Safety Science xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

A System-Theoretic Accident Model and Process with Human Factors Analysis and Classification System taxonomy

Michał Lower[a], Jan Magott[a], Jacek Skorupski[b,*]

[a] Wrocław University of Technology, Faculty of Electronics, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
[b] Warsaw University of Technology, Faculty of Transport, Koszykowa 75, 00-662 Warszawa, Poland

ARTICLE INFO

Keywords:
System-Theoretic Accident Model and Process (STAMP)
Human Factors Analysis and Classification System (HFACS)
Causal Analysis using STAMP (CAST)

ABSTRACT

Formal methods are necessary for effective analysis of the causes of complex accidents. One of possibilities is the System-Theoretic Accident Model and Processes (STAMP) using a hierarchical safety control structure for finding control flaws leading to hazards. The aim of this paper is to enhance STAMP error taxonomy by Human Factors Analysis and Classification System (HFACS). The method proposed in this paper is STAMP-HFACS framework for accident analysis. This framework is STAMP structure-driven, i.e. levels of the HFACS structure are incorporated into components of the STAMP safety control structure. A result of the proposed procedure is the STAMP-HFACS diagram. To illustrate the applicability of the method one thread of the Überlingen midair accident was analyzed. The STAMP-HFACS methodology can express interactions between people, technical equipment, and the environment. It is not bound to an incident/accident events chain. It allows for an analysis of a safety-related occurrence focused on finding some adverse relationships between the components, especially at higher levels of the HFACS methodology. Proper recognition of these relationships, and especially their interpretation in system-theoretic terms related to specific components, can be of great importance for increasing the level of air traffic safety.

1. Introduction

Accident models can be classified into three categories: sequential (e.g., Heinrich, 1931), epidemiologic (e.g., Reason, 1990, Shappell et al., 2007) and systemic (e.g., Rasmussen and Svedung, 2000, Hollnagel, 2004, Leveson, 2012). Systematic methods are required in order to find the causes of air traffic events. According to (Leveson, 2012), accidents involve a complex, dynamic process. This process arises in interactions among humans, machines and the environment. CAST (Causal Analysis using STAMP), where STAMP stands for System-Theoretic Accident Model and Processes (Leveson, 2012, CAST, 2013), can be used for incident/accident analysis (to generate plausible scenarios). According to STAMP, system safety is mainly a control problem, not a reliability one, i.e. the system should satisfy safety constraints. A strong feature of STAMP is its safety control structure, e.g. it allows to take into account inter-component interactions by control and feedback. Hence system errors can be identified. STAMP error taxonomy (Stringfellow, 2010, Leveson, 2012) is hierarchical. However, according to (Harris and Li, 2011), the human factors of STAMP are under-specified.

When searching for errors in a concrete system, STAMP error taxonomy can be supported by additional error taxonomy. Taxonomies as contained in Anticipatory Failure Determination (AFD) (Visnepolschi et al., 1999) and Hierarchical Holographic Modeling (Kaplan et al., 2001) may be useful here.

This paper is on air traffic safety. In air transport, human errors occur in more than ⅔ of accidents and incidents. Hence it is reasonable to consider the following question: Can STAMP Error Taxonomy be enhanced by Human Factors Analysis and Classification System (HFACS)? HFACS (Shappell et al., 2007) is one of the most widely used human factors accident analysis frameworks in air, rail, and maritime transport and also in civil engineering. It is based on Reason's "Swiss Cheese" model of human behavior (Reason, 1990) and Rasmussen's human error taxonomy (Rasmussen, 1982). HFACS studies human error at four levels: Unsafe acts, Preconditions for unsafe acts, Unsafe supervision and Organizational influences. Each higher level affects the next downward level. This influence represents not only chains of events; it has recognized statistical dependencies between the levels (Li et al., 2008).

In (Harris and Li, 2011), the authors proposed an extension of the HFACS approach, called HFACS-STAMP, with constraint and control action concepts taken from STAMP. This approach is HFACS structure-

* Corresponding author.
E-mail addresses: michal.lower@pwr.edu.pl (M. Lower), jan.magott@pwr.edu.pl (J. Magott), jsk@wt.pw.edu.pl (J. Skorupski).

https://doi.org/10.1016/j.ssci.2018.04.015
Received 7 November 2016; Received in revised form 3 April 2018; Accepted 21 April 2018

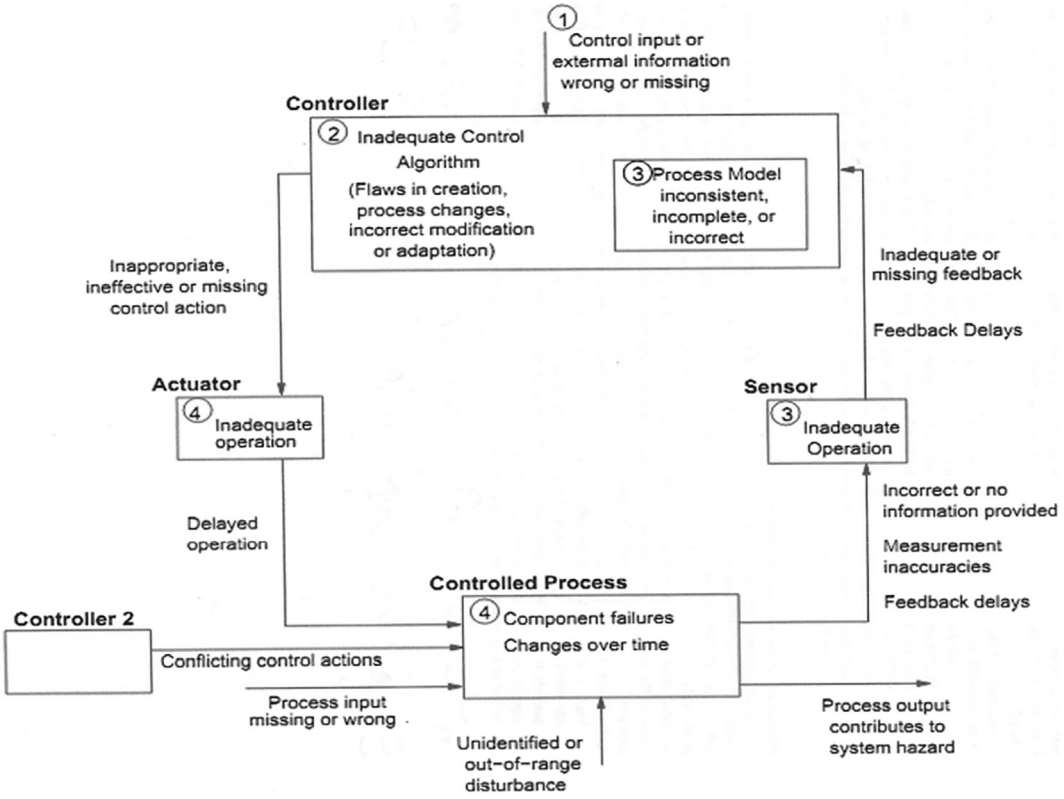

Fig. 1. Classification of control flaws leading to hazards.
Source: Leveson, 2012.

driven. Applying Rasmussen's human mental model to STAMP/STPA is provided in (Hoshino, 2014).

Our approach, as proposed in this paper, is contrary to that of Harris and Li. It is called STAMP-HFACS (Lower et al., 2015). This framework is STAMP structure-driven, i.e. levels of the HFACS structure are incorporated into components of the STAMP safety control structure. The main difference between our STAMP-HFACS and the HFACS-STAMP as created by Harris and Li is that in HFACS-STAMP the levels of HFACS of an organization are not distributed into different components. Hence, in HFACS-STAMP the structure of the system is only partially represented.

In (Luxhoj and Coit, 2006), the authors presented the Aviation Safety Risk Model (ASRM) for risk modeling and analysis. An early version of the ASRM is based on Bayesian Belief Networks (BBN), a BBN extension called influence diagrams, and HFACS. The HFACS is primarily focused on human performance including errors as well as organization failures or deficiencies. For later version of the ASRM (Luxhoj and Oztekin, 2009), authors developed Hazard Classification and Analysis System (HCAS) to address some of the limitations of the HFACS. In (Luxhoj and Oztekin, 2009), the HCAS is Unmanned Aircraft System oriented. The HCAS is based on the Federal Aviation Administration (FAA) regulatory perspective: Aircraft, Airmen, Certification/Airworthiness, Flight Operations. The ASRM is appropriate for Modeling risk in the absence of hard statistical data, e.g. for novel systems. In this case, expert judgements are incorporated into BBN. In (Luxhoj et al., 2017), the ASRM has been used in risk estimation for UAS (Unmanned Aerial System) operations in precision agriculture for targeted aerial application. In STAMP, an emphasis is put on control and feedback between the components, while they are in analysis focus neither in HFACS nor HCAS.

In (Lower et al., 2015), only the outline of STAMP-HFACS methodology is proposed. As an example, a serious air traffic incident of the Runway Incursion Type is analyzed. In this paper, a detailed description of the STAMP-HFACS method is presented. The direct aim of the paper is to present a methodology rather than a comprehensive accident analysis. To show the usefulness of the method, it was applied to an analysis of the Überlingen air traffic accident. Because of its complexity, we propose to split the analysis into threads. The analysis is focused on Tu-154 pilots. Many of the interesting relationships that illustrate our approach to the combined use of STAMP and HFACS can be shown on their example. At the same time, the existing dependencies at all levels of HFACS related to the work of the Tu-154 crew are not so well documented in the literature, where more attention is paid to issues related to the organization of air traffic control. Taking into account the necessity of limiting the size of the paper, only the thread of the incident related to the Tu-154 pilots is presented in more details. The application of the STAMP-HFACS method for multithreading analysis will be the subject of another work.

A suitable software tool is required in order to analyze a complex incident/accident process and to record it. We will show how to represent STAMP-HFACS analysis results in an A-CAST tool (Abdulkhaleq, 2015) which will be a plug-in for XSTAMPP. XSTAMPP is An-eXtensible-STAMP-Platform tool support for safety engineering. Representation of the results in A-CAST was not considered in (Lower et al., 2015).

The rest of the paper is organized as follows. In Section 2 an introduction to STAMP is presented. Section 3 contains a description of HFACS. In Section 4 a description of the proposed STAMP-HFACS framework is given. In Section 5 we describe some aspects of the Überlingen accident in a way that is suitable for STAMP-HFACS application, which is then presented in Section 6. In the next section a representation of the STAMP-HFACS analysis results in the A-CAST tool is described. The last section contains final conclusions and further work plans.