Reliability Engineering and System Safety 132 (2014) 60–71

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Controller recovery from equipment failures in air traffic control: A framework for the quantitative assessment of the recovery context

Branka Subotic, Wolfgang Schuster*, Arnab Majumdar, Washington Ochieng

Centre for Transport Studies, Department of Civil and Environmental Engineering, Imperial College London, London SW7 2AZ, UK

ARTICLE INFO

Article history:
Received 24 May 2013
Received in revised form
5 June 2014
Accepted 23 June 2014
Available online 1 July 2014

Keywords:
Air traffic control
Controller recovery
Equipment failures
Recovery context

ABSTRACT

Air Traffic Control (ATC) involves a complex interaction of human operators (primarily air traffic controllers), equipment and procedures. On the rare occasions when equipment malfunctions, controllers play a crucial role in the recovery process of the ATC system for continued safe operation. Research on human performance in other safety critical industries using human reliability assessment techniques has shown that the context in which recovery from failures takes place has a significant influence on the outcome of the process. This paper investigates the importance of context in which air traffic controller recovery from equipment failures takes place, defining it in terms of 20 Recovery Influencing Factors (RIFs). The RIFs are used to develop a novel approach for the quantitative assessment of the recovery context based on a metric referred to as the Recovery Context Indicator (RCI). The method is validated by a series of simulation exercises conducted at a specific ATC Centre. The proposed method is useful to assess recovery enhancement approaches within ATC centres.

1. Introduction

The Air Traffic Control (ATC) system comprises a set of components that interact in a complex manner to achieve safe and efficient flow of traffic. These components are human operators, equipment, and procedures. This paper addresses equipment failures and the response by air traffic controllers in the recovery of the ATC system to assure continued safe operation.

Defences in an ATC system offer protection against the majority of failures that occur. In the case of most technical failures, the built-in protection mechanisms are triggered automatically and seamlessly [7], resolving failures with no interruption of service. However, on occasions, the technical defences are insufficient to maintain the normal ATC system state and protect against negative outcomes [12]. On such occasions, the intervention of the Air Traffic Control Operator (ATCO) is essential for the safe separation of aircraft. The recovery process generically, starts with the detection of a failure, followed by the diagnosis of the problem and the decision and implementation of the most appropriate recovery strategy. To better understand the entire recovery process it is necessary to identify and capture the main factors that influence controller recovery performance. To date ATCO recovery from failure has seen very little research in terms of a detailed definition of the elements of each of the three stages in the recovery process [1,7,15].

Whilst there is growing recognition of the impacts of equipment failures [8,9,12], there is a need for detailed knowledge of how controllers perform during unexpected or unusual situations (including equipment failures). Various researchers have highlighted the importance of understanding the context surrounding hazardous events [2,3], which provides crucial information on the causal and contributory factors. Extensive research has been conducted on contextual factors in the Human Reliability Assessment (HRA) discipline, e.g. in the chemical and nuclear industries.

In Air Traffic Management (ATM), contextual factors or contextual conditions are defined as "internal or external factors that influence the controller's performance of ATM tasks" [6]. Based upon HRA theory, Subotic et al. [20,21] investigated the context regarding controller recovery from equipment failure, referring to the contextual factors as Recovery Influencing Factors (RIFs). The selection of these RIFs was based primarily upon a review of contextual factors from human reliability techniques in:

- ATC/ATM, e.g. Human Error in ATM (HERA) [5], Technique for the Retrospective and Predictive Analysis of Cognitive Errors in ATC (TRACEr), and Recovery from Automation Failure Tool (RAFT) [7], and
- other relevant safety critical industries, e.g. nuclear and chemical process industries.

These were complemented by both those factors related to specific equipment failure and those that play an important role in an operator's decision-making and performance in emergencies.

* Corresponding author.
E-mail address: w.schuster@ic.ac.uk (W. Schuster).

http://dx.doi.org/10.1016/j.ress.2014.06.010
0951-8320/

A total of 20 relevant RIFs were identified (summarised in [22] and captured in Table 1), divided into four main groups: internal factors related to the ATCO; equipment failure factors that capture the characteristics of a failure; external factors that capture the working conditions surrounding a controller at the moment of the failure, and airspace related factors that capture the characteristics of dedicated airspace during the failure and recovery.

This paper proposes a quantitative method to analyse the impact of the context on controller recovery performance from an equipment failure. Section 2 develops the framework for the quantitative assessment of the recovery context. Section 3 outlines the methodology for testing the framework and Section 4 uses the new framework to assess the controller recovery performance at a particular European Civil Aviation Authority ATCC.

2. Framework for the quantitative assessment of recovery context

The qualitative and quantitative definition of RIFs assume that a failure has occurred and that it is possible to define every possible context as a combination of RIFs and their corresponding levels of influence. This approach is important for the prospective analysis of controller performance, as well as a retrospective event analysis. However, in retrospective analysis, quantifying RIFs may be difficult given the potential lack of data and information about the context. For predictive analysis, specifying the RIFs becomes significantly more difficult, with an inherent level of uncertainty in the process.

The quantification of the RIFs uses a probabilistic approach, which has several advantages. Firstly, if a given RIF is not clearly specified or known, it is possible to assume probabilities for each of its levels based on operational data. This allows any uncertainties to be considered more explicitly (see e.g. [14]). However, the quantification of RIFs poses a number of challenges:

(i) the difficulty to quantify human performance;
(ii) the lack of consistent data in the occurrence reporting schemes for equipment failure related RIFs;
(iii) the majority of the external RIFs are ATCC specific and difficult to define in a generic form.

These challenges are addressed by developing a methodology consisting of six steps, summarised in Fig. 1 and outlined below. The probabilistic assessment aims to capture the characteristics of a 'generic' ATCC as a basis for further refinement to the unique characteristics of a specific ATCC.

2.1. Recovery context: six steps

2.1.1. Step 1: Assessment of relevant RIFs

Firstly, all candidate RIFs are assessed and those relevant to a generic ATCC are identified. In order to investigate the impacts of RIFs on controller recovery performance, the principles of the Cognitive Reliability and Error Analysis Method (CREAM) are used [11]. This assumes that favourable performance conditions improve controller recovery, whilst unfavourable conditions are expected to worsen it. Based on this, qualitative descriptors are allocated for each RIF to define its level of impact on recovery performance. The descriptors are divided into Level 1 (positive impact on recovery), Level 2 (tolerable impact on recovery), and Level 3 (negative impact on recovery). Whilst some RIFs have three qualitative descriptors, others may only have two.

2.1.2. Step 2: Probabilistic assessment of RIFs

In order to provide a reliable quantitative analysis of controller recovery performance, probabilities for each RIF and its corresponding levels are determined. The methodology behind the probabilistic definition of each RIF is detailed in Subotic [22]. Probabilities were determined from:

(i) over 20,000 operational failure reports originating from three Civil Aviation Authorities and one ATCC system control and monitoring database;
(ii) survey results aimed at capturing controller experience with equipment failures from 134 controllers in 58 ATCCs worldwide;
(iii) responses of eight ATM specialists from Ireland, Norway, Sweden, Austria, New Zealand, Australia, and Japan, and
(iv) a review of two major studies: EUROCONTROL [4] and Hilburn and Flynn [10].

In order to avoid skewing the probability distributions of equipment failures towards those with monitoring and audit functions, the probability distributions should be based on historical data from the system control and monitoring function (if available) in each ATCC or alternatively from its engineering function. For planned equipment installations, the probability distributions should be determined on the basis of historical data from the manufacturer (for COTS) or from the outcomes of risk management procedures (for equipment designed in-house). All RIFs are initially assumed to be independent and their corresponding levels of influence on controller performance take integer values.

2.1.3. Step 3: Interactions between recovery influencing factors

The two-way interactions between RIFs are expressed in terms of symbols '1', '2', '3', or 'x' in Table 1. The interactions were validated by:

- two HRA techniques: CREAM [11] and the Connectionism Assessment of Human Reliability – CAHR [18] – these techniques highlighted the most generic interactions between RIFs, and
- inputs from three SMEs with more than 10 years of experience in the ATC domain.

Despite its highly generic nature, approximately 22% of identified RIF interactions are reflected in the CREAM study and approximately 35% in the CAHR study. The independent validation by the SMEs accounted for approximately 90% of the identified RIF interactions. Only the interactions validated between the three methods were used in the analysis, accounting for a total of 95% (107 out of 113) of all possible interactions. The RIF interactions were then individually quantified. The assumption is made that when two RIFs interact, the influence of a given RIF (i.e. its level) changes linearly with each interaction. Additionally, ATM operational experience dictates that the total influence of all RIFs on a given RIF cannot change its level by more than one unit (in line with the approach in [11]). The final RIF-level, accounting for RIF interactions, is then expressed mathematically as

$$RIFY_{j'} = RIFY_j + \sum_x k_{xy} R_x \qquad (1)$$

where $RIFY_j$ represents the level j of $RIFY$ before interactions are taken into consideration; $j=1$, 2, or 3; $RIFY_{j'}$ represents the level j' of $RIFY$ after accounting for RIF interactions; $0.0 \le j' \le 4.0$; k_{xy} represents the coefficient of interaction between $RIFX$ and $RIFY$; R_x measures the direction of influence of $RIFX$ onto $RIFY$, where $R_x = \{+1,\ 0,\ -1\}$ and x represents the sub-space of the given context. In the current implementation of the model, the assumption is made that all interactions have the same level of influence (i.e. $k_{xy} = k$):

$$RIFY_{j'} = RIFY_j + k \sum_x R_x \qquad (2)$$