HAZARD ANALYSIS FOR THE REQUIREMENTS SPECIFICATION OF SAFETY-CRITICAL SYSTEMS USING THE COMBINATION OF FHA AND FTA TECHNIQUES

KIRIYADHATSHINI A/P GUNARATNAM

MASTER OF SCIENCE

UNIVERSITI MALAYSIA PAHANG

Universiti Malaysia PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis, and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

____

(Supervisor's Signature)

Full Name : TS. AZMA BINTI ABDULLAH

Position : LECTURER

Date : 30/8/2023

UMP
Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

STUDENT’S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

____

(Student’s Signature)

Full Name : KIRIYADHATSHINI A/P GUNARATNAM
ID Number : MCS19001
Date : 30/8/2023

HAZARD ANALYSIS FOR THE REQUIREMENTS SPECIFICATION OF SAFETY-CRITICAL SYSTEMS USING THE COMBINATION OF FHA AND FTA TECHNIQUES

KIRIYADHATHINI A/P GUNARATNAM

A thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

AUGUST 2023

ACKNOWLEDGEMENTS

As a master's student, completing this thesis has been made possible with the help of The Almighty, who has given me wisdom, health, strength, and patience, and through the encouragement, support, and guidance of many individuals.

First and foremost, truly and honestly, this journey would not behave en achieved without two individuals who have patiently supported and continuously encouraged me to finish this work. From the bottom of my heart, I would like to express my deepest appreciation to my main supervisor, Ts. Azma Binti Abdullah, for her wonderful guidance, insights, and words of motivation. Also, I thank my senior lecturers, Associate Professor Dr. Rohani Binti Abu Bakar, Dr. Zalili, Dr. Noorlin, and Dr. Fadhl Hujainah, for their generous and patient reviews, comments, and thoughtful suggestions to improve this thesis. I am forever grateful to have met all of them and been allowed to work with them.

I would like to dedicate these years of hard work to my family members: my mother, Thanaletchmi Kanthan; my aunt, Puspavalli Apparsamy; my grandmother, Thanalatchmy Munusamy; my sister, Mirashini Gunaratnam; and my brother-in-law, Johnathan Yap, for their endless support, patience, and prayers.

My sincere gratitude to my mentors, Dr. Mohd Khairul Nizam bin Zainan Nazri and Dr. Mardiana Binti Mat Ishak, for guiding me to love this master's journey and the process of thesis management and for guiding me to go further in my life. I would like to extend my special thanks to Ms. Izzati Husna, who has helped me greatly in applying formal method elements to my thesis.

My heartfelt gratitude goes to my friend, Jayabharthy and her family, for taking care of me by providing me accommodation when needed and the support I received throughout my thesis preparation phase. A huge thanks also to my wonderful master's and Ph.D. friends, Cik. Nik Zuliani, Pn. Maznah Ibrahim, Pn. Mayamin Yuhaniz, Cik. Norliana, Pn. Shimo Osman, and Dato' Dania Irfan, who never failed to keep supporting and offering hands throughout my thesis journey. It has been a great pleasure to receive help from wonderful guides on this journey: Dr. Zati Yusnira, Dr. Shuhaida Hanim, Ustaz Fahmi, and Dr. Hidayah Ahmad Azam.

I would like to acknowledge the Institute of Postgraduate Studies (IPS) of UMP and the Faculty of Computing and Software Engineering, the dean of the faculty, the deputy deans, and all the supporting and technical staff for their assistance and for making the procedures clear and smooth to complete this work.

ABSTRAK

Analisis Bahaya (HA) adalah proses penting untuk mengenal pasti dan mengurangkan risiko yang berkaitan dengan pembangunan sistem. Walau bagaimanapun, teknik HA semasa mempunyai beberapa kekurangan, termasuk kurangnya pengenalpastian bahaya awal dan dokumen bahaya yang tidak mencukupi, yang boleh menyebabkan keruntuhan sistem. Oleh itu, penyelidikan ini bertujuan untuk meningkatkan teknik HA dengan menangani kekurangan ini dengan menjalankan HA pada peringkat keperluan dan menghasilkan log bahaya yang lebih komprehensif. Untuk mencapai tujuan ini, metodologi penyelidikan yang terdiri daripada tiga fasa telah direka. Fasa 1 melibatkan analisis teknik HA sedia ada dan mengenalpasti kesenjangan dalam analisis bahaya. Fasa 2 melibatkan pembangunan teknik analisis bahaya gabungan yang menangani kekurangan utama ini dengan menggabungkan teknik analisis bahaya fungsional (FHA) dan analisis pepohonan kegagalan (FTA). Teknik yang dicadangkan dimaksudkan untuk digunakan semasa peringkat keperluan pembangunan sistem untuk menghasilkan log bahaya yang lebih komprehensif. Dalam Fasa 3, teknik yang dicadangkan dinilai melalui kajian kes model pam analgesia pesakit generik yang dikawal. Prestasi teknik yang dicadangkan dinilai menggunakan ukuran F1-score, ketepatan, dan ketepatan yang tepat. Empat kaedah penilaian digunakan untuk membandingkan hasil FHA tunggal, FTA tunggal, menggunakan FHA dan FTA, dan menggabungkan teknik FHA dan FTA. Hasil menunjukkan bahawa teknik FHA dan FTA yang digabungkan mencapai nilai prestasi tertinggi 0.96 untuk ketepatan dan 0.98 untuk ketepatan, pengingatan, dan ukuran F1-score. Ini menyimpulkan bahawa walaupun secara individu FHA menghasilkan data keluaran yang besar sementara FTA bukan teknik awal tetapi kedua-duanya melengkapkan satu sama lain untuk mencapai tujuan menjalankan HA pada peringkat keperluan dan menghasilkan log bahaya yang minimal dan komprehensif. Berdasarkan hasil ini, teknik FHA dan FTA yang digabungkan disarankan untuk dilaksanakan semasa peringkat keperluan pembangunan sistem untuk mengenal pasti bahaya dan menghasilkan log bahaya yang komprehensif. Arahan masa depan untuk penyelidikan boleh merangkumi mengautomatiskan teknik untuk mengenal pasti bahaya dengan menganalisis fungsi sistem menggunakan faktor kausal dalam bentuk pemboleh ubah.

ABSTRACT

Hazard Analysis (HA) is a crucial process for identifying and mitigating risks associated with systems development. However, current HA techniques suffer from several limitations, including a lack of preliminary hazard identification and inadequate hazard documentation, which can lead to system breakdowns. Therefore, this research aims to enhance HA techniques by addressing these limitations by conducting HA in requirement specification and producing a more comprehensive hazard log. To achieve this aim, a research methodology consisting of three phases was designed. Phase 1 involved analyzing existing HA techniques and identifying gaps in hazard analysis. Phase 2 involved developing a combined hazard analysis technique that addresses these key limitations by integrating functional hazard analysis (FHA) and fault tree analysis (FTA) techniques. The proposed technique is intended for use during the requirement specification of system development to produce a comprehensive hazard log. In Phase 3, the proposed technique was evaluated through a case study of a generic patient-controlled analgesia pump model. The performance of the proposed technique was evaluated using the F1-score measure, precision, and accuracy. Four evaluation methods were used to compare the results of single FHA, single FTA, using both FHA and FTA, and combining FHA and FTA techniques. The results showed that the combined FHA and FTA technique achieved the highest performance value of 0.96 for accuracy and 0.98 for precision, recall, and F1-score measure. This concludes that though individually FHA produces a large output data while FTA is not a preliminary technique yet both of them complements each other to achieve the aim of conducting HA in requirement specification and produce a minimalized and comprehensive hazard log. Based on these findings, the combined FHA and FTA technique is recommended for implementation during the requirement specification of systems development to identify hazards and produce a comprehensive hazard log. Future directions for research could include automating the technique to identify hazards by analyzing system functions using the causal factors in terms of variables.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

REFERENCES

Abdullah, A. B., & Liu, S. (2013). Hazard analysis for safety-critical systems using SOFL. *Proceedings of the 2013 IEEE Symposium on Computational Intelligence for Engineering Solutions, CIES 2013 - 2013 IEEE Symposium Series on Computational Intelligence, SSCI 2013*, 133–140. https://doi.org/10.1109/CIES.2013.6611740

Aleixo, O., & Rocha, C. (2022). Adapting a system-theoretic hazard analysis method for interoperability of information systems in health care. Retrieved from https://dspace.library.uvic.ca/handle/1828/13871

Alexander, R., & Kelly, T. (2013). Supporting systems of systems hazard analysis using multi-agent simulation. *Safety Science*, *51*(1), 302–318. https://doi.org/10.1016/j.ssci.2012.07.006

Asare, P., Lach, J., & Stankovic, J. A. (2013). FSTPA-I: A Formal Approach to Hazard Identification via System Theoretic Process Analysis. *2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, 150. https://doi.org/10.1145/2502524.2502545

Averett, M. W. (1988). Fault Tree Analysis. *Risk Analysis*, *8*(3), 463–464. https://doi.org/10.1111/j.1539-6924.1988.tb00510.x

B, P. M., Zhang, Y., & Jones, P. (2017). A Hazard Analysis Method for Systematic Identification of Safety Requirements for User, *1*, 284–299. https://doi.org/10.1007/978-3-319-66197-1

Baig, A. A., Ruzli, R., & Buang, A. B. (2013). Reliability Analysis Using Fault Tree Analysis: A Review. *International Journal of Chemical Engineering and Applications*, *4*(3), 169–173. https://doi.org/10.7763/ijcea.2013.v4.287

Banghart, M., & Fuller, K. (2014). Utilizing confidence bounds in Failure Mode Effects Analysis (FMEA) Hazard Risk Assessment. *IEEE Aerospace Conference Proceedings*, 1–6. https://doi.org/10.1109/AERO.2014.6836222

Baybutt, P. (2014). Requirements for improved process hazard analysis (PHA) methods. *Journal of Loss Prevention in the Process Industries*, *32*, 182–191. https://doi.org/10.1016/j.jlp.2014.08.004

Baybutt, P. (2015). Competency requirements for process hazard analysis (PHA) teams. *Journal of Loss Prevention in the Process Industries*, *33*, 151–158. https://doi.org/10.1016/j.jlp.2014.11.023

Burney, S. M., & Saleem, H. (2008). INDUCTIVE & DEDUCTIVE RESEARCH APPROACH Hussain Saleem Assistant Professor. *Lecture Delivered On*, (March), 6–9.

Burns, D. J., & Pitblado, R. M. (1993). A Modified Hazop Methodology For Safety Critical System Assessment. *Directions in Safety-Critical Systems*, 232–245. https://doi.org/10.1007/978-1-4471-2037-7_15

Cha, S., Taylor, R. N., & Kang, K. (2019). *Handbook of software engineering*. *Handbook of Software Engineering*. https://doi.org/10.1007/978-3-030-00262-6

Chartres, N., Bero, L. A., & Norris, S. L. (2019). A review of methods used for hazard identification and risk assessment of environmental hazards. *Environment International*, *123*, 231–239. https://doi.org/10.1016/J.ENVINT.2018.11.060

Chazette, L., Brunotte, W., & Speith, T. (2021). Exploring Explainability: A Definition, a Model, and a Knowledge Catalogue. *Proceedings of the IEEE International Conference on Requirements Engineering*, 197–208. https://doi.org/10.1109/RE51729.2021.00025

Cheng, H., Zhu, L., & Meng, J. (2022). Fuzzy evaluation of the ecological security of land resources in mainland China based on the Pressure-State-Response framework. *Science of The Total Environment*, *804*, 150053. https://doi.org/10.1016/J.SCITOTENV.2021.150053

Daramola, O., Stålhane, T., Sindre, G., & Omoronyia, I. (2011). Enabling hazard identification from requirements and reuse-oriented HAZOP analysis. *2011 4th International Workshop on Managing Requirements Knowledge, MaRK'11 - Part of the 19th IEEE International Requirements Engineering Conference, RE'11*, 3–11. https://doi.org/10.1109/MARK.2011.6046555

Dokas, I. M., Feehan, J., & Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science*, *58*, 11–26. https://doi.org/10.1016/j.ssci.2013.03.013

Du, J., Wang, J., & Feng, X. (2014). A safety requirement elicitation technique of safety-critical system based on scenario. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8588 LNCS*, 127–136. https://doi.org/10.1007/978-3-319-09333-8_15

Duan, J. (2022). Improved Systemic Hazard Analysis Integrating with Systems Engineering Approach for Vehicle Autonomous Emergency Braking System. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, *8*(3). https://doi.org/10.1115/1.4051780/1114604

Dunjó, J., Fthenakis, V., Vílchez, J. A., & Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials*, *173*(1–3), 19–32. https://doi.org/10.1016/j.jhazmat.2009.08.076

Ferris, I. M. (2022). 10. Hazard analysis and critical control points (HACCP). *Applied Food Science*, 187–213. https://doi.org/10.3920/978-90-8686-933-6_10

Foster, N., & Jacob, J. (2002). Hazard Analysis for Security Protocol Requirements, 75–92. https://doi.org/10.1007/0-306-46958-8_6

Frank, S., Hakamian, A., Wagner, L., Kesim, D., Zorn, C., von Kistowski, J., & van Hoorn, A. (2022). Interactive Elicitation of Resilience Scenarios Based on Hazard Analysis Techniques. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in*

Bioinformatics), 13365 LNCS, 229–253. https://doi.org/10.1007/978-3-031-15116-3_11/COVER

Gharib, M., & Bondavalli, A. (2019). On the evaluation measures for machine learning algorithms for safety-critical systems. *Proceedings - 2019 15th European Dependable Computing Conference, EDCC 2019*, (September), 141–144. https://doi.org/10.1109/EDCC.2019.00035

Gleirscher, M. (2013). Hazard analysis for technical systems. *Lecture Notes in Business Information Processing, 133 LNBIP*, 104–124. https://doi.org/10.1007/978-3-642-35702-2_8

Golabi, A., Erradi, A., & Tantawy, A. (2022). Towards automated hazard analysis for CPS security with application to CSTR system. *Journal of Process Control*, *115*, 100–111. https://doi.org/10.1016/J.JPROCONT.2022.04.008

Graubohm, R., Stolte, T., Bagschik, G., & Maurer, M. (2020). Towards Efficient Hazard Identification in the Concept Phase of Driverless Vehicle Development. *IEEE Intelligent Vehicles Symposium, Proceedings*, 1297–1304. https://doi.org/10.1109/IV47402.2020.9304780

Gray, A., Wimbush, A., de Angelis, M., Hristov, P. O., Calleja, D., Miralles-Dolz, E., & Rocchetta, R. (2022). From inference to design: A comprehensive framework for uncertainty quantification in engineering with limited information. *Mechanical Systems and Signal Processing*, *165*. https://doi.org/10.1016/J.YMSSP.2021.108210

Grunske, L., Lindsay, P., Yatapanage, N., & Winter, K. (2005). An automated failure mode and effect analysis based on high-level design specification with behavior trees. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3771 LNCS*, 129–149. https://doi.org/10.1007/11589976_9

Guiochet, J. (2016). Hazard analysis of human-robot interactions with HAZOP-UML. *Safety Science*, *84*, 225–237. https://doi.org/10.1016/j.ssci.2015.12.017

Guo, H., Su, G., Jia, Y., Feng, G., Zhou, R., & Wang, Y. (2019). A systemic approach to hazard analysis and control based on energy function. *Proceedings of 2018 IEEE International Conference of Safety Produce Informatization, IICSPI 2018*, 20–25. https://doi.org/10.1109/IICSPI.2018.8690482

Han, X., & Zhang, J. (2013). A combined analysis method of FMEA and FTA for improving the safety analysis quality of safety-critical software. *Proceedings - 2013 IEEE International Conference on Granular Computing, GrC 2013*, 353–356. https://doi.org/10.1109/GrC.2013.6740435

Häring, I. (2021). Introduction to System Analysis Methods. *Technical Safety, Reliability and Resilience*, 57–69. https://doi.org/10.1007/978-981-33-4272-9_5

Heimdahl, M. P. E. (2007). Safety and software intensive systems: Challenges old and new. *FoSE 2007: Future of Software Engineering*, 137–152. https://doi.org/10.1109/FOSE.2007.18

Henderson, M. C. (1989). A comparison of two approaches to empathy training. *Nurse Educator*, *14*(1), 423–437. https://doi.org/10.1097/00006223-198901000-00007

Horn, D., Ali, N., & Hong, J. E. (2019). Towards Enhancement of Fault Traceability Among Multiple Hazard Analyses in Cyber-Physical Systems. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, *2*(July), 458–464. https://doi.org/10.1109/compsac.2019.10249

Huang, Z., Zhang, D., Pitilakis, K., Tsinidis, G., Huang, H., Zhang, D., & Argyroudis, S. (2022). Resilience assessment of tunnels: Framework and application for tunnels in alluvial deposits exposed to seismic hazard. *Soil Dynamics and Earthquake Engineering*, *162*, 107456. https://doi.org/10.1016/J.SOILDYN.2022.107456

Jain, P., Rogers, W. J., Pasman, H. J., Keim, K. K., & Mannan, M. S. (2018). A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer. *Process Safety and Environmental Protection*, *116*, 92–105. https://doi.org/10.1016/j.psep.2018.01.016

Jain, P., Rogers, W. J., Pasman, H. J., & Mannan, M. S. (2018). A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. *Process Safety and Environmental Protection*, *118*, 115–124. https://doi.org/10.1016/j.psep.2018.06.037

Kamaraj, A. V., Domeyer, J. E., & Lee, J. D. (2021). Hazard Analysis of Action Loops for Automated Vehicle Remote Operation. *Undefined*, *65*(1), 732–736. https://doi.org/10.1177/1071181321651022

Kariuki, S. G., & Löwe, K. (2007). Integrating human factors into process hazard analysis. *Reliability Engineering and System Safety*, *92*(12), 1764–1773. https://doi.org/10.1016/j.ress.2007.01.002

Kitchenham Barbara, and S. C. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical Report*, *Ver. 2.3 EBSE Technical Report. EBSE*.

Knight, J. C. (2002a). Safety critical systems: Challenges and directions. *Proceedings - International Conference on Software Engineering*, 547–550. https://doi.org/10.1109/icse.2002.1007998

Knight, J. C. (2002b). Safety critical systems: Challenges and directions. *Proceedings - International Conference on Software Engineering*, 547–550. https://doi.org/10.1109/icse.2002.1007998

Krishnan, R., & Bhada, S. V. (2020). An Integrated System Design and Safety Framework for Model-Based Safety Analysis. *IEEE Access*, *8*, 146483–146497. https://doi.org/10.1109/ACCESS.2020.3015151

Kritzinger, D. (2017a). *Fault tree analysis BS EN 61025*. *Aircraft System Safety* (Vol. 3). https://doi.org/10.1016/B978-0-08-100889-8.00004-0

Kritzinger, D. (2017b). Functional Hazard Analysis. *Aircraft System Safety*, 37–57. https://doi.org/10.1016/b978-0-08-100889-8.00003-9

Kubai, E. (2019). Reliability and Validity of Research Instruments Correspondence to kubaiedwin@yahoo.com. *Critical Analysis Ofpolicies on Special Education in Kenya*, 1–9.

Kuo, D.-H., Hsu, D.-S., Chang, C.-T., & Chen, D.-H. (1997). Prototype for intergated hazard analysis. *AIChE Journal*, *43*(6), 1494–1510. https://doi.org/10.1002/aic.690430613

Kural 435, குறள் 435, The Correction of Faults, குற்றங்கடிதல், Chapter: 44,பொருட்பால்,Wealth,Thirukural,திருக்குறள்,திருவள்ளுவர்,thiruvalluvar,tamil,english translation,transliteration. (n.d.). Retrieved 17 November 2022, from https://www.ytamizh.com/thirukural/kural-435/

Laufenberg, X. (1995). Modeling and Model-Based Analysis for Safety and Hazard Analysis. *IFAC Proceedings Volumes*, *28*(25), 263–268. https://doi.org/10.1016/s1474-6670(17)44854-3

Lawrence, J. D., & Gallagher, J. M. (1997). A proposal for performing software safety hazard analysis. *Reliability Engineering and System Safety*, *55*(3), 267–282. https://doi.org/10.1016/S0951-8320(96)00098-1

Li, W., & Zhang, H. (2011). A software hazard analysis method for automotive control system. *Proceedings - 2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE 2011*, *3*, 744–748. https://doi.org/10.1109/CSAE.2011.5952781

Liu, H. C., Chen, X. Q., Duan, C. Y., & Wang, Y. M. (2019). Failure mode and effect analysis using multi-criteria decision making methods: A systematic literature review. *Computers and Industrial Engineering*, *135*(October 2018), 881–897. https://doi.org/10.1016/j.cie.2019.06.055

Maier, T. (1997). FMEA and FTA to Support Safe Design of Embedded Software in Safety-Critical Systems. *Safety and Reliability of Software Based Systems*, (C), 351–367. https://doi.org/10.1007/978-1-4471-0921-1_22

Marcus, A., Cardei, I., & Alsenas, G. (2013). Automation of the SHIELD methodology for system hazard analysis and resilient design. *SysCon 2013 - 7th Annual IEEE International Systems Conference, Proceedings*, 894–901. https://doi.org/10.1109/SysCon.2013.6549990

Mauborgne, P., Deniaud, S., Levrat, E., Bonjour, E., Micaëlli, J. P., & Loise, D. (2016). Operational and System Hazard Analysis in a Safe Systems Requirement Engineering Process - Application to automotive industry. *Safety Science*, *87*, 256–268. https://doi.org/10.1016/j.ssci.2016.04.011

Medikonda, B. S., & Panchumarthy, S. R. (2008). A framework for software safety in safety-critical systems. *SoMeT_08 - The 7th International Conference on Software Methodologies, Tools and Techniques*, *34*(2), 1–9. https://doi.org/10.1145/1507195.1507207

Mohseni, S., Block, J. E., & Ragan, E. (2021). Quantitative Evaluation of Machine

Learning Explanations: A Human-Grounded Benchmark. *International Conference on Intelligent User Interfaces, Proceedings IUI*, 22–31. https://doi.org/10.1145/3397481.3450689

Muller, M., Roth, M., & Lindemann, U. (2016). The hazard analysis profile: Linking safety analysis and SysML. *10th Annual International Systems Conference, SysCon 2016 - Proceedings*. https://doi.org/10.1109/SYSCON.2016.7490532

Niu, H., Ma, C., Wang, C., & Han, P. (2019). Hazard Analysis of Traffic Collision Avoidance System Based on STAMP Model. *Proceedings of the 2018 IEEE International Conference on Progress in Informatics and Computing, PIC 2018*, 445–450. https://doi.org/10.1109/PIC.2018.8706283

O'Connell, D., Thomas, D. H., Lewis, J. H., Hasse, K., Santhanam, A., Lamb, J. M., … Low, D. A. (2019). Safety-oriented design of in-house software for new techniques: A case study using a model-based 4DCT protocol. *Medical Physics*, *46*(4), 1523–1532. https://doi.org/10.1002/MP.13386

Oh, H.-J., & Hong, J.-P. (2012). A Study of Software Hazard Analysis for Safety Critical Function in Military Aircraft. *Journal of IKEEE*, *16*(2), 145–152. https://doi.org/10.7471/ikeee.2012.16.2.145

Ortmeier, F. (2014). Deductive Cause-Consequence Analysis (DCCA), (January 2006).

Paneerselvam, A., & Yamat, H. (2021). Validity and Reliability Testing of the Adapted Foreign Language Classroom Anxiety Scale (FLCAS). *International Journal of Academic Research in Business and Social Sciences*, *11*(4). https://doi.org/10.6007/IJARBSS/V11-I4/9027

Pereira, D. P., Hirata, C., & Nadjm-Tehrani, S. (2019). A STAMP-based ontology approach to support safety and security analyses. *Journal of Information Security and Applications*, *47*, 302–319. https://doi.org/10.1016/j.jisa.2019.05.014

Pinto, C. A. (2022). Dynamic Modelling for Reliability Analysis of Power Supply Systems in a Large European Hospital by Petri Nets, Fuzzy Inference System, Stochastic or Markov Chains. Retrieved from https://estudogeral.sib.uc.pt/handle/10316/101753

Popović, V., & Vasić, B. (2008). Review of hazard analysis methods and their basic characteristics. *FME Transactions*, *36*(4), 181–187.

Ribeiro, Q., Pereira, T., Melo, M., Castro, J., Alencar, F., & Lencastre, M. (2021). Toward Requirements for Embedded Systems. *Cadernos Do IME - Série Informática*, *46*(0), 19–41. https://doi.org/10.12957/CADINF.2021.68156

Rong, H., Dong, H., Xu, D., & Chen, Z. (2019). Model based interaction hazards analysis of integrated modular avionics system. *International Conference on Communication Technology Proceedings, ICCT*, *2019–Octob*, 1440–1444. https://doi.org/10.1109/ICCT.2018.8599946

Saad, A., Bal, M., & Khatib, J. (2022). The Need for a Proper Waste Management Plan for the Construction Industry: A Case Study in Lebanon. *Sustainability*

(Switzerland), *14*(19). https://doi.org/10.3390/SU141912783

Sechser, B. (2011). Functional safety - SPICE for professionals? *Communications in Computer and Information Science*, *155 CCIS*, 212–216. https://doi.org/10.1007/978-3-642-21233-8_24/COVER

Simpson, A., & Stoker, J. (2002). Will it be Safe? — An Approach to Engineering Safety Requirements. *Components of System Safety*, 140–164. https://doi.org/10.1007/978-1-4471-0173-4_9

Smith, S. P., & Harrison, M. D. (2005). Measuring reuse in hazard analysis. *Reliability Engineering and System Safety*, *89*(1), 93–104. https://doi.org/10.1016/j.ress.2004.08.010

Song, H., & Schnieder, E. (2018). Evaluating Fault Tree by means of Colored Petri nets to analyze the railway system dependability. *Safety Science*, *110*(September), 313–323. https://doi.org/10.1016/j.ssci.2018.08.017

Subriadi, A. P., & Najwa, N. F. (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon*, *6*(1). https://doi.org/10.1016/J.HELIYON.2020.E03161

Sulaman, S. M., Abbas, T., Wnuk, K., & Höst, M. (2014). Hazard analysis of collision avoidance system using STPA. *ISCRAM 2014 Conference Proceedings - 11th International Conference on Information Systems for Crisis Response and Management*, 424–428.

Sulaman, S. M., Beer, A., Felderer, M., & Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods–a case study. *Software Quality Journal*, *27*(1), 349–387. https://doi.org/10.1007/s11219-017-9396-0

Sun, L., Li, Y. F., & Zio, E. (2022). Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, *8*(3). https://doi.org/10.1115/1.4051940/1115198

Teufel, S. (2014). Lecture 5 : Evaluation.

The Generic Infusion Pump (GIP). (n.d.). Retrieved 18 November 2022, from https://rtg.cis.upenn.edu/gip/

Tian, J., Wu, Y., Wang, X., & Zhao, T. (2011). Hazard analysis based on human-machine-environment coupling. *Proceedings - Annual Reliability and Maintainability Symposium*, 1–7. https://doi.org/10.1109/RAMS.2011.5754444

Törner, F., Johannessen, P., & Öhman, P. (2006). Assessment of hazard identification methods for the automotive domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4166 LNCS*, 247–260. https://doi.org/10.1007/11875567_19

Tran, V. N., Tran, L. V., & Tran, V. N. (2021). Functional hazard analysis for engineering safe software requirements. *Proceedings - 2021 4th International Conference on*

Information and Computer Technologies, ICICT 2021, 142–148. https://doi.org/10.1109/ICICT52872.2021.00031

Vilela, J., Castro, J., Martins, L. E. G., & Gorschek, T. (2017a). Integration between requirements engineering and safety analysis: A systematic literature review. *Journal of Systems and Software*, *125*, 68–92. https://doi.org/10.1016/j.jss.2016.11.031

Vilela, J., Castro, J., Martins, L. E. G., & Gorschek, T. (2017b). Integration between requirements engineering and safety analysis: A systematic literature review. *Journal of Systems and Software*, *125*, 68–92. https://doi.org/10.1016/J.JSS.2016.11.031

Vilela, J., Castro, J., Martins, L. E. G., & Gorschek, T. (2020). Safety Practices in Requirements Engineering: The Uni-REPM Safety Module. *IEEE Transactions on Software Engineering*, *46*(3), 222–250. https://doi.org/10.1109/TSE.2018.2846576

Wang, H., Zhong, D., Zhao, Y., & Sun, R. (2017). A system safety analysis method based on multiple category hazard factors. *Proceedings - 4th International Conference on Dependable Systems and Their Applications, DSA 2017*, *2018–Janua*, 29–34. https://doi.org/10.1109/DSA.2017.14

Wang, R., & Zheng, W. (2013). Research and application of the BFM-STAMP hazard analysis method. *IEEE ICIRT 2013 - Proceedings: IEEE International Conference on Intelligent Rail Transportation*, 174–178. https://doi.org/10.1109/ICIRT.2013.6696289

Wei, X., Dong, Y., Li, X., & Wong, W. E. (2018). Architecture-level hazard analysis using AADL. *Journal of Systems and Software*, *137*, 580–604. https://doi.org/10.1016/j.jss.2017.06.018

Xiao, M. rui, Dong, Y. wei, Gou, Q. wen, Xue, F., & Chen, Y. hua. (2020). Architecture-level particular risk modeling and analysis for a cyber-physical system with AADL. *Frontiers of Information Technology and Electronic Engineering*, *21*(11), 1607–1625. https://doi.org/10.1631/FITEE.2000428

Yang, S., & Chung, P. W. H. (1998). Hazard analysis and support tool for computer controlled processes. *Journal of Loss Prevention in the Process Industries*, *11*(5), 333–345. https://doi.org/10.1016/S0950-4230(98)00012-6

Yang, S. H., & Chung, P. W. H. (1998). Life cycle hazard analysis for computer controlled processes. *Computers and Chemical Engineering*, *22*(SUPPL.1). https://doi.org/10.1016/s0098-1354(98)00091-x

Yuan, C., Cui, H., Tao, B., & Wang, W. (2018). Fault Tree Analysis for Emergency Process of Fire Accident in Oil-Gas Storage and Transportation. *Journal of Hazardous, Toxic, and Radioactive Waste*, *22*(3), 04018011. https://doi.org/10.1061/(asce)hz.2153-5515.0000402

Zahabi, M., & Kaber, D. (2019). A fuzzy system hazard analysis approach for human-in-the-loop systems. *Safety Science*, *120*(April), 922–931.

https://doi.org/10.1016/j.ssci.2019.08.029

Zhang, Y., Dong, C., Guo, W., Dai, J., & Zhao, Z. (2022). Systems theoretic accident model and process (STAMP): A literature review. *Safety Science*, *152*, 105596. https://doi.org/10.1016/J.SSCI.2021.105596

Zhang, Y., Jones, P. L., & Jetley, R. (2010). A Hazard Analysis for a Generic Insulin Infusion Pump. *Journal of Diabetes Science and Technology*, *4*(2), 263. https://doi.org/10.1177/193229681000400207

Zhao, L., Alhoshan, W., Ferrari, A., Letsholo, K. J., Ajagbe, M. A., Chioasca, E. V., & Batista-Navarro, R. T. (2021). Natural Language Processing for Requirements Engineering. *ACM Computing Surveys (CSUR)*, *54*(3). https://doi.org/10.1145/3444689

Zhou, J., Hanninen, K., Lundqvist, K., & Provenzano, L. (2017). An ontological approach to hazard identification for safety-critical systems. *2017 2nd International Conference on Reliability Systems Engineering, ICRSE 2017*, (Icrse). https://doi.org/10.1109/ICRSE.2017.8030746

Zhou, J., Hänninen, K., Lundqvist, K., & Provenzano, L. (2018). An ontological approach to identify the causes of hazards for safety-critical systems. *2017 2nd International Conference on System Reliability and Safety, ICSRS 2017*, *2018–Janua*, 405–413. https://doi.org/10.1109/ICSRS.2017.8272856

Zhu, D., Tan, H., & Yao, S. (2018). Petri Nets-based method to elicit component-interaction related safety requirements in safety-critical systems. *Computers and Electrical Engineering*, *71*(May), 162–172. https://doi.org/10.1016/j.compeleceng.2018.07.019

Zhu, D., & Yao, S. (2019). A Hazard Analysis Method for Software-Controlled Systems Based on System-Theoretic Accident Modeling and Process. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, *2018–Novem*, 90–95. https://doi.org/10.1109/ICSESS.2018.8663927

Zikrullah, N. A., Kim, H., van der Meulen, M. J. P., Skofteland, G., & Lundteigen, M. A. (2021). A comparison of hazard analysis methods capability for safety requirements generation. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *235*(6), 1132–1153. https://doi.org/10.1177/1748006X211003463