Safety Science 55 (2013) 173–187

Contents lists available at SciVerse ScienceDirect

Safety Science

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

Safety assurance in NextGen and complex transportation systems ☆

Cody Harrison Fleming [a], Melissa Spencer [a], John Thomas [a], Nancy Leveson [a,*], Chris Wilkinson [b]

[a] MIT, United States
[b] Honeywell Aerospace, United States

ARTICLE INFO

Article history:
Received 8 May 2012
Received in revised form 17 December 2012
Accepted 19 December 2012
Available online 15 February 2013

Keywords:
Air transportation
System safety
Hazard analysis

ABSTRACT

The methods currently used to assure the safety of planned changes to our air transportation systems were developed 50 years ago for systems composed primarily of hardware components and of much less complexity than the systems we are building today. These methods are not powerful enough to handle the complex, human and software intensive systems being planned and introduced today. This paper describes an alternative and demonstrates it on a new NextGen procedure to allow more flight level changes over oceanic and other regions with limited radar coverage. The new approach and results are compared with the results obtained by the more traditional methods being used for NextGen.

1. Introduction

The plan to transform the National Airspace System (NAS), called NextGen, changes the system through an evolution from a ground-based air traffic control system to a satellite-based system of air traffic management (FAA, 2011). The overarching goals of NextGen are to (1) reduce flight delays by improving airport operations; (2) improve aviation's impact on the environment through reduced CO_2 emissions and fuel use; and (3) make the airspace safer via more precise tracking, improved information-sharing, and implementing a Safety Management System (EUROCAE ED-78A/RTCA DO-264, 2002).

As changes are designed and implemented to realize the NextGen goals, assurance is necessary that the current high level of safety will not be degraded. The complexity of the current system and the changes envisioned makes this process challenging. Powerful tools will be required to assure aircraft and airspace safety.

Traditional approaches to safety analysis assume that accidents are caused by component failures (Leveson, 1995; Roland and Moriarty, 1983). They therefore focus on reliability analysis techniques, particularly fault tree or event tree analysis. The goal of these traditional approaches is to determine scenarios of component failures that together will lead to an accident or loss event. Failures may be single or multiple and are usually assumed to be random. After the component failure scenarios are identified, engineers use fault tolerance or fail-safe techniques to protect against hazards caused by the identified failures and to increase individual component integrity. A fly-fix-fly approach augments the design techniques with investigation of accidents and potentially serious incidents in great depth and recommendations made from the results to prevent reoccurrences.

This approach has been very effective in the past because there have been relatively few changes in the basic aircraft or air traffic control design; the systems are relatively simple; technology has changed slowly; engineers have been able to use very conservative design approaches; and the system components can be effectively decoupled so that interactions can be anticipated, simplified, and guarded against. This approach, by itself, is becoming less effective, however, as these assumptions start to be violated in our new or enhanced system designs.

Software is increasingly an important part of systems and allows enormously more complex and tightly coupled systems to be constructed. The potential for accidents arising from unsafe interactions among non-failed components, i.e., unplanned system and software behavior, is increasing. NextGen components, for example, may involve more than just one aircraft and one onboard system and include multiple aircraft, ground controllers, space-based systems, and communication links between aircraft. The traditional hardware-oriented safety engineering techniques focusing on failures do not adequately handle these types of new accident causes.

In addition, human roles are changing from direct control to supervision of automation, which requires more cognitively complex human decision-making. Like software, the changing roles of pilots and ground controllers introduces the potential for new causes of accidents that are not well handled by today's failure-oriented and hardware-oriented approaches.

☆ This research was partially supported by the NASA Aviation Safety Program (Contract NNL10AA13C).

* Corresponding author. Address: Massachusetts Institute of Technology, Room 33-334, 77 Massachusetts Ave., Cambridge, MA 02142, United States. Tel.: +1 617 258 0505; fax: +1 617 253 7397.
E-mail address: leveson@mit.edu (N. Leveson).

0925-7535/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ssci.2012.12.005

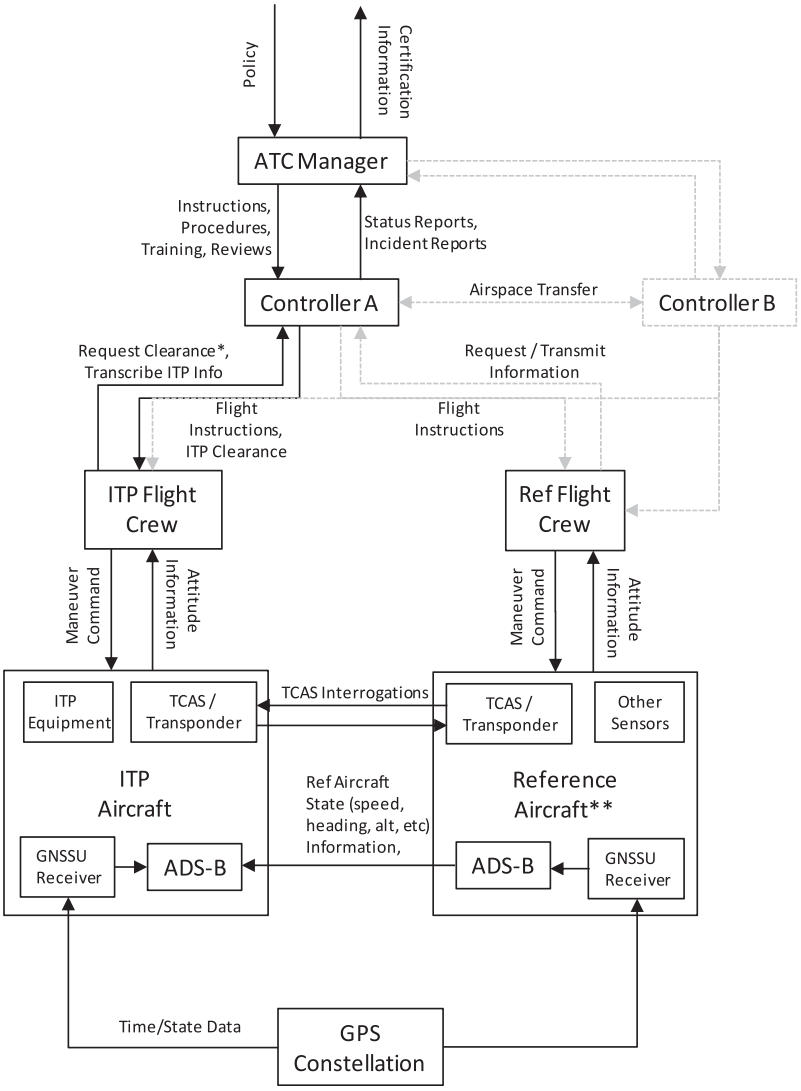

Fig. 1. Safety control structure for ATSA-ITP.

To deal with these new accident causes, more powerful tools are needed. This paper describes and demonstrates a new approach to safety analysis based on systems and control theory rather than reliability theory. Safety is treated as a control problem rather than a "prevent failures" problem, allowing not only consideration of the causes of the component failure accidents that were predominant in the past but also the new causality factors that are increasingly important today. This approach can be applied to NextGen and to other upgrades to complex transportation systems.

To demonstrate and evaluate the approach, we use a new Air Traffic Control (ATC) procedure, called Airborne Traffic Situational Awareness In-Trail Procedure (ATSA-ITP). ATSA-ITP, or simply ITP, was chosen because the safety analysis and underlying methodology has already been documented in DO-312 (RTCA, 2008). ITP provides a real-world case study with which to compare our safety assurance philosophy and analytical techniques being proposed to those being used by the Federal Aviation Administration (FAA), European Organisation for the Safety of Air Navigation (EUROCONTROL), and their associated organizations.

We first describe our new approach and the results of applying it to ATSA-ITP. We then compare the results to those of the ITP safety analysis documented in DO-312, particularly the difference philosophical underpinnings of these different approaches.

2. Using STAMP and STPA for safety assurance

The significant technical changes envisioned for NextGen creates a necessity for a new, more powerful model of accident causality that better represents today's complex, socio-technical systems. The new model used in our analysis, called Systems Theoretic Accident Model and Processes (STAMP) (Leveson, 2012), extends the types of accidents and causes that can be considered by including non-linear, indirect, and feedback relationships among events. In this way, the traditional causality model is extended to consider new types of accident causes arising from component interactions (rather than just component failures), cognitively complex human mistakes, management and organizational errors, software errors (particularly requirements errors), etc. Accidents or unacceptable losses can result not only from system component failures but also from interactions among system components—both physical and social—that violate system safety constraints.

2.1. Systems Theoretic Accident Model and Process (STAMP)

In systems theory, emergent properties (like safety) associated with a set of components are related to constraints upon the degree