2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS) | 979-8-3503-1093-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSECS58457.2023.10256294

Safety Property Attributes in Critical Systems for Requirement Specification: A Review

Azma Abdullah *
Faculty of Computing
University Malaysia Pahang Al-Sultan Abdullah (UMPSA)
Pahang, Malaysia
azma@ump.edu.my

Rohani Abu Bakar
Faculty of Computing
University Malaysia Pahang Al-Sultan Abdullah (UMPSA)
Pahang, Malaysia
rohani@ump.edu.my

Kiriyadhatshini a/p Gunaratnam
Faculty of Computing
University Malaysia Pahang Al-Sultan Abdullah (UMPSA)
Pahang, Malaysia
kiriya@ump.edu.my

Fadhl Hujainah
Volvo Car Corporation
Sweden
Fadhl.hujainah@volvocars.com

Mohd Fairus Abdul Farid
Malaysia Nuclear Agency
Malaysia
m_fairus@nuclearmalaysia.gov.my

***Abstract*—The integration of critical system components, requirement specification, and safety properties plays a crucial role in advancing the development and verification processes of critical systems. This integration enables effective analysis, management of safety requirements, and identification of potential risks. Although several studies have explored safety properties in safety analysis (SA), they often lack a comprehensive presentation of all possible safety properties with proper categorization. This paper aims to address this gap by analyzing a comprehensive list of possible safety properties in requirement specification. The list is derived through an extensive analysis of studies published between 2019 and 2023, with a focus on past researchers' contributions. Additionally, our future work includes a systematic literature review encompassing a broader range of studies to further enhance the analysis. By providing a structured approach for addressing safety aspects, this paper contributes valuable insights into the significance of safety properties in ensuring the safety and reliability of critical systems. It lays the foundation for improved safety analysis (SA) practices and strengthens the overall development process of critical systems.**

Keywords*—*safety critical system, safety analysis, requirement specification, safety property, safety attributes

I. Introduction

Critical systems are characterized by their potential impact on human lives and the environment, as well as the severe consequences that may arise from their failure [1]. Examples include flight control systems, medical devices used in healthcare settings, autonomous vehicles, and nuclear power plant control systems. The complexity and significance of these systems necessitate rigorous analysis and adherence to stringent safety standards [2].

Requirement specification in critical systems represents the desired functionalities, constraints, and performance objectives of the critical system are defined. Comprehensive requirement specification ensures the capture of stakeholders' expectations and compliance with regulatory standards which facilitates a clear understanding of the system's intended behavior, promoting effective communication among designers, developers, and end-users [3][4].

Safety property attributes ensure that critical systems operate within predefined safety boundaries and comply with industry-specific regulations [5]. By incorporating safety considerations throughout the development lifecycle, potential failures can be systematically addressed, and risks associated with critical system operations can be minimized [6].

Unfortunately, a comprehensive analysis by the authors of this paper reveals that not all potential safety properties have been adequately addressed, as depicted in Table II. For instance, among the 24 studies analyzed, only 16 papers have made mention of failure. Consequently, the primary objective of this paper is to collate all dispersed safety properties and systematically classify them into eight distinct categories, namely, time constraint (TC), functional behavior (FB), input and output devices (IOD), safety standard (SS), prior knowledge (PK), environment (E), domain (D), and failure characteristic (FC). The ensuing section, Section II presents the research background, Section III presents research methodology, Section IV, presents the findings and discussion with a detailed exposition of each research questions, and ends with Section V which concludes this paper for its aim and findings.

II. Research Background

Previous studies have come up with models, frameworks, and techniques to conduct SA by considering safety properties.

For an instance, Kumar et al. [7] has discussed about have constructing a state-space model-based framework aimed at assessing reliability during the early stages of system development. The primary objective of this framework is to mitigate losses incurred as a result of system failure subsequent to installation. Additionally, this study emphasizes the significance of conducting SA during the architectural design phase for systems subject to Safety Critical Computer Systems (SCCS). By incorporating safety considerations early on, potential issues can be effectively identified and addressed prior to the testing and operational phases, ensuring a more robust and secure system overall.