Inter-Organizational Safety Debate: The Case of an Alarm System from the Air Traffic Control Domain

Paola Amaldi, Middlesex University, UK
Simone Rozzi, Middlesex University, UK

ABSTRACT

The management of safety critical operations cannot be left to the initiative of those individuals directly in contact with the production processes. Society as a whole has a role. This paper explores the interface between societal components having a direct active role in the “safety debate”. The reference domain is air traffic management and the interface is among air traffic controllers and pilots – as directly involved in the management of the air traffic – and two agencies, the NTSB (responsible for safety investigation after an accident) and FAA (responsible for regulating, upgrading and training of the workforce). Recent debates in safety management highlight that safe practice is a control problem: the result of effective hierarchical transmissions of safety constraints and making the boundaries of acceptable performance visible. This work analyzes how safety constraints related to an alarm system are represented, transmitted and interpreted by several parties – all committed to safety of operations in air traffic management. A “miscalibration” pattern has emerged where the tendency to ignore the alarm was initially addressed at higher hierarchical levels in relation to alarm design, and only in 2006 was addressed in relation to the core issue of nuisance or false alerts (FA).

Keywords: Alarms, False Alarms, Human-Alarm Interaction, Organizational Safety, Resilience Engineering, Societal Risk Management

INTRODUCTION AND OBJECTIVE

Risk management in safety critical domains like Air Traffic Management is not a technical issue only but a societal one. Near misses, accidents and disasters are considered to reflect a general and gradual drift of the organization towards an unsafe state (e.g., Rasmussen, 1997, 2000; Madni & Jackson, 2009; Leveson, 2011; Marais, Saleh, & Leveson, 2007). This macro process reflects the decisions of diverse actors – located at different organizational levels and scattered across different organizational boundaries – whose aggregated effect pushes the operation of safety critical processes beyond their safety envelope. This drift can be mitigated by the adoption of safety constraints at all hierarchical levels of the socio-technical system, where each level, can regulate the behavior of the lower one.
Hence, safety is a control problem depending on the whole socio-technical system involved in the provision of a safety critical service.

The present study aims at understanding how safety constraints are generated, transmitted, and implemented across diverse organizational boundaries and levels. The study takes an alarm system implemented in the US Air Traffic Control domain, the Minimum Safe Altitude Warning system (MSAW), as a case study. It analyzes how safety recommendations aiming at its improvement were generated and debated between (i) the accident investigation body, the NTSB, which developed the safety recommendations following investigation of accidents/incidents where the alarm was not used as intended; and (ii) the regulator and service provider organization, the FAA, i.e., the recipient of these safety recommendations.

BACKGROUND

In the Western world, every transport accident is followed by an investigation carried out by a Safety Board whose aim is not to identify “legal” responsibilities but to identify areas where operations could be improved. The present study focuses on the debate developed around safety recommendations following investigation of accidents/incidents where the alarm was not used as intended; and (ii) the regulator and service provider organization, the FAA, i.e., the recipient of these safety recommendations.

The analysis of an accident should be informed by four dimensions including the cover story, the targets of the hazards, in our case human life and technical equipment, the nature of the hazard, in our case the spatial and temporal relationship between aircraft and obstacles, and the control strategy which can address one or more of the phases characterizing the adverse event. Such event or rather “flow of effects” can be causally linked to at least three preceding conditions: the root cause, the casual chain, the critical event itself. Safety control depends on means to break or deviate the flow of events leading to the accident. A consensus should ideally be reached among decision makers at all levels of the socio-technical system with respect to the hazard sources and their control requirements. Following the representation of the accidental event, two main strategies can be identified: either blocking those events close to the critical ones or stepping backwards towards the “root causes” (Rasmussen et al., 2000).

Given a simplified representation of a sequence of events leading to an accident (Table 1), the following represents a schematic view of events in the worst scenario of Controlled Flight Into Terrain (CFIT).

What is to be included in the “root causes” is an old debate and whether such a concept is of any interest is still controversial. Notably, Carroll (1995) alluded to the “root cause seduction”: a phenomenon popular among managers who seem to believe that accidents can be prevented through the suppression of the “root causes”. One of the problems is that there is no “stop rule” for deciding how far back to go in the search of such “root cause”. Therefore limiting the search space is bound to exclude potential responsibilities. For the purpose at hand, we use the concept only to highlight how far back our data go in the search of “root cause”.

“Root causes” not only are not immediately linked to accidents but in order for them to act as “cause” a set of conditions has to be in place. Further some of these “causes” such as mountains or layout of runways, can hardly be removed or modified. In the current framework intervening on root causes amounts to managing the risk of loss of control, while intervention to alter the loss of control itself amounts to managing the risk of accident. Our investigation focuses on the latter. The purpose of the current study is not to investigate how Organizations understand accident. Rather while focusing on a single safety device, we aimed at studying how Organizations responsible for safety improvement and management of operations respectively “debate” about a limited set of safety issues elicited by the interaction of an alarm system with Air Traffic controllers.

Controlling the flow of events after the release of the hazard depends on the design of
The Technopolitics of the Ethiopian Nation
www.igi-global.com/chapter/technopolitics-ethiopian-nation/52222?camid=4v1a

An Analysis of the Impact of 2.0 Tools and Technologies on Organizational Processes
www.igi-global.com/article/analysis-impact-tools-technologies-organizational/52764?camid=4v1a