Structuring a Safety Case for an Air Traffic Control Operations Room

Ron Pierce
CSE International Ltd, Glanford House, Bellwin Drive, Flixborough, Scunthorpe DN15 8SN, UK

Herman Baret
EUROCONTROL Maastricht Upper Area Control Centre, Horsterweg 11, 6199 AC Maastricht Airport, The Netherlands

1 Introduction

Production of a formal safety case is a valuable part of the safety management of a safety related system. A safety case is a written justification that the given system will be tolerably safe during installation, commissioning and operation, and in some cases decommissioning. A well-written safety case will give all stakeholders (operating authority, members of staff and regulators) justifiable confidence that the system is safe to operate and to continue in operation. Although production of a safety case is now regarded as best practice in many quarters, there is still relatively little experience of writing safety cases and only a limited amount of literature on the topic. Many safety engineers find it a daunting task and some safety cases are still poorly structured, difficult to understand and less than compelling.

This paper describes the authors' approach to the development of the safety case, in the period between mid 2001 and mid 2003, for a major safety related system, namely a new air traffic control (ATC) operations room for the EUROCONTROL Maastricht Upper Area Control Centre (UAC). The Maastricht UAC controls all air traffic flying at over 24,500 feet over the Benelux countries and north-west Germany. It is a busy centre which handles over 1.2 million flights per year and the airspace is complicated by the presence of crossing air routes and by traffic climbing and descending from the many busy airports in the Maastricht UAC's area of responsibility or just outside it, such as Frankfurt, Paris, Amsterdam and London.

It is hoped that the experience related here will be helpful to other engineers who are faced with the task of constructing a safety case.

2 The New Operations Room

The New Operations Room (N-OR) is located in a new building adjacent to the old operations room and is equipped with a large suite of modern workstations for air traffic controllers, supervisors and flight data preparation staff.

The new equipment is collectively known as the New Operator Input and Display System or N-ODS. Each controller workstations (CWP) consists of a large (2K by 2K pixel) high resolution display screen for the advanced air traffic situation display, a screen for supporting information, mouse, keyboard and two touch input panels. Flight plan data is presented electronically, as was the case with the old equipment, and paper flight progress strips which are still used by many ATC centres are absent.

The Compaq computers which drive the display screens run Unix and X-Windows and are connected by a reliable multi-ring fibre optic (FDDI) LAN to the servers which provide flight data, radar data and other services. Workstations are grouped in sector suites as is normal practice in ATC. In addition to the controller workstations, there is an advanced recording and replay system which allows the air situation to be replayed exactly as it was presented to the air traffic controller at time of recording, including all the interactions with the machine. An operational monitoring system is used to display and control the status of all equipment and software.

In the event of failure of the radar surveillance data system, a fallback facility consisting of a diverse radar data processing system associated to a limited flight plan capability provides the radar picture to the CWP display screens via a video switch. An Ultimate Fallback Facility prints up to date flight plan information on high speed printers in case of loss of communication between the main flight data processing system and the CWP.

Procurement of the N-ODS system and the fallback facility pre-dated the need for a formal safety management regime and much of the safety evidence had to be constructed by retrospective analysis.

3 Arguments, Evidence and Goal Structuring Notation

A properly constructed safety case should consist, in essence, of arguments and evidence. The arguments provide the structure of the safety case, in terms of safety claims and explanations, while the evidence provides the facts to support the arguments.

The Use of Goal Structuring Notation (GSN) as a graphical means to express the essential argument and evidence structure of a safety case is becoming increasingly popular. GSN was used to develop the N-OR safety case and was found to be very useful both for thinking about the safety case when developing it, and for presenting it to others. Use of GSN is increasing, and other published examples of safety cases which use GSN are the RVSM Pre-Implementation Safety Case for Europe (EUROCONTROL 2001), the Merlin helicopter fly-by-wire control system (Chinneck et al 2004) and autonomous vehicle operation on an airport (Spriggs 2003).