Developing systematic procedures to identify causal factors in Systems Theoretic Process Analysis

John Thomas

Department of Aeronautics and Astronautics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

Abstract: Although recent work has developed systematic procedures and formal methods to help identify unsafe control actions for Systems-Theoretic Process Analysis (STPA) Step 1, the identification of causal factors in STPA Step 2 has received less attention. This research develops additional guidance and procedures that can be used to identify causal factors and build scenarios in STPA Step 2.

1. Introduction

Systems-Theoretic Process Analysis (STPA) is a new hazard analysis technique that addresses many growing causes of accidents including requirements flaws, design errors, complex human behavior, and dysfunctional component interactions as well as traditional component failures [Le12]. Systematic procedures have been defined to identify unsafe control actions in STPA, but the current process for identifying causal factors and scenarios in STPA Step 2 has been less structured and guided mainly by a generic causal factor diagram. Although this process has proven useful in existing applications to date, the results often include substantial repetition and overlap in terms of the identified causal factors. These results indicate that there is an opportunity for improvement if a structured process can be defined to reduce repetition in the analysis while improving consistency among users and ensuring that no factors are overlooked.

2. Case Study

In this research, new procedures are developed and applied to an automotive shift-by-wire example. The shift-by-wire system replaces the traditional shift lever and mechanical cable with electronic actuators and a shift computer. Most manufacturers are now providing or developing similar systems that also utilize the shift computer to incorporate additional functionality and logic to either prevent certain operator shift commands or to automatically issue additional shift commands.

Previous work [Su14] has already identified unsafe control actions and safety constraints for this system using STPA Step 1. STPA Step 2 has also been performed on this system using the traditional approach, although only for a limited scope of the system. In this research, new Step 2 procedures are developed and applied to the same system to enable evaluations of the effectiveness and efficiency of the approaches.

3. Developing a structured process

The proposed new process begins with the safety constraints produced by STPA Step 1. It is hypothesized that beginning with the safety constraints may lead to a more holistic process than beginning separately with unsafe control actions and independently considering actions not followed. However, both approaches are evaluated and considered in this research.

The new procedures structure the STPA Step 2 analysis by first identifying the conditions in the safety constraints from STPA Step 1. For example, an identified safety constraint could be "Train doors must not be opened while train is moving". The two embedded conditions are "train doors are open" and "train is moving". Many of the causal factors in STPA Step 2 will relate to these or similar conditions identified in other safety constraints. For example, process model flaws, inadequate feedback, control algorithm flaws, and the ultimate behavior of the controlled process all relate to the conditions in the safety constraints that must be enforced. The current overlap and inefficiency in STPA Step 2 results may be due to the fact that a single causal factor such as missing position feedback can affect many safety constraints (and unsafe control actions) that reference the same conditions in the system. For example, incorrect feedback that the train is stopped when in fact it is moving could lead to a violation of many safety constraints that all involve the condition "train is moving". By identifying these conditions and using them to structure the Step 2 analysis, there is an opportunity to potentially reduce or avoid repetition while providing additional guidance and procedures for this part of the analysis. There is also a potential to improve the way Step 2 results are documented, which currently involves significant repetition as many of the same or similar causes are listed separately for every unsafe control action.

References

[Le12] Leveson, N.: Engineering a Safer World, MIT Press, 2012

[Su14] Sundaram, P.; Vernacchia, M.; Thomas, J.; Placke, S.: Application of STPA to a Shift by Wire System, MIT STAMP Workshop, 2014