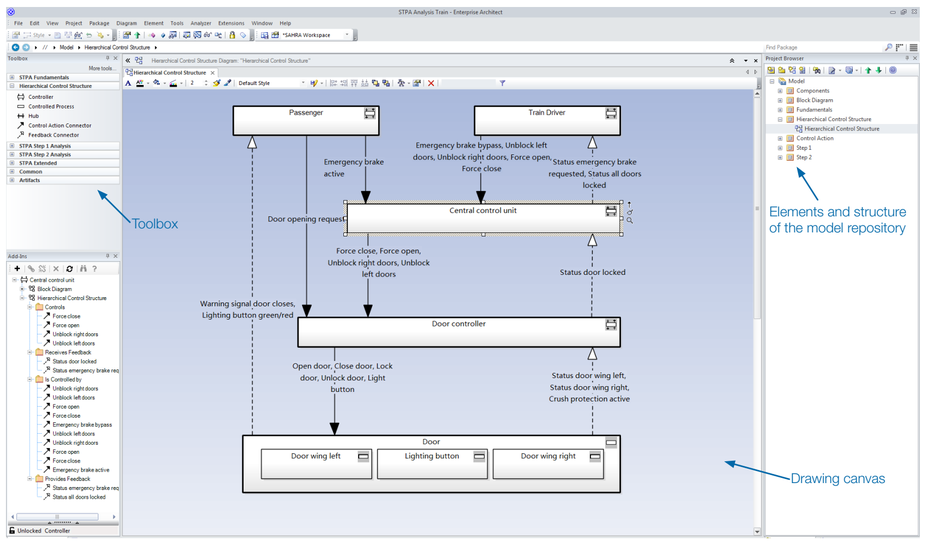
SAHRA - An integrated software tool for STPA

Sven S. Krauss, Martin Rejzek, Christoph W. Senn, Christian Hilbes
Institute of Applied Mathematics and Physics IAMP
Zurich University of Applied Sciences ZHAW, Switzerland

SAHRA (STPA based Hazard and Risk Analysis) as a software tool for STAMP/STPA improves the analysis work-flow by not only supporting the complete STPA process but by also offering a unique way to capture Step 1 and 2 using the visual style of mind maps. SAHRA is seamlessly integrated into the widely used UML solution Sparx Systems Enterprise Architect (EA). This integration enables synergies between design of a system and its safety analysis and thus allows to use STPA in the paradigm of safety-guided design.

Capturing the Hierarchical Control Structure

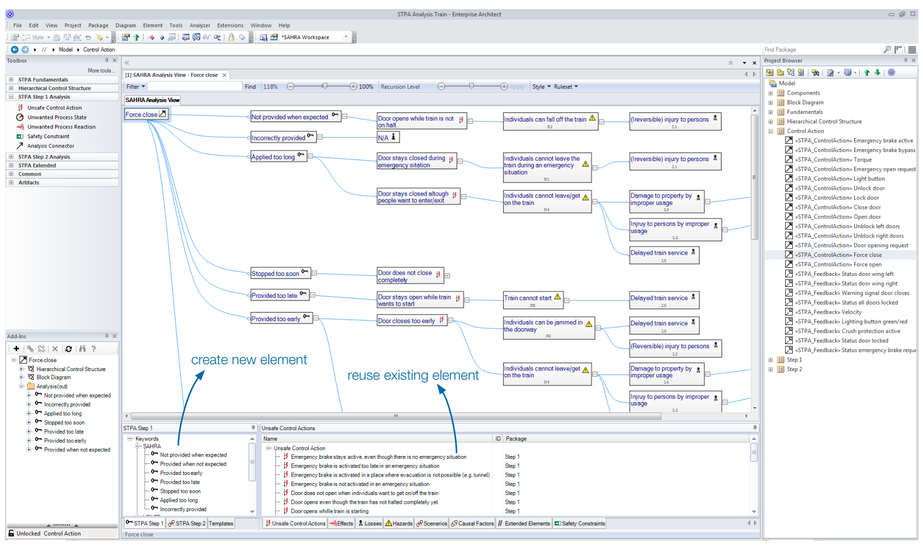
We consider hierarchical control structures (HCS) as just ‘another view’ of a system. SAHRA allows to capture HCS as diagrams and stores all information, together with design data in a common database, the so called model repository.



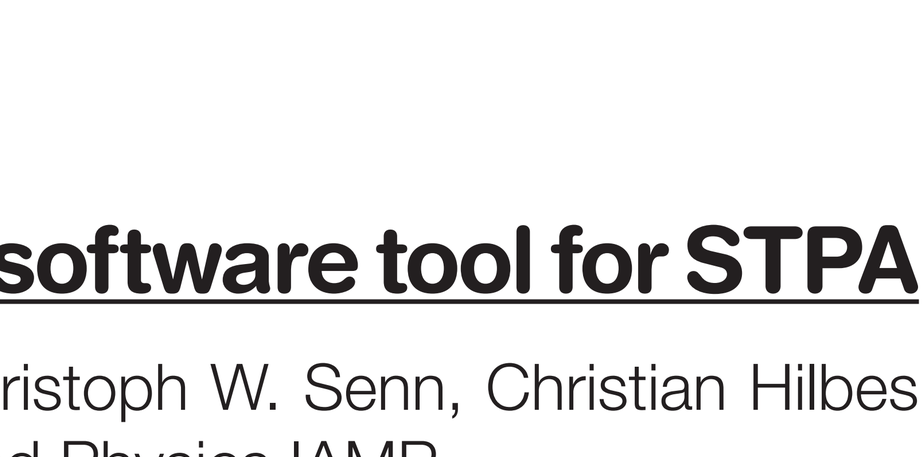
Screenshot of SAHRA as extension for the UML/SysML tool Enterprise Architect. The model of a Hierarchical Control Structure is shown in the center of the screenshot. The controller ‘Central control unit’ is currently selected. The toolbox (top left) contains all elements needed for capturing STPA diagrams. The model repository and its structure is shown in the repository tree (right).

A Unique Style of Analysis

A tendency of the wide spread approach to document STPA Step 1 using tables is to omit details as there is only very limited space for writing them down and to maintain consistency as relationships need to be maintained by hand. SAHRA therefore introduces mind maps, as means of visually representing and editing an analysis. This enables the analyst to see relationships at a glance and provides maximal flexibility with respect to documentation details.



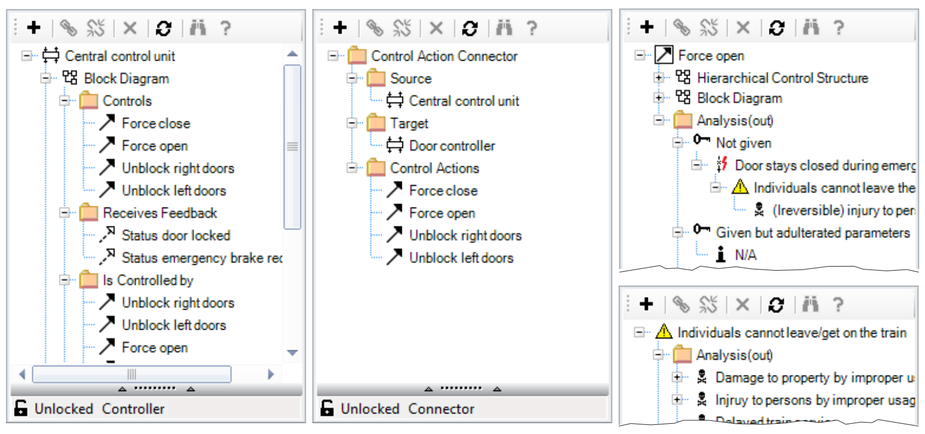
SAHRA allows to capture STPA Step 1 and 2 analysis in the visual style of mind map diagrams. The analysis information is captured by individual elements reflecting for example Keywords, UCAs, Hazards, and Losses. This provides maximum flexibility to the analyst in terms of documenting the analysis. Drag and drop from the lower left panel allows to easily create new elements. Drag and drop from the lower right panel allows to reuse existing elements while inheriting existing relationships.



STPA step 2 control loops can be captured just as hierarchical control structures.

SAHRA Object Browser for Traceability

The information of the mind maps is used to build a directed graph in the model repository serving as foundation for traceability analysis. To support the analyst, SAHRA provides a context sensitive object browser.



SAHRA’s context sensitive object browser shows information for the currently selected element: controller (left), control action connector (center), control action (top right), hazard (bottom right).

Requirements, Design & Analysis in One Repository

All elements created with SAHRA are stored in a common model repository. This allows to easily reuse them in other diagrams and to establish relationships between requirements, design, and safety analysis.

Integration Advantages

SAHRA is integrated into EA which enables the user to fully benefit from already existing EA features like multi-user support, scripting, automation, and configuration management integration. These features are extended by providing a dedicated STPA profile, including diagram types, elements and toolboxes for STPA modelling. SAHRA comes with a set of templates to generate customizable documents, reports and search queries.

Results

SAHRA has been successfully used in the context of applied research and development projects in industry and academia. The innovative approach using a directed graph and its visual representation as mind map proved SAHRA‘s capability to analyze large and complex systems.

www.sahra.ch
www.zhaw.ch/iamp/sks

Acknowledgements
The project is funded by the Swiss Commission for Technology and Innovation (CTI, 15822.1 PFIW-IW) and by Curtiss-Wright Drive Technology GmbH.

References
Sparx Systems Pty Ltd. http://www.sparxsystems.com
Thomas, J. (2013). Phd Thesis, MIT Boston USA