Review: The limitations of hazard analysis techniques in safety critical system development

Kiriyadhatshini a/p Gunaratnam[1], Azma binti Abdullah[1]*
[1] Faculty of Computing (FK), Universiti Malaysia Pahang, Malaysia
[*]Corresponding Author: kiriya@ump.edu.my

ABSTRACT

Hazards might lead to major system breakdowns. For instance, it has been known in the US since 2009 that a software flaw led to an underestimation of patients' heart rates. Serious adverse effects have resulted from this. The accident shows how important it is to use hazard analysis (HA) when making safety-critical systems (SCS), because it helps find specific harms, their effects, what causes them, and how dangerous they are. Even though existing HA techniques have been improved, a deeper study reveals that they still face significant obstacles. So, the point of this research is to bring attention to the problems with more HA techniques. Researchers and practitioners could use this kind of research to learn more about the limitations of the methods and make HA plans that take them into account. The study is carried out in three phases, according to a process-oriented methodology: formulating research questions, locating pertinent studies, and analysing the studies that were located. There are a total of five (5) different sorts of limitations using HA techniques, according to the analysis. These are time-consuming and costly, unable to be conducted in early-stage of HA, unreliable input or output data, require expert participation, unable to detect hazards from multiple components, and controllers. More research is required to identify methods to enhance the HA technique and conduct a case study application and assessment because of the limitations that have been discovered.

KEYWORDS

Safety-critical system;Hazard analysis; Hazard analysis techniques; Significance of hazard analysis

ACKNOWLEDGMENT

This work was supported in part by UMP under [Grant Number = RDU210313]