53rd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Quality and Safety, always a beginning! (1)

Author: Mr. Akram Abdellatif
German Aerospace Centre (DLR), Germany, akram.abdellatif@dlr.de

Ms. Aya Mamdoh Mohamed Mostafa
Technical University of Munich, Egypt, ayamamdoh653@gmail.com
Mr. Abdelrahman Ouda
Technical University of Munich, Germany, Abdelrahmanhassanouda@gmail.com
Mr. Fady Saweeres
Technical University of Munich, Egypt, fadysaweeres@gmail.com
Prof. Florian Holzapfel
Technical University of Munich, Germany, florian.holzapfel@tum.de

A NEW COMPLETE SOLUTION TO EFFICIENTLY UTILIZE MODEL BASED SAFETY ANALYSIS (MBSA) TO EVALUATE AEROSPACE SYSTEMS

Abstract

Aerospace systems became very complex in the last years which made classic safety analysis methods unfit to handle them. Model-Based Safety Analysis (MBSA) is an approach in which design and safety engineers share a common system model created using a Mode Based Object-Oriented development process. MBSA intends to act as a bridge between design engineers and safety engineers reducing the time required to verify the safety of a new designed system The work in [1] represented a new prototype for a safety analysis tool utilizing the MBSA approach. Although the tool has shown decent results with various systems, but an exclusive qualitative tool requires high computational power for complicated systems with large number of components and sometimes the system can be unsolvable. The work in [2] introduced the addition of quantitative analysis methods to the MBSA tool. The extension of the components or system models by their failure probabilities gives the opportunity to solve complicated systems by neglecting failures of low probabilities. This paper introduces the full solution of the tool combining various algorithms and techniques such as Back Tracking Constraint Satisfaction Problems (CSP) and Markov Chains. The developed tool also introduces the STPA (System-Theoretic Process Analysis) technique to capture all unsafe scenarios even those that are not related to component failures. The user-friendly tool combines all various techniques to solve complicated systems. The tool is also developed under the assumption of the user not being an expert in MBSA tools or software programming. The tool will be tested on various systems and analyzed with comparison of classic analysis methods or with other MBSA tools. In conclusion, the complete tool will be evaluated if it could be an efficient solution to handle complex aerospace systems and replace the classic safety analysis methods.

[1] Akram Amin Abdellatif and Florian Holzapfel. "New methodology for model- based safety analysis". 2019 IEEE Aerospace Conference.

[2] Akram Amin Abdellatif and Florian Holzapfel. "Model-Based Safety Analysis (MBSA) Methods in Aerospace Applications". International Astronautical Congress 2019.