Comparison of the FMEA and STPA safety analysis methods–a case study

Sardar Muhammad Sulaman[1] Armin Beer[2] Michael Felderer[3] Martin Höst[4]

Abstract: This summary refers to the paper 'Comparison of the FMEA and STPA safety analysis methods–a case study' [Su17]. The paper was published as an article in the Software Quality Journal. It compares the Failure Mode and Effect Analysis (FMEA) and the System Theoretic Process Analysis (STPA) in an industrial case study.

Keywords: Hazard analysis; safety analysis; critical systems; risk management; failure mode and effect analysis; system theoretic process analysis; FMEA; STPA

1 Overview

As our society becomes more and more dependent on IT systems, failures of these systems can severely harm people and organizations. Diligently performing risk and hazard analysis helps to minimize the potential harm of IT system failures on individuals and the society and increases the probability of their undisturbed operation. Risk and hazard analysis is an important activity for the development and operation of critical software intensive systems, but the increased complexity and size puts additional requirements on the effectiveness of risk and hazard analysis methods. The paper presents a qualitative comparison of the two prominent hazard analysis methods Failure Mode and Effect Analysis (FMEA) [St03] and System Theoretic Process Analysis (STPA) [Le04] by applying the case study research methodology.

2 Results

To compare FMEA and STPA, both safety analysis methods been applied in a case study on the same forward collision avoidance system. Moreover, the analysis process of FMEA and STPA was also evaluated by applying qualitative criteria derived from the Technology Acceptance Model. It turned out that almost all types of hazards that were identified

[1] Lund University, Lund, Sweden sardar@cs.lth.se

[2] Beer Test Consulting, Baden, Austria armin.beer@bva.at

[3] Universität Innsbruck, Innsbruck, Austria michael.felderer@uibk.ac.at

[4] Lund University, Lund, Sweden martin.host@cs.lth.se

doi:10.18420/se2019-55

in the study were found by both methods. That is, both methods found hazards of type component interaction, software, component failure and system. With regard to component failure hazards, FMEA identified more component failure hazards than STPA. With regard to software hazards, STPA found more hazards than FMEA. With regard to component interaction hazards, STPA found some hazards, however, FMEA did not find any distinct hazards. Finally, with regard to system type error hazards, FMEA found slightly more hazards than STPA. Both FMEA and STPA consider system decomposition (FMEA decomposes and STPA considers whole system for analysis), identification of potential failures, their causes and effects, as well as definition of countermeasures. But STPA does not consider risk assessment in terms of risk priority number calculation and assignment of the application function to each subsystem. The methods have a different focus. FMEA especially takes the architecture and complexity of components into account, whereas STPA is stronger in finding causal factors of identified hazards. It can be concluded that, in this study, there was no hazard type that was not found by any of the methods. This means that it is not possible to point out any significant difference with respect to the identified hazard types. However, it can be observed that none of the methods in the study was effective enough to find all identified hazards, which means that they complemented each other well in that study.

3 Conclusion

We summarized the paper 'Comparison of the FMEA and STPA safety analysis methods–a case study' [Su17] that was published as an article in the Software Quality Journal. In the future, additional empirical studies (especially case studies and experiments) are needed in order to investigate differences, but also combinations of the methods and possible extensions of FMEA and STPA. In addition, safety has been defined as an important risk driver for testing, but the number of risk-based testing approaches taking safety analysis into account is limited. Comparing different safety analysis methods like FMEA and STPA with respect to test planning, design, execution and evaluation is another suggested topic for further research that could help to increase adoption of safety analysis methods for risk-based testing.

References

[Le04] Leveson, Nancy G: A systems-theoretic approach to safety in software-intensive systems. IEEE Transactions on Dependable and Secure computing, 1(1):66–86, 2004.

[St03] Stamatis, Dean H: Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press, 2003.

[Su17] Sulaman, Sardar Muhammad; Beer, Armin; Felderer, Michael; Höst, Martin: Comparison of the FMEA and STPA safety analysis methods–a case study. Software Quality Journal, pp. 1–39, 2017. online first at https://doi.org/10.1007/s11219-017-9396-0.