Abstract

The Context and Its Importance For analyzing safety and reliability of systems, so-called Minimal Cut Sets (MCS) are generated. The information generated by Minimal Cut Set (MCS) analysis is large. This information contains the logic of a fault tree (FT) under analysis. The Top Level Event (TLE), which is the root of the FT, represents a hazardous state of the system being analyzed. MCS analysis helps in analyzing the fault tree qualitatively—and quantitatively when accompanied with quantitative measures. MCS analysis identifies weaknesses of the system being examined.

Safety analysis (containing the MCS analysis) is especially important for critical systems, where harm can be done to the environment, or to humans causing injuries or even death during the system usage. MCS analysis is performed using computers generating a lot of information. This phase is called *MCS analysis I* in this thesis. The information is then analyzed by the analysts to determine possible issues and to improve the design of the system regarding its safety as early as possible. This phase is called *MCS analysis II* in this thesis.

The goal of my thesis was developing interactive visualizations to support MCS analysis II of one fault tree (FT).

The Methodology As safety visualization—in this thesis, Minimal Cut Set analysis II visualization—is an emerging field and no complete checklist regarding Minimal Cut Set analysis II requirements and gaps were available from the perspective of visualization and interaction capabilities, I have conducted multiple studies using different methods with different data sources (i.e., triangulation of methods and data) for determining these requirements and gaps before developing and evaluating visualizations and interactions supporting Minimal Cut Set analysis II. Thus, I used the following methodology in my thesis:

1. First, I conducted a triangulation of mixed methods and data sources for:
   (a) Understanding the importance of MCS analysis II by its purposes (obtained from both literature and practice)
   (b) Building a baseline of requirements with respect to MCS analysis II from both literature and practice for guiding the visualization field
   (c) Identifying the minimum requirements that are the most achieved requirements by the tools and that should at least be provided by any newly developed tool to avoid degrading its quality in comparison to the other tools
   (d) Identifying the gaps of the best currently used tools that perform MCS analysis I from both literature and practice so that they will be addressed while developing prospective visualizations supporting MCS analysis II. The gaps are derived by characterizing the tools regarding their completeness in providing the necessary information and regarding their representations and their interaction facilities that support MCS analysis II.
   (e) Identifying suitable tools that represent the characteristics of most tools for a control group for comparative experiments
   (f) Identifying the problem sizes of the generated information from MCS analysis I that most analysts deal with
   (g) Identifying an estimation of the time needed for performing MCS analysis II and comparisons

2. Then, I developed three novel interactive visualizations and one novel interaction widget.
3. Finally, I evaluated these interactive visualizations both objectively and subjectively from the point of view of the users and developers of the safety and reliability tools that perform MCS analysis I with respect to their degree in supporting MCS analysis II and from the point of non-domain people using empirical strategies. Both real and manipulated data were used for assessing the visualizations and the interaction widget.

The Main Findings Regarding MCS Analysis II My main findings of the triangulation are:

Requirements: Over 100 requirements were determined and are provided in a table.

Gaps: Almost all safety/reliability tools represent the information generated by MCS analysis I in textual or tabular form. Therefore, the safety analysts need to navigate a lot through this textual/tabular information to gain an adequate overview in order to understand the system. Also, almost all tools do not provide overviews of this generated information leading to missing potential critical MCSs. Additionally, almost all tools do not provide interactions—such as sorting and filtering according to multiple measures—with the generated information to enhance the exploration and the analysis of the information. Moreover, an interactive mapping between the generated information from MCS analysis I and the model of the system being analyzed—whether in 2D or 3D—is rarely provided. Further, no information is given about the properties and shape of the physical parts related to the BEs or their location in the system. Still, some necessary information are rarely provided such as the basic event number of occurrence among others. Besides, no information regarding the distribution of the measures are provided by the tools. Finally, the communication between the analysts and their stakeholders—e.g., system engineers—is not considered being easy. Thus, there is a need to fill these gaps while at the same time achieving the requirements of the analysts and their stakeholders to support the analysts in finding alternative solutions for improving the safety and reliability of their systems, i.e., MCS analysis II.

Suitable Tools: The suitable tools (control group) for evaluating newly developed interactive tools are (without order): FaultTree+, RAM Commander, OpenFTA, FinPSA, Relex, SAPHIRE, WinNUPRA, ViSSaAn, ESSaRel, CARA, DPL Fault Tree, Item Toolkit, MagicDraw, RiskSpectrum, BlockSim, Cabtree, LOGAN FTA, CAFTA, PLFault-CAT, FTAnalyzer, and C^{2}FT.

Common Problem Sizes Dealt with in Practice: The practitioners consider problem sizes (generated information from MCS analysis I that should be analyzed by the analysts) being small when having 10s of MCSs, medium having 100s MCSs, and large having 1000s of MCSs or more. Thus, evaluations should use at least one data set having medium problem size.

Time Spent: Finally, the amount of time spent during MCS analysis II takes up to several days using FaultTree+ for analyzing a medium sized FT (with 100s of MCSs) and up to 2 hours for comparing two FTs having the same medium size regarding their single points of failure using RiskSpectrum.

The Main Contributions Regarding Interactive Visualizations To solve all of these cumbersome problems, I developed multiple interactive visualizations in order to support MCS analysis II of one fault tree.

I have found that, indeed, integrating high quality interactive visualizations into the safety/reliability tools makes the tasks of the analysts—analyzing the results of MCS analysis I (i.e., MCS analysis II)—easier and faster. This leads to increasing their productivity, helps in understanding the system at a glance, provides finding new ways in analyzing the generated information, supports finding unexpected patterns, and last but not least helps in communicating with their stakeholders.

The Spiral interactive visualization tool The *Spiral interactive visualization tool* is the main development. It contains two novel contributions: the Safety Spiral visualization and the Dynamic Slider interaction widget. The properties of this tool are:

1. Multiple novel concepts were introduced in all the visualization domain, the MCS analysis domain, and the empirical studies domain:
    - the physical part importance,
    - the BE (or physical part) quality,
    - the cascading effect,
    - the dynamic shape change of the slider thumb,
    - the filtering type 'simulating solving',
    - cross filtered BEs and MCSs,
    - the expectation questionnaire with a comparison baseline.
2. It supports analysts with different color visions, i.e., full color vision, color deficiency protanopia, deuteranopia, and tritanopia.
3. It achieved 100 out of 103 (97%) requirements obtained from the triangulation and it filled 37 out of 39 (95%) gaps.
4. Its usability was rated high by the users of the safety and reliability tools (better than their best currently used tools: RiskSpectrum, ESSaRel, FaultTree+, and a self-developed tool) and at least similar to the best currently used tools from the point of view of the CAFTA tool developers.
5. Compared to the FaultTree+ tool, its quality was rated higher regarding its degree of supporting MCS analysis II.
6. The time spent for discovering the critical MCSs for a problem size of 540 MCSs (with a worst case of all MCSs having equal order) was less than a minute while achieving 99.5% accuracy.
7. The scalability of the Spiral visualization is above 4000 MCSs for a comparison tasks.
8. The Dynamic Slider interaction widget solved the overlapping thumbs issue existing in all previous sliders.

CakES interactive visualization tool The properties of the CakES interactive visualization tool using the CakES metaphor for analyzing safety issues of Embedded Systems are:

1. It is a pioneer in representing the MCSs as non node-link objects: circles whose colors show their FP levels.

2. It encodes the classification of the MCSs according to their FPs by holder position, color, and two saturation levels (complementary coding).

3. It provides the ability to change the coloring of MCSs according to the color vision of the user.

4. It provides filtering the information according to the MCSs' FP.

5. It provides the physical parts (shape and location) related to the BEs of an MCS.

6. It provides the 3D model view of the system being analyzed.

7. It provides interacting with the views for exploration and analysis of the system (3D interactions: rotation, zoom, and pan).

8. It supports exploring the inside of the physical model by choosing the option translucent.

9. It provides switching between standard and stereo view for the model view (developed by Dr. Taimur Khan) using the Anyscreen library.

10. It provides demonstrating the information on monitor, tiled-wall, or power wall (developed by Dr. Taimur Khan) using the Anyscreen library.

Enhanced CakES interactive visualization tool The Enhanced CakES interactive visualization tool for analyzing safety issues of Embedded Systems uses the CakES metaphor for showing the MCSs and their properties. The improvements over the CakES interactive visualization tool are:

1. It provides three different saturation levels for more detailed exploration.

2. It provides an additional color vision representation for the users with color deficiency "Tritanopia".

3. It provides the MCS order (i.e., domino representation integration).

4. When a MCS is selected, the physical part related to the BE with the highest FP is automatically provided in the BE view.

5. It provides a MCS tab and a BE tab supporting the analysis starting by the MCSs or the BEs, respectively.

6. It provides selecting a BE (i.e., multi-selection of MCSs). Thus, the analyst can observe the BEs' NoO and its quality.

7. It provides two interaction speeds for panning and zooming in the MCS, BE, and model views.

8. It combines MCS analysis results and the model of an embedded system enabling the analysts to directly relate safety information with the corresponding parts of the system being analyzed and provides an interactive mapping between the textual information of the BEs and MCSs and the parts related to the BEs.

9. It can be used on different screen configurations. (developed by Dr. Taimur Khan) using the Anyscreen library.

10. Its users achieved higher accuracy (247%-100%=147% increase) while spending slightly more time (since not all users of the ESSaRel tool could complete the required task, 35 minutes - 32 minutes = 3 minutes more) for identifying the MCSs with the highest FPs compared to the ESSaRel tool using text for the generated information from MCS analysis I.

11. Regarding its usability: its usefulness was rated higher than the usefulness of the ESSaRel tool for identifying the MCSs with the highest FPs and their related information.

12. It can be used on different screen configurations. (developed by Dr. Taimur Khan) using the Anyscreen library

13. It combines MCS analysis results and the model of an embedded system enabling the analysts to directly relate safety information with the corresponding parts of the system being analyzed and provides an interactive mapping between the textual information of the BEs and MCSs and the parts related to the BEs.

Verifications and Assessments I have evaluated all visualizations and the interaction widget both objectively and subjectively. Finally, I also evaluated the final Spiral visualization tool both objectively and subjectively regarding the quality perceived by its users and regarding its degree of supporting MCS analysis II.

Conclusions and Recommendations for Future Research Integrating high quality interactive visualizations into the tools for safety/reliability analysis eases and speeds up the execution of the tasks of the analysts: analyzing the results of MCS analysis I (i.e., MCS analysis II). This leads to increasing their productivity, helps in understanding the system at a glance, provides finding new ways in analyzing the generated information, supports finding unexpected patterns, and last but not least helps in communicating with their stakeholders.

It would be nice to test the Spiral visualization tool using other application examples from the ViERforES and related projects and other projects.

Finally, I invite other researchers of interactive visualization tools that support MCS analysis II to perform an empirical controlled experiment on large problem sizes to measure the quality of the tools.