World Academy of Science, Engineering and Technology
International Journal of Industrial and Systems Engineering
Vol:16, No:06, 2022

Towards Safety-Oriented System Design: Preventing Operator Errors by Scenario-Based Models

Authors : Avi Harel

Abstract : Most accidents are commonly attributed in hindsight to human errors, yet most methodologies for safety focus on technical issues. According to the Black Swan theory, this paradox is due to insufficient data about the ways systems fail. The article presents a study of the sources of errors, and proposes a methodology for utility-oriented design, comprising methods for coping with each of the sources identified. Accident analysis indicates that errors typically result from difficulties of operating in exceptional conditions. Therefore, following STAMP, the focus should be on preventing exceptions. Exception analysis indicates that typically they involve an improper account of the operational scenario, due to deficiencies in the system integration. The methodology proposes a model, which is a formal definition of the system operation, as well as principles and guidelines for safety-oriented system integration. The article calls to develop and integrate tools for recording and analysis of the system activity during the operation, required to implement validate the model.

Keywords : accidents, complexity, errors, exceptions, interaction, modeling, resilience, risks
Conference Title : ICSE 2022 : International Conference on Safety Engineering
Conference Location : Oslo, Norway
Conference Dates : June 23-24, 2022

Open Science Index, Industrial and Systems Engineering Vol:16, No:06, 2022 publications.waset.org/abstracts/141005.pdf