Dynamic Risk Management in Air Traffic Management System Failures

Nicholas J. Lowth | LUND UNIVERSITY

Dynamic Risk Management in

Air Traffic Management System Failures

Nicholas J. Lowth

Lund 2024

Title: Dynamic Risk Management in Air Traffic Management System Failures

Author: Nicholas J. Lowth

Number of pages: 98

Illustrations: 15

Keywords

Air Traffic Control, Uncertainty, Risk Management, Air Traffic Management, Resilience, Emergence, Trade-offs

Abstract

Context This research looks at managing uncertainty and recovery processes following failure of a sociotechnical system. The provision of Air Traffic Services (ATS) is an essential service that must continue to function supporting at a minimum; medical flights, search and rescue operations, humanitarian aid, State and military flights (as demonstrated during the recent global pandemic). **Purpose** The objective of this research is to see what operationally deployed processes supported the resumption of ATS while emerging from, or still in, an uncertain degraded system state. **Methodology** A qualitative case study approach using semi-structured interviews was adopted. Two failure events were examined. Failure event report documentation was reviewed, face to face interviews with key personnel involved in ATS systems failures were conducted. The interview data was collected, crosschecked against event documentation, and then coded and analysed. **Results** While the use of air traffic flow restrictions to mitigate system overload are used daily to prevent overload, it is not acceptable to society as a prolonged mitigation against system degradation. The emergence of safety strategies displayed in dealing with uncertainty contained elements of a resilience system. The trade-offs required to achieve the safety processes necessary to resume service provision demands were fine tuned to edge, closer to the edge of an unfamiliar

safety boundary (for both events) in a dynamic setting with multiple adjustments as both systems returned to service. **Discussion** The current popularity of resilience as a design prerequisite for new systems doesn't address the requirement to achieve resilience in current operational systems. Opportunities exist to adopt some practices and strategies that can enhance resilience. The interplay between boundaries and actors is key to navigating uncertainty in a dynamic ATM environment. While the front-line operators (ATCOs, Ops Supervisors & ATS Engineers) are key to negotiating the production boundary, there needs to be protection counterbalance strategies.

Several items are proposed in Chapter 5 for consideration; complexity considerations, retro fitting resilience i.e. dedicated abnormal degraded system operations training module to specifically allow front-line operators to practice for failure, uncertainty, and fundamental surprise, & inclusive training strategies and regulatory considerations, these discussion items are intended to be of use to those tasked with navigating uncertainty in degraded Air Traffic Management operations in preparing for such events.

Acknowledgements

It all started with a cup of coffee bought by Smokes in a Dublin pub overlooking a grey O'Connell Street and the river Liffey, "Of course you can" he said…. ultimately, he was right. But not without his endless support, patience, provocation, and guidance. I am eternally grateful. Go raibh míle maith agat a chara.

On the first day I met JB he told me the safety world wasn't flat. On the second day I met JB he told me the safety world as I knew it wasn't even round, I panicked. And then he introduced me to a "new view" of safety, with some gentle nudges… and some not so gentle nudges, he too supported and nurtured me along this journey. Likewise, I am eternally grateful. The HFSS community they have cultivated at Lund is a special place of learning.

Thanks is also due to Jim Nyce who animated the learning journey in his own unique manner, recounting experiences from his eastern travels and offering insights into research methods. Peter Nolan and Claire O'Donoghue believed in me, supported me, and gave me the opportunity and confidence to take those first steps. I am grateful for your support. I would also like to thank the interviewees who participated in this research for their time and patience. The insights you provided were fascinating. My fellow course mates from San Francisco to Singapore, your kindness, support, and intellect are astounding. I look forward to continued friendship with you all.

To my partner Céline, without your support I simply would not have made the finish line. Thank you.

Riskhantering och samhällssäkerhet
Lunds tekniska högskola
Lunds universitet
Box 118
SE-221 00 Lund
Sweden
http://www.risk.lth.se

Division of Risk Management and Societal Safety
Faculty of Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden
http://www.risk.lth.se

CONTENTS

List of Figures

List of Tables

ABBREVATIONS & ACRONYMS

ACC – Area Control Centre (operations room where air traffic services are provided from)

ANSP – Air Navigation Service Provider

AON – ATS Operations Notice

ASSR – Assigned SSR Code

ATC – Air Traffic Control

ATCO – Air Traffic Control Officer

ATM – Air Traffic Management

ATS – Air Traffic Services

C2K – IAA CAIRDE 2000 ATM System

CAIRDE – Civil Aviation Integrated Radar Display Equipment ("Cairde" is also the Irish language word for "Friends")

CDM – Critical Decision Method

CWP – Controller Working Position

ENG – Engineering

ETIC – Engineering Technical Incident Cell (NATS)

EUROCONTROL – European Organisation for the Safety of Air Navigation

FDDI LAN – Fiber Distributed Data Interface Local Area Network

FIR – Flight Information Region

HAZOP – Hazard and Operability, a form of risk management to identify, evaluate, and control hazards and risks in complex processes

IAA – Irish Aviation Authority (Irish Air Navigation Services Provider 1994-2023, renamed Airnav Ireland in 2023)

ICAO – International Civil Aviation Organisation

IRA/ IRR – Inter-Rater Agreement/ Reliability

LAC = London Area Control

LAN – Local Area Network

LTC – London Terminal Control

MTBF – Mean Time Between Failure

NAS – National Airspace System

NATS – National Air Traffic Services (UK Air Navigation Services Provider)

NAVIAIR – Navigation Via Air (Danish Air Navigation Services Provider)

NIC – Network Interface Card

NMOC – Network Management Operations Centre (EUROCONTROL Flow Control)

ONL – Operation LAN (Local Area Network)

OPS – ATC Operations

plámás – Irish language word which loosely translates as flattery

SFS – System Flight Server

SMC – Systems Monitoring and Control (H24 Engineering function)

SME – Subject Matter Expert

SMS – Safety Management Systems

SMU – IAA Safety Management Unit

STAMP – Systems-Theoretic Accident and Model Processes

SR – Safety Requirement (a safety mitigation derived from risk assessment HAZOP process)

SRD – IAA Safety Regulatory Department

SRM – Safety Risk Management

SSR – Secondary Surveillance Radar

TMA – Terminal Area around a group of airports

TMCS – Technical Monitoring and Control System

UK – United Kingdom

VSM – Viable System Model

WAV – Waveform Audio File Format

1. INTRODUCTION

1.1 Broader Topic & Relevance

In this chapter the research topic is introduced and related to a specific occurrence.

During the summer of 2008 there were multiple failures of the Air Traffic Management (ATM) System at Dublin Area Control Centre (ACC). The main operational networked system failed on six occasions between the 2nd of June and 9th July (on 2nd June, 4th June, 2nd July and three on 9th July), (IAA SRD, 2009, p. 4). After the initial failures a flow control rate was applied to restrict air traffic levels as a mitigation against repeat failures. As the failures continued over the weeks there was intense blunt pressure to increase traffic levels. This event is studied further in this research.

One of the most basic of contingency measures within Air Traffic Control (ATC) is the deployment of an Aldis lamp or a light signal (ICAO, 2005; IFATCA, 2022). This is used to send visual signals to any aircraft in the vicinity of an aerodrome who has experienced a loss of radio communications. It is a simple light system which operates using either green, red or white light signals e.g. green means cleared to land, red means do not land. It has served aviation well since the 1940's and is still a contingency method available in control towers today. The current edition of International Civil Aviation Organisation (ICAO) Annex 2 Rules of the Air, Section 4. Signals for Aerodrome Traffic (ICAO, 2005) contains instructions for the use of light and pyrotechnic signals (see Figure 1 below). There are of course some meteorological issues that impact the effectiveness of its use e.g. rain, low cloud, fog, which reduce its effectiveness in low visibility conditions. Wicaksono outlines several additional environmental factors which impact its effectiveness e.g. accuracy of beam,

additional aircraft intercepting the signal, etc. (2020). The application of contingency measures, like the Aldis Lamp, to compensate for system or equipment failures have been utilised in ATC since the service began.

Figure 1. Light Signals for Aerodrome Traffic.

Light		*From Aerodrome Control to:*	
		Aircraft in flight	*Aircraft on the ground*
Directed towards aircraft concerned (see Figure A1-1).	Steady green	Cleared to land	Cleared for take-off
	Steady red	Give way to other aircraft and continue circling	Stop
	Series of green flashes	Return for landing*	Cleared to taxi
	Series of red flashes	Aerodrome unsafe, do not land	Taxi clear of landing area in use
	Series of white flashes	Land at this aerodrome and proceed to apron*	Return to starting point on the aerodrome
Red pyrotechnic		Notwithstanding any previous instructions, do not land for the time being	

* *Clearances to land and to taxi will be given in due course.*

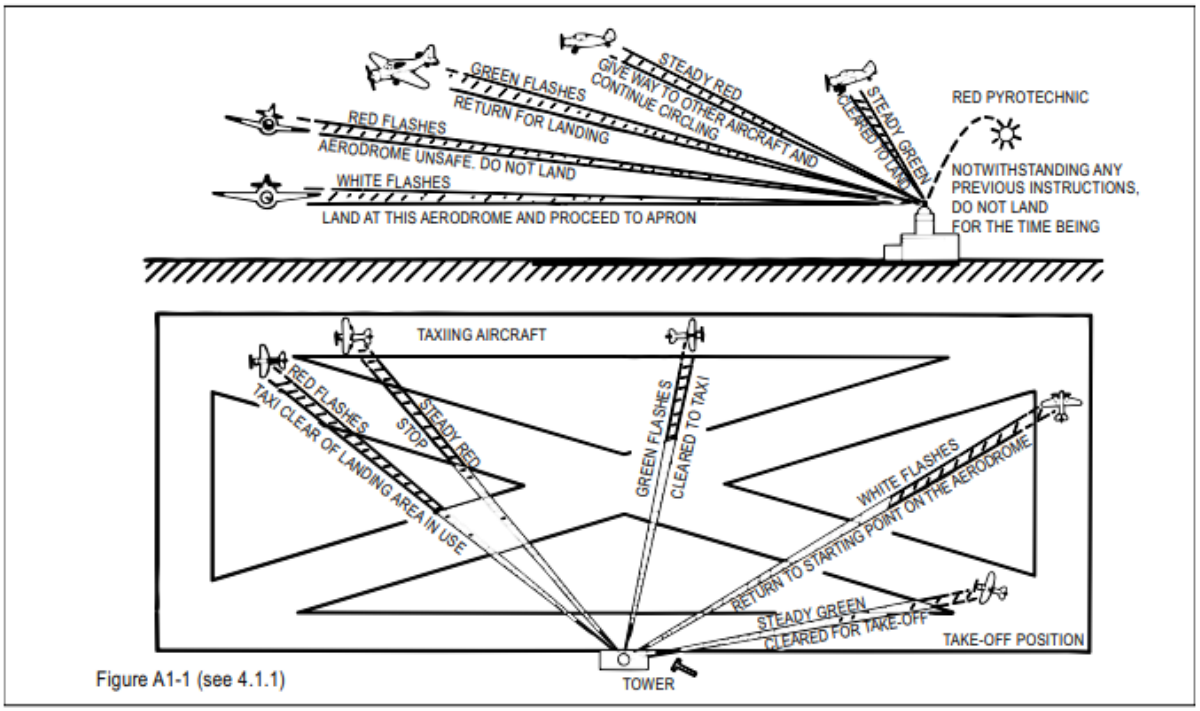


Figure A1-1 (see 4.1.1)

Advances in technology have resulted in increased automation in ATC over the last thirty years. New technologies introduced include; the use of electronic flight progress strips rather than paper flight progress strips in control tower operations, integrated radar display screens employing windows, icons, menus and drop down lists to input updated flight plan data, multi frequency re-transmission communication systems taking the place of a single

radio channel with a manual selector dial to change frequency, the use of electronic on-line data interchange (OLDI) exchange of flight information between air traffic control units taking the place of air traffic controllers (ATCOs) making phone calls with boundary estimates for incoming and outgoing flights. These advances in technology have allowed individual air traffic controllers to handle increased amounts of air traffic and have brought some new and improved safety features presented onscreen with audio safety alerts to ATCOs. These include safety nets (short & medium term conflict alert tools, minimum safe altitude warnings) and monitoring aids (route adherence & final approach path monitoring). As ATC systems have advanced, so has their complexity, and consequently the contingency methods in use have also become more complex.

A typical ATM system consists of the following components; flight data processers, multiple radar surveillance trackers, communications systems to allow air-ground, ground-ground voice, and data communications, and air navigation systems which are all connected to multiple air traffic controller working positions (CWP). Typical system design is based on a distributed network architecture where local area networks (LAN) connect these system components. At the centre of the system is the human, the operational air traffic controllers and the ATS engineers who operate and support the system. The ATM system enables the provision of Air Traffic Services (ICAO, 2018) to aircraft. The ATM system can be considered a tightly coupled socio-technical system which is subject to both linear *and* complex interactions (Perrow, 1999; Rasmussen, 1997).

ATM systems have inbuilt redundancy with multiple backup systems. This redundancy is based on the defences in depth concept and mitigate against system failures as imagined by the system designers. Reasons “Swiss cheese” model (1997) best depicts this concept. This principle and Reasons model are both prevalent across aviation. When incidents or accidents occur investigators typically follow the safety chain of events model where “an

accident path is defined by a series of sequential events from initiating event to accident realization" (Singh et al., 2019) and look for a root cause which can be blamed for the event. So, what if an ATM system fails in an unpredicted manner, with no identifiable root cause? And what then if it keeps failing?

"A locomotive in an accident is a heavy object, not a thermodynamical machine"

(Rasmussen et al., 1990)

Rasmussen describes the performance of engineered systems, like an ATM system, as, "Technical designs could be verified and tested by quantitative models and controlled laboratory experiments" (Rasmussen et al., 1990, pp. 449-450). This leads to system safety verification being achieved in controlled theoretical environments where the probability of failure for some systems is expressed in theoretical values up to 10^{-7}. Systems with these levels of safety assurance values can be classed as "ultra-safe systems" (Amalberti, 2001) and are prevalent throughout aviation. Rasmussen continues that, in today's dynamic systems "the complexity of the situation required the use of less stringent causal analyses in terms of chains of events" and uses a simile that "a locomotive in an accident is a heavy object, not a thermodynamical machine." (Rasmussen et al., 1990, p. 450). When complex systems fail, the results can be blunt, traumatic, and unexpected. Rasmussen argues that despite this, the design of complex systems our mitigations against failure, must be improved (1990, 1997).

The Irish Aviation Authority (IAA) Safety Regulatory Division (SRD) investigation report into the failures at Dublin describes the ATM system architecture as "A fault tolerant architecture" with multiple layers of redundancy and is "designed to ensure radar data remains available should the LAN fail" (IAA SRD, 2009, p. 9). The SRD report further concludes that "the system safety assurance documentation identified that, from statistical analysis, a failure

into emergency mode was not likely to occur during the operational lifetime of the system" (IAA SRD, 2009, p. 4). Yet, despite the multiple layers of redundancy the system did fail. Six times in six weeks. Initial investigations into the failures did not identify a root cause. There was no apparent fix for the "ultra-safe system" despite considerable effort to resolve the technical issues. Without a fix, air traffic levels at Dublin were subject to continued flow control restrictions.

The SRD report also highlights "that the system did not fail in the predicted manner and the unexpected system behaviour was found to have influenced the operational response adopted to deal with the situation." (2009). The unexpected system behaviour caused radar screens that were not supposed to lose flight information, to suddenly lose flight information. Consequently, confidence and trust in the system was knocked as the busy summer progressed.

The air traffic flow control measures remained in effect for eight weeks after the first failure and to manage this period of uncertainty there were multiple risk assessments conducted aimed at increasing traffic levels. The risk assessment method was a somewhat subjective process and over weeks of continued assessments there was mounting pressure to increase the levels of traffic permitted. The proposed scenarios were pushed closer to the boundary of unacceptable risk.

Ultimately a *root cause* of the failures was identified as a combination of "a single network interface card together with a weakness in the FDDI LAN failure recovery mechanism" (IAA SRD, 2009, p. 41) and the solution to resume full-service provision became a numbers game. To revalidate the overall probability for the total failure of the Flight Plan Information within the Cairde ATM system back to a value of $5.3 * 10^{-7}$ per hour of operation. Which represents a Mean Time Between Failure (MTBF) of about 1000 years.

The failure of ATM systems is not isolated to Dublin, nor to 2008. Since 2015 there have been multiple failures of ATC systems across Europe e.g., Belgium airspace closed due to a failure at Belgocontrol ATC Centre in 2015, Air Traffic Control "communications" problem in Sweden stop departures in 2016, failure at Karlsruhe Upper Area Control Centre in 2017, EIROCONTROL's Enhanced Tactical Flow Management System failure in 2018, Naviair system failure in Copenhagen 2022, technical failure over Switzerland which closed Swiss airspace in June 2022 and most recently in the UK in August 2023 (Dearden, 2015; Hand, 2023; Hollnagel et al., 2022; Orban, 2017; Statt, N. 2018; Swiss airspace re-opens after 'technical malfunction', 2022; 'Technical issue' briefly cripples Swedish air traffic, 2016). The impact of these failures is significant both in terms of disruption to passenger's travel plans and in fiscal costs to the airlines, airports, passengers, ATC, etc.

Safety is an emergent property of systems

Cook argues that "Safety is an emergent property of systems; it does not reside in a person, device or department of an organization or system." (2000, p. 4). Leveson asserts that "In the past, our designs were more intellectually manageable and the potential interactions among components could be thoroughly planned, understood, anticipated, and guarded against. In addition, thorough testing was possible and could be used to eliminate system design errors before system use." (2011). Similar to Perrow's view that systems will become harder to manage in a crisis, Leveson further argues that modern high-tech systems have become so complex that they are the cause of many accidents (Leveson,2011; Perrow, 1999).

So, how do we manage active failures in complex systems? What to do when Newtonian reductionist reasoning fails? and a system fails in an unexpected way? What happens when a sociotechnical system uncouples, and a locomotive ends up crashing through

an operational air traffic control centre? How do you know when making the decision or choice that it's *safe* to return to operations? How can you *trust* the system again following uncertainty?

Hence my choice of research question:

What processes support the decision to allow a return to full capacity when recovering from degraded operations in ATM?

2. LITERATURE REVIEW

In the first part of this chapter, the current ATM literature relevant to the chosen research topic and the gap in which this research sits are outlined. In the second part of this chapter, the concept of safety as a moveable dynamic is introduced as it features later in this research.

2.1 ATM Specific Research

There is research already existing on the performance of controllers recovering from system failures, e.g. Subotic et al. (2014) but this is focused on the controller and their immediate recovery actions. Research in the field of ATM covering topics like, identifying paths towards emerging hazards, and system dynamics approach to the efficiency thoroughness trade off in complex systems in ATM Applications (Kontogiannis & Malakis, 2019; Yi et al., 2022; Yu et al., 2021) is well established. This research focuses on system design and not on managing active system failures from an operational perspective. This research relates to the immediate actions and response of the controllers involved system failures and unusual situations and while not specific to this research they may be consulted by the reader as additional background information.

“Dead Reckoning” by Diane Vaughan (2021) examines the complexities and challenges of ATC within the Federal Aviation Administration (FAA), the focus of Vaughan’s research is between human organizational systems, the importance of people, human performance, and problem solving. While Vaughan warns on the complexity of the technical systems involved, system recovery from uncertainty is not included.

Bieder (2022) outlines the origins of Safety Management Systems (SMS) in aviation and covers its application to the various stakeholders in modern sociotechnical systems. Uncertainty is acknowledged "safety does not value uncertainty due to its alarming nature" (2022. p. xvii) and Bieder outlines a gap in aviation safety where living with "uncertainty calls for other tools (e.g., concepts, methods, practices, regulatory regimes, legal systems) that are not yet available and articulated" (2022. p. 139).

There is also research focused on the controller work practices remaining safe at the edge of compliance (Kontogiannis & Malakis, 2019) and forward-looking system design on operational risk (Kontogiannis et al., 2017). Kontogiannis & Malakis's work to date has culminated in the development of integrated models of human performance that support the design and operation of joint cognitive engineering. They analysis the UK National Air Traffic Services (NATS) System Flight Server (SFS) failure event in 2014 (which will be listed as a case study later on in this research, see Section 3, Cases, below) to illustrating the link between STAMP and VSM modelling techniques (Kontogiannis & Malakis, 2018, pp. 317-340), but their research does not examine the methods applied in the decision process to restore operations.

There are few detailed reports on ATM failures available to the public and those that exist are factual reports rather than research articles e.g. Walmsley et al., 2015, but there are some academic *research* articles on ATM system failures. Hollnagel et al. examine a system failure where a group of operational controllers "were able gracefully to recover from an unexpected condition" (2022, p. 5). Like Hollnagels approach, this research document looks at two separate failure events where "nothing" happened, but where solutions were created by an organisation. This notion is explored further in Chapters 4, 5 & 6 of this research.

McDermid & Whysall also provide a review the NATS 2014 system failure focusing on an analysis of the systems and drawing out lessons learnt pertinent to evolution within

complex systems (2015). Their article concludes with two findings; “First, it is impossible to ensure that software is fault free and therefore the broader system must be resilient to failures.” and, “Second, several non-technical factors are important in the management of incidents, including a collaborative culture.”.

It is within the second of these findings, that this research fits, within a non-technical collaborative management process when dealing with incidents. This research also sits in the uncertainty gap identified by Bieder above.

2.2 Safety as a Dynamic

As this research developed it became clear that there was a dynamic element to safety performance within ATM that warranted a revisit to the literature review to address this. The review is expanded beyond ATM specific research to include Cook and Rasmussen. Rasmussen's safety performance boundaries model (1997) serves to define safety as a dynamic. Cook explores how complex systems fail and simplifies Rasmussens boundaries model into several steps showing movement to the accident boundary and affirming that Safety is dynamic (Cook, 1998, 2014).

There is already valuable research on goal conflicts using Rasmussen's Model of Boundaries which provides for the formal incorporation of worker "resilience" into work practices of front-line operators e.g. in the field of Biomedical Laboratory research (Vijayan & Smoker, 2021). There are of course many articles relating to resilience (Hollnagel et al., 2006; Woods, 2015), one of Bergström's many contributions to research stands out where he examines safety science resilience literature and raises ethical questions to be addressed (2015). While the value of this work is undoubted, it relates more to ethics whereas my focus is more specific on a derived practical application.

Noteworthy is the role of SMS in the concept of safety as applied to aviation and specifically ATC. While Bieder addresses the origins of SMS in aviation (2022), it is left to Malakis, Kontogiannis & Smoker to highlight the limitations of SMS in aviation (Malakis et at., 2023). The role of SMS as applied to the case studies within this research is addressed later on in this document.

Pertinent to the gap identified above is the work of Cook who outlines features applying to How Complex Systems fail;

1. Complex systems are intrinsically hazardous systems.
2. Complex systems are heavily and successfully defended against failure.
3. Catastrophe requires multiple failures – single point failures are not enough.
4. Complex systems contain changing mixtures of failures latent within them.
5. Complex systems run in degraded mode.
6. Catastrophe is always just around the corner.
7. Post-accident attribution accident to a 'root cause' is fundamentally wrong.
8. Hindsight biases post-accident assessments of human performance.
9. Human operators have dual roles: as producers & as defenders against failure.
10. All practitioner actions are gambles.

(Cook, 1998)

Cook expands and illustrates this standpoint by simplifying and adapting Rasmussens model (1997) and affirming that safety is dynamic as depicted in Figures 2, 3 & 4 below. Rasmussens original model is shown in Figure 5 for reference.

Figure 2. Dynamic Point Safety

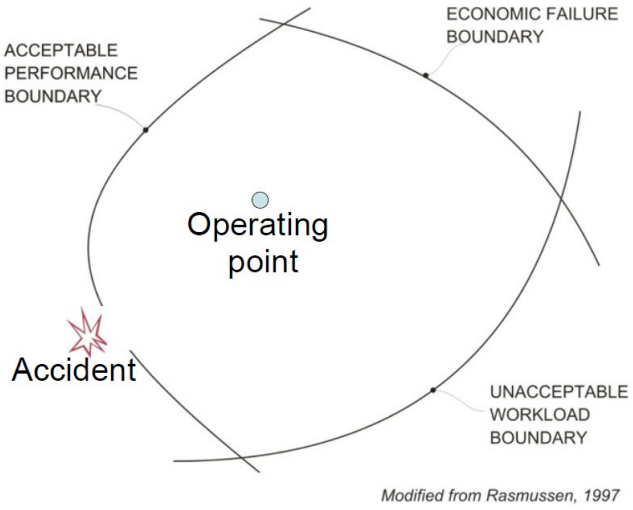


Figure 3. Movement of Point of Safety Over Time

**The operating point tends to move towards the accident boundary over time.*

Figure 4. Operating Point Close to the Margin

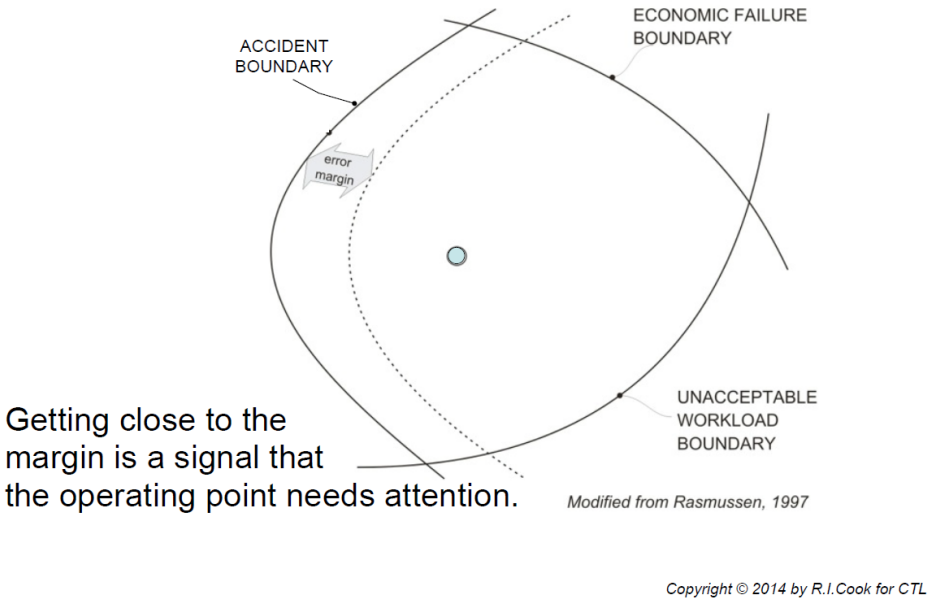
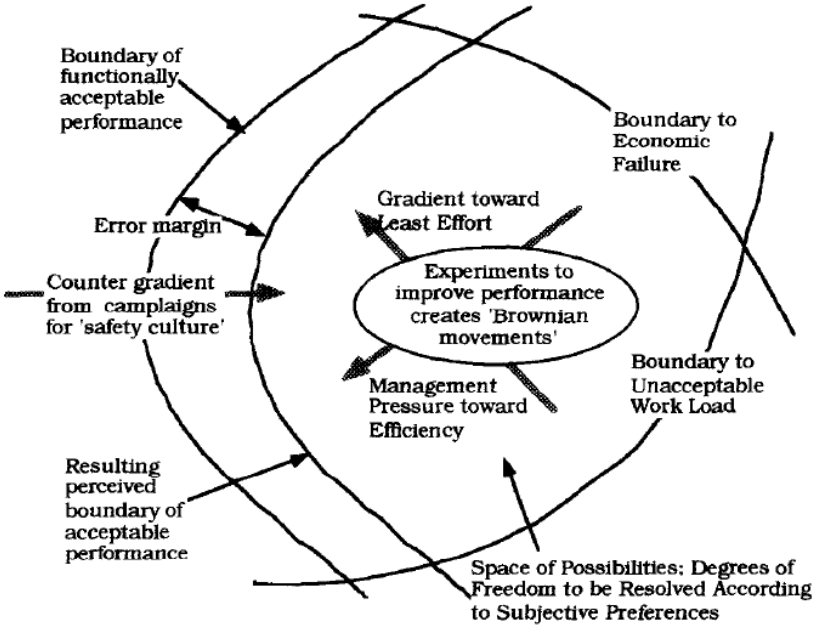


Figure 5. Rasmussens Safety Boundaries model



This concept of Rasmussen's safety boundaries showing movement to the accident boundary and affirming that Safety is dynamic is referenced in Chapters 4 & 5 as it applies to this research.

3. RESEARCH METHOD

In this chapter the research methodology is defined, and the case studies are introduced. The data collection interview methods are described, and the associated analysis processes explained. An ethics subsection is also included to address ethical concerns.

3.1 Methodology

A “case study” research methodology is applied to this research (Creswell & Poth, 2016.; Ávila-Cabrera, 2016). Case study research is a qualitative research method which can apply to the study of a single case or of multiple cases in real life. Defining features of case study research include, identification of specific bounded case events (to allow comparison), multiple forms of qualitative data collection, case “themes” are identified, and the conclusions of the research are derived by building on patterns, explanations, or general lessons from the study (Creswell & Poth, 2016; Yin, 2018).

Methodology & Methods:

Case Study

Qualitative research

Desk top review system failure documentation, prepare interview questions

Semi-structured interviews

Process tracing & Critical Decision Method (CDM)

Yin (2014) defines five approaches to conducting a case study as;

1. ***Determine*** if a case study is best examined using a case study.

   My chosen research topic is centred around the comparison of ATM system failure events which are contained within identifiable boundaries, i.e. the failure events resulted in restricted traffic levels being applied and a degraded system operation, and the systems affected are subjected to safety assurance procedures.

2. ***Identify*** the intent of the study and select the cases.

   While the occurrences are of a similar nature, they occurred in different countries and with different Air Navigation Service Providers (ANSP). The different perspectives and decision processes that enabled a return to full operations are addressed.

3. ***Develop*** procedures for data collection.

   Yin advocates the replication of procedures for use. Common events for the selected cases are used as interview cues, and for analysis i.e. decision moments or other common issues from the event description documents, and procedures/ CDM interview questions are based around these markers (Klein et al., 1989).

4. ***Specify*** the analysis approach.

   To conduct an embedded analysis of the decision processes to restore the system around the common markers and to see what "trade-offs" (Amalberti, 2013) were encountered by the organisation to allow a graceful reset of the system. Additional information on analysis methodology is included in section 3.3 below.

5. ***Report*** the case study, lessons learned and use case assertions.

   Interview data will be transcribed and analysed for common themes. Lessons learned and assertations are reported on.

3.2 Cases

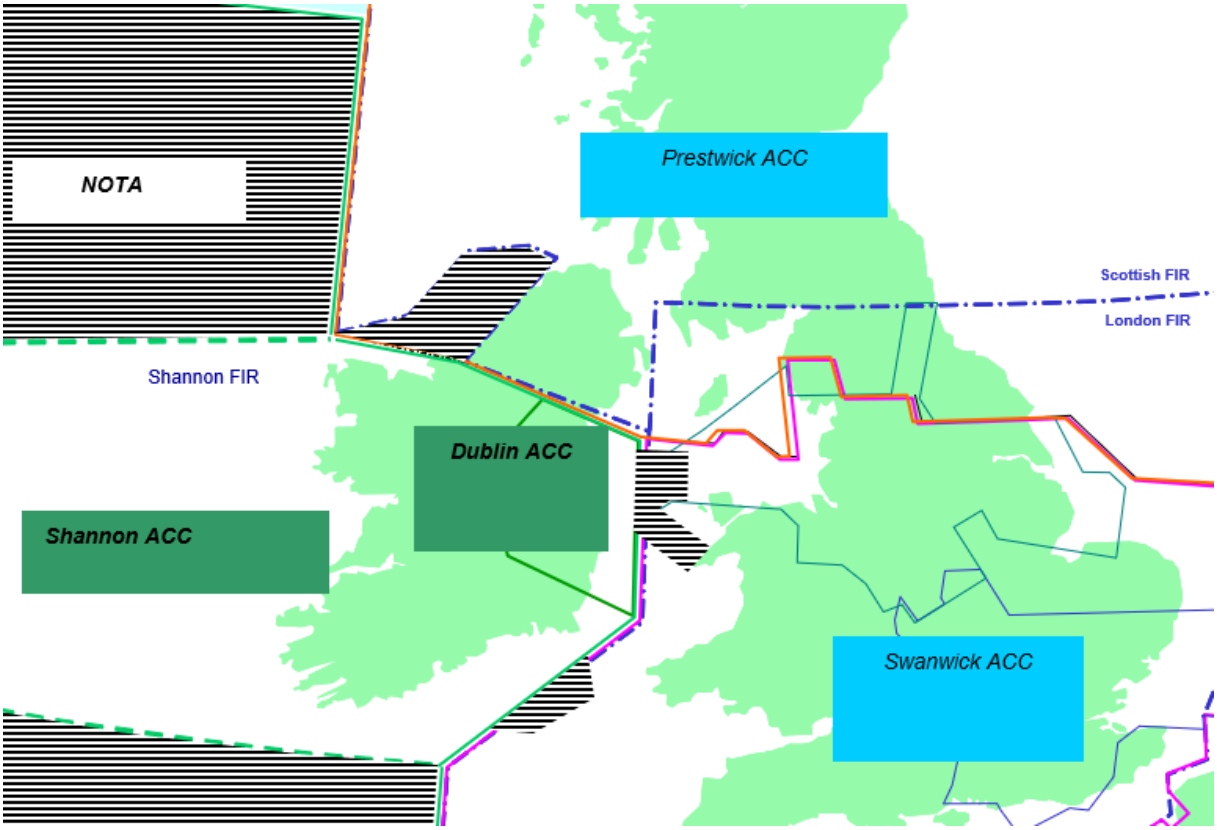
Two case studies involving ATM system failures experienced by different ANSPs, are selected for this research, the operation local area network (ONL) failure in Dublin ACC 2008, and the SFS Failure in Swanwick ACC UK 2014. Figure 6 below depicts a Map of Irish – UK airspace showing ACCs. This figure is included to add context to this research. A review of the system failure documentation which contain a description of the individual events (IAA ANSP, 2008a; IAA ANSP, 2008b; IAA SRD, 2009; Kontogiannis & Malakis, 2018; Walmsley et al., 2015) enabled the development of process tracing techniques and the conduct of semi-structured interviews based on CDM (Hoffman et al.,1998; Klein et al., 1989; Patrick & James, 2004; Raynard & Svenson, 2019; Woods, 1993).

The NATS failure, while significantly impactful on the congested airspace over the UK, was a relatively straight forward ATM failure in that the failure was resolved and the system was restored within hours without further repeat events. The IAA failure on the other hand had a prolonged period of uncertainty that impacted the decision-making process to return to operations. In the context of Perrow (1999) it can be considered a system incident involving the unanticipated interaction of multiple failures.

The most noteworthy consideration regarding the selection of the 2008 IAA ONL failure is the time lag since the occurrence and whether people would still remember it clearly. The event is perhaps the most interesting because of the prolonged period of uncertainty lasting eight weeks in total before the system was restored to full operational capacity. As such it was a high impact event within the organisation and the interviewees involved in this research still have vivid recollections of the period as a large amount of pressure to resolve the failures was experienced by all involved. This included instances such as individuals having to return early from family holidays, taking tense phone calls sheltering under a tree while attending a son's university graduation, consulting daily with airline and airport operators and experiencing their frustration first-hand, etc. This consideration is mitigated as much as possible through the development of both process tracing and CDM techniques applied at interview and throughout the analysis of data which is described later in this document.

Both cases were high impact events for the traveling public and were widely reported in the media at the time (Ando, 2014; Airport chaos 'could be repeated', 2008; Casey, 2008; Failure of radar causes chaos at Dublin airport, 2008; IAA may face cost of airport radar chaos, 2008; Kirka & Katz, 2014; Ladkin, 2015; More delays expected at Dublin Airport, 2008; Pitas, 2014; Radar malfunction causes chaos at Dublin Airport, 2008; Saran, 2015).

Figure 6. Map of Irish – UK Airspace showing ACCs



A third system failure which occurred in Naviair Copenhagen 2022 was also considered (Hollnagel et al., 2022) but it was rejected from this research as the IAA and Naviair systems are supplied by the same manufacture and share similar system architecture. This commonality could have led to an engineering comparison narrative about the system rather than a non-technology approach. It is important to note that the single point of failure detailed later in this research document was not present in the Naviair system, nor is it present in the current system in use in Dublin. The feature was designed out of the system by the manufacture following analysis of the Dublin ONL failure.

3.3 Procedures & Analysis

Document review

Documentation to be considered as bassline description reports, were used to provide extract information and timelines for each event are;

NATS

- NATS System Failure 12 December 2014-Final Report Independent Enquiry, Final Report dated 13 May 2015 (Walmsley et. al., 2015)
- Cognitive Engineering and Safety Organization in Air Traffic Management (Kontogiannis & Malakis 2018) contains multiple references to the failure and contains a detailed analysis of the event (by applying a STAMP analysis)

IAA

- The Safety Regulation Division Investigation Report (IAA SRD, 2009)
- Dublin HAZOP ONL LAN 080801 (IAA ANSP, 2008a)
- The ANSP occurrence Report into the ATM System Malfunction at Dublin Airport (IAA ANSP, 2008b)

Each case study was first reviewed individually and then jointly. A timeline for each event was developed (see Figures 7 & 8 in Chapter 4 below). The timelines developed are bespoke to suit the purposes of this research and are not an encompassment of all the failure events. They are edited and condensed from the bassline description documents listed above. Both timelines were reviewed multiple times to mark events, decisions taken, or what sources of information were consulted, etc., that were either individual or common, or aligned to the cases. The initial review stage contributed to the development of process tracing techniques and CDM questions, cues, and analysis (Hoffman et al.,1998; Klein et al., 1989; Patrick & James, 2004; Raynard & Svenson, 2019; Woods, 1993). They were later updated and

enhanced with interview data. Colour coding has been applied the timeline diagrams to provide for identification of common events to both failures where applicable.

3.4 Interviews

Semi structured interviews were prepared and conducted using process tracing techniques based on CDM. The CDM method is illustrated by Klein (Klein et al., 1989) as "Questions sometimes require the decisionmakers to reflect on their own strategies and bases for decisions." and where "The CDM is a retrospective interview strategy" intended to probe "nonroutine incidents that required expert judgment or decisionmaking.". This coupled with his assertion, "We have found the dialogue format to be essential in maintaining full cooperation and interest from participants." reinforced the decision to conduct verbal face to face interviews (Klein et al., 1989),

While the ONL failure in Dublin was in 2008, there are several strategies that can help mitigate any hindsight bias e.g. "by examining individuals' perceptions across several points in time" (Azungah, 2018) and using common procedures (Yin, 2018). The use of process tracing also allows for a retrospective analysis and the use of cues to trigger memory of specific moments within the prolonged period (Woods, 1993). It transpired that all interviewees exhibited clear recollections of the failure events. Their recounting of the events broadly matched the baseline reports, with only one minor exception. In relation to a specific recollection stated during one of the interviews. At the time the researcher was unsure of the accuracy of what was stated and used additional gentle cues to reaffirm what was being stated. The interviewee contacted the researcher the next morning to clarify that the specific comment made was in relation to a separate event. This clarification was considered in the analysis of the interview data.

Common procedures and interview questions were applied to each case study (Yin, 2018). Common markers in the case study documents were used in the conduct of the semi structured interviews with questioning on procedures applied and with cued questions e.g. failure(s) occurrence, involvement in failure, aftermath, diagnosis, rectification, etc.

Semi-structured Interviews were conducted face-to-face to create a more relaxed atmosphere and to allow interviewees speak more freely. Interviews were one to one with the researcher and the interviewee only. The interview audio was recorded, and the raw data transcribed for analysis.

The interviewees for each case study were selected from the Safety, Operations & Engineering disciplines. All interviewees were either Manager or Supervisor grade and each had more than 15 years' experience at the time of the events. Each interviewee had a direct involvement in the failure events as they happened. The number and calibre of interviewees provided for valuable diversity within both case studies in alignment with the perspective from the sage of the anthropological Mount Sinia (Flannery, 2009).

For all interviews the researcher travelled to accommodate the interviewees. In the case of the NATS, the researcher travelled to the UK on two separate occasions in October and November 2023, and hired a car to travel to meet the interviewees. In the case of the IAA interviews the researcher travelled to accommodate the interviewees choice of interview location in June and July 2023. The interview conservations were recorded on a Sony Icd-UX570 Digital Voice Recorder and simultaneously on an Evistr L157 USB Rechargeable Dictaphone Machine as a backup device.

The researcher's involvement in the IAA case (see Ethics sub-section below) provided an additional insight into the Dublin ONL failure, this insight allowed the researcher to ask probing questions during the IAA interviews. The use of semi-structured interview techniques

facilitated this and approximately 15-20 minutes were given over to this discussion at the latter stages of each interview. At the end of each IAA interview the researcher detailed some of their experience of the ONL failure event. This process revealed not only additional insight to the researchers understanding but also contributed to, and expanded on, the data collected. This tactic was also used during the NATS interviews and proved beneficial allowing for a comparison of events. The researchers experience as a controller and as active participant in the Dublin ONL event allowed for probing questions related to the interviewees experience. It also provided for "inter rater agreement" (IRA) and "inter-rater reliability" (IRR) (Armstrong et al., 1997, Chaturvedi et al., 2015) where events from one occurrence were validated through discussion with interviewees from the other occurrence. This was also applied throughout the analysis which provided independent cross case validation and identification of themes, strategies, and concepts.

Participants representative of the perspectives below were interviewed;

- Operations Manager/ Supervisor– Operational Service Delivery Perspective
- Engineering Manager Function – Engineering Manager Perspective
- Safety Manager – Safety Risk Management Perspective

Interview details are show in Table 1. below.

Table 1. Interview details

	Interview date	Duration (hours: minutes)	Words transcribed
Interviewee 1	12th June 2023	1:27	14,905
Interviewee 2	20th June 2023	1:17	14,643
Interviewee 3	10th July 2023	1:21	13,636
Interviewee 4	16th October 2023	1:42	19,102
Interviewee 5	1st November 2023	1:36	16,339
Interviewee 6	1st November 2023	1:40	17,748

3.5 Transcription & Analysis technique

Process Tracing

The use of process tracing is suited to retrospective events and allowed for data to be "correlated and combined to produce a record of participant data acquisition, situation assessment, knowledge activation, expectations, intentions, and actions as the case unfolds over time." (Woods, 1993). The use of cued interview questions in this method enabled a process to "map out how the incident unfolded including available cues actually noted by participants, and participants' interpretation in both the immediate and in the larger institutional and professional contexts." (Woods, 1993).

Ericsson and Simon argue that the use of verbal reports in process tracing are a source of data if the information has an enduring trace in long term memory (1980, 1993). The failures of both case studies were high impact events, and the interviewees involvement was such that the memories are still vivid. The use of nonverbal process measures i.e. the case study report documents, combined with the verbal process data provided for a converging interpretation with no contradiction between the two sources of data (Raynard & Svenson, 2019, pp. 271-273). The verbal data was checked against the case study documentation and the associated timelines. This allowed for cross validation of the interviewees data against the case study documentation.

As outlined above, a qualitative approach using a case study methodology was employed. For these reasons an approach employing inductive reasoning and analytic induction was adopted as being more suited to this research. This choice leads to several consequential practical considerations, firstly if safety is an emergent property as Cook advocates (2000) then a clear-cut approach would have been to follow the inductive approach. But alternatively, if you are moving back and forth between data and the theory during

analysis then the line between “inductive” and “deductive” becomes blurred. There is a distinction and perhaps a conflict between data driving the theory, and an emergent theory driving where you look in the data. Hyde expands on Yin and provides for this by asserting “A balance of induction and deduction is required in all research.” (2000), as is adopted in this research.

Azungah additionally describes the inductive approach to reasoning by citing Neeley and Dumas (2016), stating “It is a recursive process that involves moving back and forth between data analysis and the literature to make meaning out of emerging concepts” (Azungah, 2018). With that in mind transcribed interview data has been referenced to the common case markers and cross referenced against the narrative of those involved in the same failure, and against the narrative of those in the additional cases. The analysis of this data has led to the identification of common themes or lessons learned through an iterative process of back and forth. These are reported on in the results and analysis section of this research document.

Transcription process

The audio recordings for interviewees 1, 2, 3 & 4 were transcribed manually by playing back the audio recording and the researcher typing the text manually. The audio recordings for interviewees 5 & 6 were transcribed using an online automatic transcription tool called Sonix (https://sonix.ai) which converted audio Waveform Audio File Format (WAV) files into Microsoft Word text documents. This proved to be very effective, and the simultaneous transcription of the files took about 40 minutes to complete (including upload time of the WAV files which were around a Gigabyte each in size). The accuracy of the

transcription is incredibly accurate, above 95%. The automated transcriptions were subject to a manual audio review and editing process.

All transcripts were reviewed multiple times against the original recordings to check accuracy. All transcripts were reviewed to identify themes and to provide an analysis of the decision processes utilised to restore the system following an ATM system failure. A back-and-forth analysis between the transcribed data and the recordings was undertaken and a coding analysis for each interview was conducted. This coding analysis was consolidated into a spread sheet to allow for filtering and comparison. This process has produced multiple themes unique to each case, and also some themes common to both cases. These themes are reported upon in Chapter 4 Results and Analysis of this document.

Process Tracing interview data

The transcription data was reviewed simultaneously with audio recordings to capture any relevant inclinations which could add insight. The reviewed data was packeted and coded into various themes using Microsoft excel. The excel data was again coded into further packets and themes were refined. Multiple interviewee comments contained reference to more than one theme, in some cases it was possible to separate out these into individual themes, and in others some cross pollination remains. Consequently, some individual comments listed apply to more than one theme. Finally, emergent themes were expanded on, and researcher interview comments were added to the document as part of the coding process.

Through the analysis and collation of the transcription data the researchers' comments, in relation to the failure events, were collated into the spread sheet separately. This allowed for the researcher data to also be captured as part of the research. The comments of the researcher were cross validated both through interview discussion with the interviewees, and

with reference to the ONL case study documentation (IAA ANSP, 2008a; IAA ANSP, 2008b; IAA, SRD, 2009) to further mitigate for any researcher bias. Additionally, the extension of the tactic where the researcher detailed some of their experience of the event as part of the closing stages of the NATS interviews, provided for some IRA/IRR cross validation and identification of common themes and markers in both studies.

3.6 Ethics

Organisational/ Interviewee considerations

The intent of the research and written consent to record interviews was obtained for each interviewee with a signed consent form in accordance with Lund University's research ethics (2022). While the role/ function of the individuals interviewed is included, the names of those interviewed is not included and the data gathering is structured as originating from the specific *function* rather than role.

Some interviewees are no longer employed by the organisations, and in all cases any views or comments expressed are their own personal views or comments. All interviewees were given a written brief on the research and each interviewee signed a consent form.

The following is an extract from Lund ethics;

> "Data that is completely anonymised is not personal data and therefore the data protection legislation does not apply to it. The data is to be completely unidentifiable. This means that there is no key and that it is not possible to identify the individuals, even though it is possible to put together the different data that is being processed."
>
> (Lund, 2022)

Considering this, multiple deidentified direct quotes from interview participants are included in Chapters 4 & 5 section of this research. The inclusion of the data enriches the analysis and adds to the narrative and perspective of the operations, engineering, and safety domains.

Research Bias

Like Snooks declaration of not being a "disinterested observer" (2011) I must also declare a personal involvement in this research. During the ONL failures at Dublin, I facilitated the safety risk management (SRM) process, the development of mitigation measures and provided advice on the subsequent decision to return to full-service provision. I was a founding member of the Safety Management Unit (SMU) in the IAA at the time. However, my primary role is this work is that of a curious student and a researcher practitioner, with my curiosity triggered by having been an insider now trying to make sense of the broader process of returning to operations following a failure.

In the interest of academic research, any potential methodological limitation of subjectivity must always be considered. Qualitative data collection, analysis and interpretations are subjective and can be vulnerable to the researcher's biases (Azungah, 2018). Azungah cites Smith and Nobel stating, "In the process of analysing data, a researcher may intuitively search for data that confirm his/her personal experience and beliefs and fail to notice data that contradicts personal values" (Smith & Noble, 2014). In order to mitigate any potential bias, the research method included a cross check process and utilised a control narrative of the case study event taken from the independent report documents (IAA SRD, 2009; Walmsley et al., 2015). This control narrative was used to formulate and confirm the

event timeline which served as a guide to support the semi structured interview structure. The data analysis involved a validation check between interview data and the control narrative.

Where there was a conflict in research data collected from interview, including the researchers' contributions, the data and narrative from the baseline description reports (IAA SRD, 2009; Walmsley et al., 2015) was applied in the first instance, and in the second instance the interviewees narrative was applied. An example of this occurred in relation to the number of ONL failure events that occurred in Dublin. One interviewee stated "five failures in five weeks" while another asserted that there was only "three failures" with some repeat occurrences of the same failure event, and the IAA SRD report refers to six failures (IAA SRD, 2009. P. 4). In this case the researchers' recollection was not considered, and the SRD bassline description report data was used. This method was applied to both case studies to ensure consistency and alignment with a case study approach (Crestwell, 2016).

4. RESULTS and ANALYSIS

In this chapter the case studies are synopsised along with event timelines to allow review and comparison. Several identified themes and processes are provided and explored in the context of each case study. A timeline for each event was developed and is shown in Figures 7 & 8 below.

4.1 Case Study Synopsis

4.1.1 IAA ONL failure Dublin

Background to the failure

During the summer of 2008 there were multiple failures of the ATM System at Dublin ATC Centre. The main operational networked system failed on six occasions between the 2nd June and 9th July (on 2nd June, 4th June, 2nd July and three on 9th July) (IAA SRD, 2009. P. 4). After the initial failures a flow control rate was applied to restrict air traffic levels as a mitigation against repeat failures. As the failures continued over the following weeks there was intense pressure to increase traffic levels.

Initial investigations into the failures did not identify a root cause, despite considerable effort to resolve the technical issues. There was no apparent fix for the system. The IAA SRD report of the failure highlights “that the system did not fail in the predicted manner and the unexpected system behaviour was found to have influenced the operational response adopted to deal with the situation.” (2009, p. 4). The unexpected system behaviour caused radar screens that were not supposed to lose flight information, to suddenly lose flight information.

Consequently, confidence and trust in the system was knocked as the busy summer progressed. The air traffic flow control measures remained in effect for eight weeks after the first failure and to manage this period of uncertainty there were multiple risk assessments conducted aimed at increasing traffic levels.

Ultimately a *root cause* was identified as a combination of the failure of "a single network interface card together with a weakness in the FDDI LAN failure recovery mechanism" (IAA SRD, 2009, p. 41) and the solution to resume full-service provision became a numbers game. The overall probability for the total failure of the Flight Plan Information within the Cairde system of was $5.3 * 10^{-7}$ per hour of operation. That represents a MTBF of about 1000 years. This reliability figure which was independently validated, and ultimately provided compliance with the original system safety claim and allowed a return to full traffic. The ONL Radar Data Architecture Diagram is contained in Appendix A. Figure 9 shows Swanwick London Terminal Control (LTC) Operations room to give context to what an ACC looks like, and Figure 10 shows a map of NATS internal airspace division. These figures are included to provide some context to this research.

4.1.2 NATS SFS failure Swanick

Background to the failure

Extracted from the Walmsley Independent Enqury Report;

"The Incident started with the failure at 1444 UTC of a computer system used to provide information to Air Traffic Controllers managing the traffic flying at high level over England and Wales. This traffic includes aircraft arriving and departing from London airports as well as aircraft transiting UK airspace. The Controllers put agreed

procedures into action so as to limit traffic entering their area of responsibility and adopted manual methods for decisionmaking to ensure aircraft continue to maintain safe separation.

At 1455 all departures were stopped from London Airports and at 1500 all departures were stopped from European airports that were planned to route through affected UK airspace. The computer system was restored to the Controllers at 1549, but without its normal level of redundancy. By 1900, the ATS engineering staff believed they understood the cause of failure and full redundancy of the computer systems was restored at 2010. Traffic restrictions were gradually lifted from 1555 as confidence increased, and the final restriction was lifted at 2030. The disruption caused by the restrictions affected some airlines, airports and passengers into the following day.

The Incident occurred at 1444 on a Friday afternoon in the run up to Christmas. By 1500 there was information available on news broadcasts and social media suggesting that there was a UK air traffic control issue and this evolved into the story that UK airspace was closed. At Gatwick, the Controller managing take-offs had received a telephone call at 1448 from NATS at Swanwick to “Stop all departures” and relayed this information to the 3 aircraft queuing to line up for take-off. At about 1500 she was called by the pilot of the leading aircraft along the lines of: “My passengers are telling me that they’re hearing on Sky News that there’s an air traffic problem. Can you tell me something?” The Incident had quickly become a cause célèbre with the media.”

(Walmsley et al., 2015, p. 3)

Figure 7. IAA Timeline of ONL Failure Event

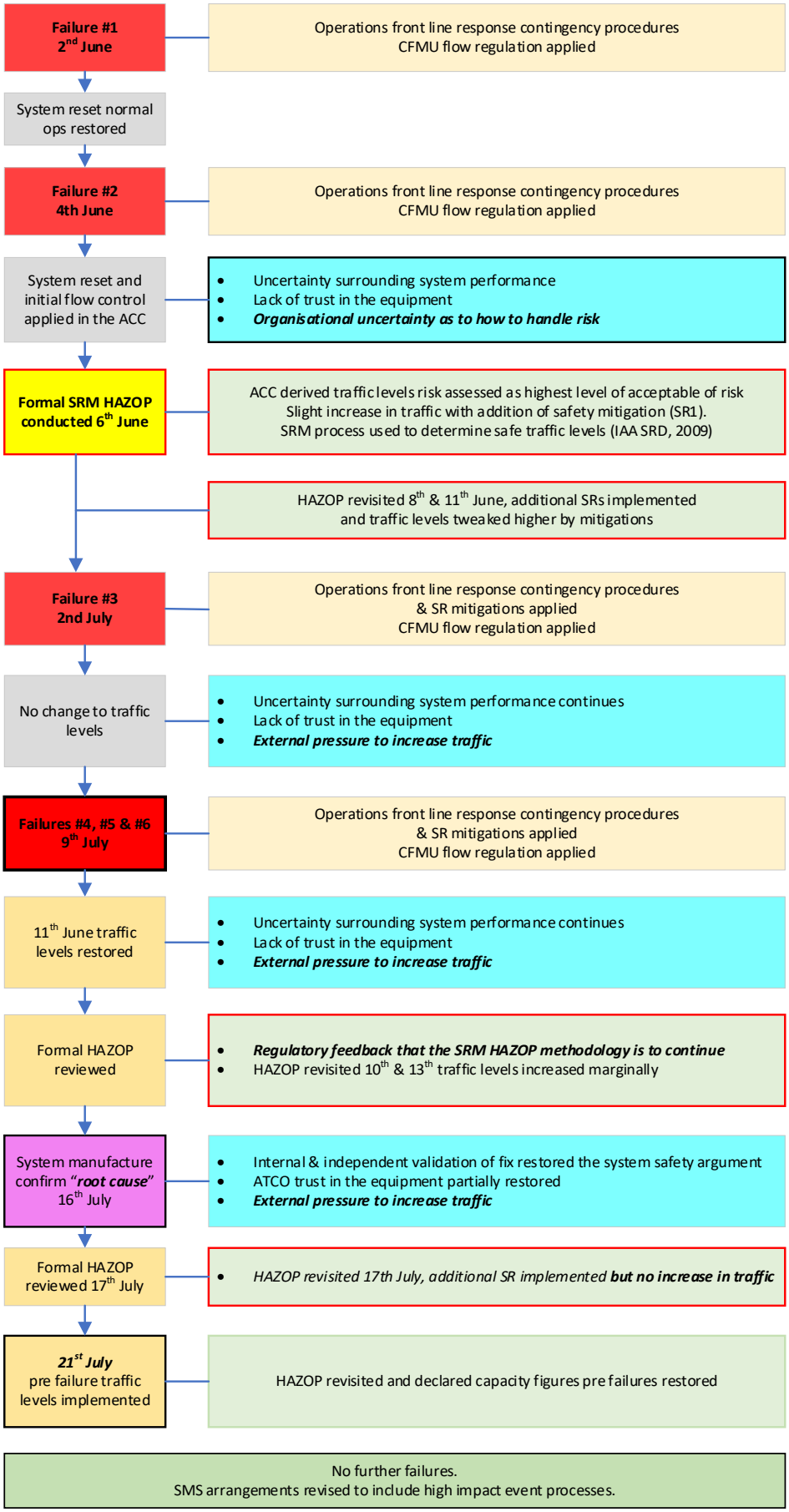


Figure 8. NATS Timeline of SFS Failure Event

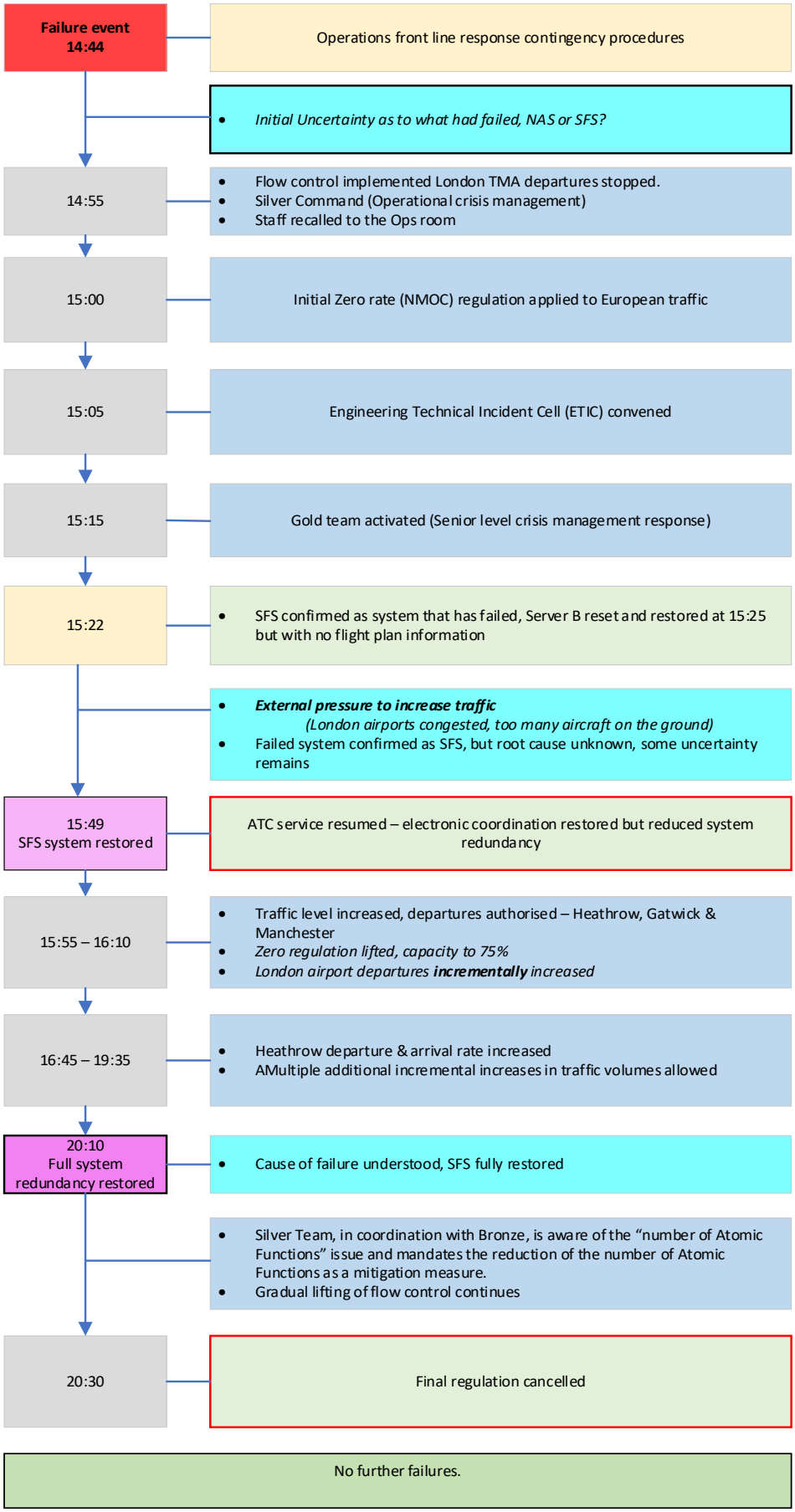


Figure 9. Swanwick London Area Control (LAC) Operations room circa 2014

Figure 10. NATS UK Airspace 2014

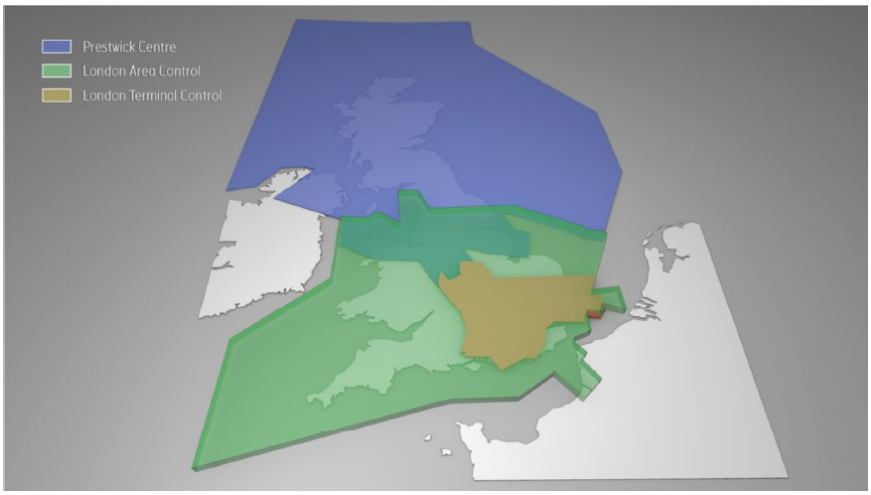
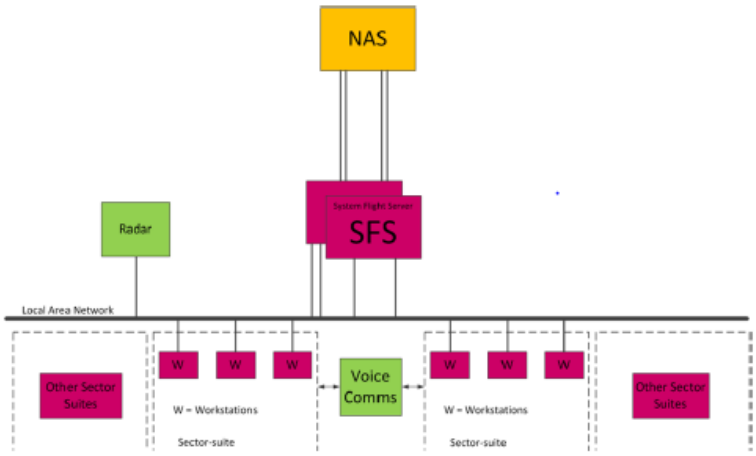


Figure 11. Systems used for control in LAC (simplified)



4.2 Themes

The following themes are introduced:

- Uncertainty and Trust
- Risk Management Processes
- Trade-offs, “flow control”
- Newtonian reasoning to explain a complex system (navel gazing)
- Root Cause Analysis & Fix
- The Human Bridge

Each theme is discussed below and how it relates to the case study events, either individually or jointly.

Note: Throughout the remainder of this document there are direct quotes from interview participants to illustrate and support the narrative. These isolated quotes appear in quotation marks, without an associated in-text citation. They are intended to non-identifiable, nor necessarily attributable to a specific case study.

e.g. “There was a degree of uncertainty”

4.2.1 Uncertainty and Trust

“Absolute transparency is a prerequisite of safety”
(de Tourtoulon, 2012)

NATS

While “Engineers in System Control at Swanwick received an indication from NAS and the LAC control and monitoring that the link between NAS and SFS was lost” (Walmsley et al., 2015, p. 70) there was an initial period of uncertainty within the London Area Control (LAC) Ops room at Swanwick, staff were uncertain which system had failed, SFS or NAS. The failure of one had degraded the other. The implication of a NAS failure was far greater that an SFS failure.

> “(NAS) provides a central air traffic data hub that supports operations across multiple NATS ATM services, including LTC (traffic generally below 21500ft), Prestwick Centre (PC) and other local NATS units at airports. Its shutdown would seriously impact operations across the UK FIR”
>
> (Walmsley, 2015, p. 31)

This period of initial uncertainty in the Ops room lasted for approximately 30-35 minutes and caused a large degree of concern as the impact NAS would reach beyond the Swanwick Centre. There is some comment in the Walmsley report on the initial response actions of those tasked with managing the unfolding situation, “to initially implement more conservative restrictions than those required.” (2015, p. 6). This comment may be influenced by hindsight bias (Woods, & Cook, 2002) as there was significant uncertainty during the initial period after the failure.

At an Engineering teleconference at 16:30 it was clear that the failure was known and there was some understanding as to what had triggered the failure, but the “root cause was not fully understood and the engineering design team could not yet be specific with

recommendations." (Walmsley et al., 2015, p. 7). This indicates that, while the system was considered stable, there was a continued period of uncertainty about what triggered the failure. They knew "it was something to do with SFS" but there was no clarity on a root cause.

Operations Rooms (ACCs) at Swanwick

There were two operational ACCs at Swanwick;

"NATS provides UK air traffic management in two adjoining regions, The Scottish Flight Information Region (FIR) and the London FIR. The London FIR is divided into:

(1) London Area Control (LAC), which handles civil aircraft over England and Wales in flight at high level.

(2) London Terminal Control (LTC) which is a smaller area, including the five main London airports, and covers aircraft generally flying below 21,500"

(Walmsley, 2015, p. 13)

SFS was not used in LTC, thus this research focuses on the events in LAC ACC.

IAA

"It has occurred; therefore, you should assume it can occur again"

As outlined above the ONL failure at Dublin also had uncertainty, but for a far longer time. Six failures over six weeks. There was a significant lack of trust amongst one team of controllers who had been exposed to two system failures, whereas other controllers who hadn't experienced any were sceptical of the mitigations, as were some senior managers. The

three failure events on the 9th July silenced the scepticism. The remaining operational staff lost trust and the controllers involved on the 9th were badly shaken by the events.

"you had to bring the staff along with it because if the staff lost confidence in you, or the equipment, if management lost the confidence of the staff, it was never going to come back."

Trust was damaged and it was not restored sufficiently enough to allow for a return to pre-failure traffic levels until assurances were received from engineering and the manufacturers technical report which included quantitative probability of recurrence values. These values were independently assessed before being accepted by operations. Staff briefings and consultations were conducted before a return to previous traffic levels.

> "And I felt so long as you could maintain that level of confidence, you weren't plámás-ing them, …but so long as that bond lasted, you knew you could keep running."

As discussed below several mitigations were implemented as "Safety Requirements" (SRs), some of which were specifically developed to help restore controller confidence e.g. SRs 7 & 14 (see Table 2. below). Additional dedicated staff briefing notices were issued following the 9th July to keep operational staff fully informed of the situation. Checklists were refined and reissued, technical briefs were given to staff and when the identification of the cause was known staff were also informed. All of these measures were intended to support staff and restore trust.

4.2.2 Risk Management Processes

In both the ONL & SFS failure events the front-line controllers involved in the responses had received degraded modes and fallback training for the respective systems. The immediate response of both sets of ATCOs resulted in maintaining a safe air situation during the system failures (IAA, SRD, 2009, p. 17; Walmsley et al., 2014, p. 3). This is testament to their skills and experience. This section looks at the risk management of the "system" failure and not the immediate management of air traffic out of the system.

NATS

From 14:55 until the end of the event later that evening, a formalised pre-prescribed set of crisis management procedures were invoked. This set of crisis management procedures established several working groups i.e. Senior management (Gold), Operational management (Silver) and Engineering specialist (Bronze). There were formal coordination protocols and in some cases group members were required to have received formal crisis training as part of their eligibility to sit at these groups. These procedures provided clearly defined lines of communication between the defined working groups and included a separate communications method for engaging with the airlines and airport authorities. All the procedures followed during the system failure had previously been subject to a safety assessment before being adopted and published. All staff in these groups had some grounding in the procedures and protocols that were applied.

One interviewee stated "Previously NATS were criticised at an audit for doing emergency training every year as opposed to every three years, because the regulatory minimum is every three years.". While another stated on reflection of the failure "I thought

that was a really good example of how to do things correctly.". In this instance there were several fortuitous circumstances that enabled a smooth diagnosis and a general response the SFS failure but perhaps it is the regular practice of contingency procedures that enabled this good fortune.

The general working relationships between staff at different levels was a consideration that NATS had been aware of and had actively taken steps at all levels across the organisation to improve working relationships and communications.

> "one of the best things we did for getting the relationships right. We put the engineer in charge of system control into the ops room. So, he was by the ops supervisors. …we put him in the ops room to break down those barriers between engineering and ops,"

IAA

> "Is there a voice saying, Is that going to be safe? And how do you know?"

The SRD reports states;

> "Dublin Operations management approached the SMU to gain reassurance and confidence that the safety management activity was appropriate and consistent with the SMS. In response the SMU suggested[1] that convening a HAZOP was the best way forward to systematically consider hazards and risks associated with a range of traffic capacities in order to determine an appropriate and safe level."

[1] The researcher was the member of the SMU who was approached by Dublin Operations management and who suggested convening a HAZOP to determine if the traffic levels in use at that time were safe in the context of the IAA's safety risk classification scheme. The researcher supported Operations with the facilitation of multiple HAZOP sessions from that date forward.

> "… changes to acceptable traffic capacities after the 6th of June were assessed and documented prior to implementation via the formal HAZOP process. HAZOP review meetings were convened as soon as any investigation development or ATM strategy suggested it was appropriate (including late on some evenings and at weekends)."
>
> (IAA SRD, 2009, p. 32)

The SRD report makes multiple references to the HAZOP process and indicates that the process and associated documentation provided the ANSP, and SRD as the Regulating entity, with evidence of a formalised risk management process. A formal HAZOP risk assessment document was updated after each of the risk assessment sessions between the 6th June and the 1st August 2008 (IAA ANSP, 2008a).

On the 6th June with mounting pressure to increase traffic we conducted a risk assessment of the operating levels of traffic in the ACC that had been arrived at on the morning of the previous failure two days earlier. The formal risk assessment process did three things, it documented the process, it derived mitigations and it provided a level of safety assurance which showed the unacceptable boundary that satisfied the regulator (cross validation from the NATS interviews supports this statement on the process applied).

> "you must do a risk assessment with the people at the coalface, the people with the first-hand knowledge of how they want to deal with it, it's not a matter of technology"

This was the first application of the "HAZOP" risk assessment process applied to an ongoing system failure (hazard) in a live operational environment. The process was a formal documented process in the SMS, but this was the first time it was applied to a live situation. Previously it was invoked when a change was being made to the operation where the change designer set out the anticipated hazards. In this instance the “hazard” were the failures and the behaviour that wasn’t anticipated. The system behaviour was described as “rogue” with inconsistencies between different CWPs during contingency mode.

The regulator wanted evidence of the risk management processes being applied to any changes or increases in traffic levels during this time. Additional HAZOP sessions were conducted where the hazard description and impact were further refined and mitigating safety requirements were derived. Participation of front-line ATCOs who had experienced the failures was essential.

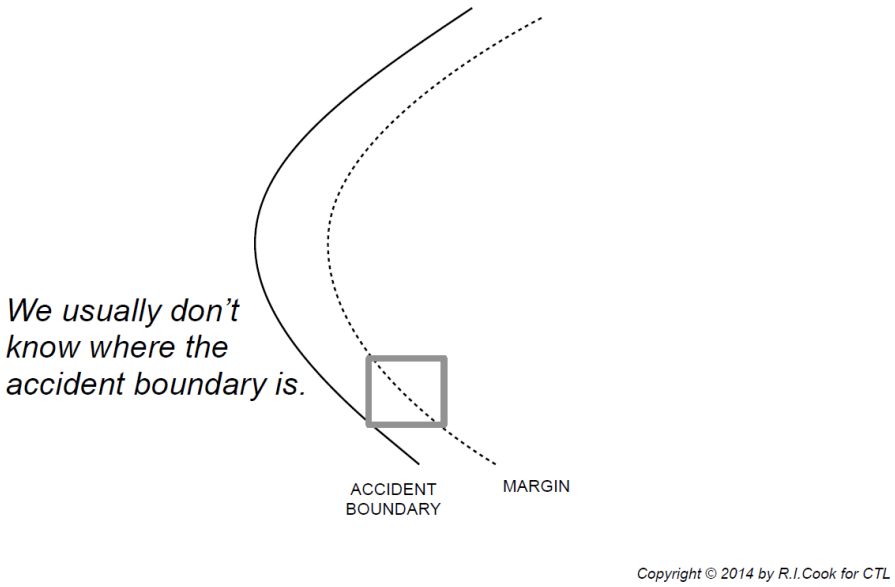
> “Nothing can replace firsthand knowledge, the firsthand knowledge of the people who were going to have to deal with the failures”

This was balanced with the perspective of staff who hadn’t been exposed to the failures to give an objective perspective. The HAZOP process was documented and it was a formalised way of tracking the safety requirement mitigations and their implementation. The safety requirements were recorded as SR’s 1-14. Examples of SR’s devised are presented in Table 2 below.

> "We kept getting closer and closer, and closer to that boundary, we kept nibbling away to get closer to the boundary. We had documented we were safe. And we had documented the edge, the boundary, we had documented where it wasn't safe."

Cooks (2014) adaptation from Rasmussen (1997) showing movement to the accident boundary and affirming that Safety is dynamic is shown in Figure 12 below.

Figure 12. Cooks adaptation from Rasmussen (1997)



Research data interviews revealed that as the situation prevailed over the weeks there was little appetite at the most senior operations management level to allow controllers call the shots on flow control (by way of risk assessment). There was mounting pressure to increase traffic levels. The adopted stance being, "you know we'll manage it by gut, by gut", meaning the controllers will manage it "by gut" effectively transferring all the responsibility from senior management to the controllers. There is a significant distinction here between these comments at avoiding responsibility and what Patriarca et al. (2018) argue as the application of extended responsibility and accountability associated with a distributed system resilience.

4.2.3 Trade-offs, "flow control"

NATS & IAA

As shown in the NATS Timeline of SFS Failure Event Figure 8. above, there were multiple applications and minor changes of flow control applied to air traffic. The failure occurred at 14:44 and all London TMA departures were stopped during the initial period of uncertainty. The effect of the failure meant that ATCOs would be presented with incorrect flight data, and associated dynamic flight plan information, e.g. clearance details and coordination data. While the loss of SFS didn't present an immediate safety threat, a prolonged lack of this information would impose a significant increase in controller workload. At 15:00 a "zero rate" was applied which would restrict the number of flights to zero and are normally applied only in unusual circumstances e.g. system failures. These restrictions were notified directly to the London TMA airports, and through the EUROCONTROL Network Management Operations Centre (NMOC). NMOC is responsible for the application of flow control measures across Europe, its primary function is to prevent overload and congestion. It serves to metre traffic into any airspace that is subject to contingency operations or reduced volumes of traffic. The application of these restrictions in the initial 45-minute period "resulted in up to 20 aircraft being diverted pre-emptively to alternative airports and around 150 flights being cancelled." (Walmsley et al., 2015, p. 7). In total, it is estimated that 230,000 passengers were affected by delays (including factors such as the delayed arrival of one flight often leading to the delayed departure of another), cancellations and diverted flights because of the failure (Walmsley et al., 2015, p. 4).

As the period of uncertainty ended and there was clarity as to which system had failed, the "Airspace Capacity Manager" (Walmsley et al., 2014, p. 14) confirmed formally to NMOC at 15:35 that the ACC was able to accept arriving traffic. There was significant

pressure to ease congestion on the ground at Heathrow, Gatwick and Manchester airports who were unable to allow any departures, but arrivals were still landing and causing congestion on the ground. Quite literally these airports were becoming saturated with aeroplanes. At 15:55 a regulated flow of departures was authorised for Heathrow, Gatwick & Manchester airports. Gradually over the next few hours there was a lifting of restrictions and at 20:30 the final regulation was lifted.

One of the tools available to middle management is the ability to make trade off decisions (Flin, 2017), these trade-off processes were applied by an application of flow control which reduced the number of aircraft in the airspace and kept aircraft on the ground, which in turn reduced the workload of the ATCOs at the front end of the failure. For the NATS event above it can be seen how a gradual lifting of these trade-off restrictions was achieved. In the case of IAAs prolonged uncertainty, the use of flow control through safety risk analysis applied the trade-offs required to protect production and to provide a level of safety assurance. During this prolonged time of flow control at Dublin flights were delayed but the daily schedule was accommodated by a steadier prolonged flow of traffic rather than the normal peaks and troughs throughout the day. The HAZOP record shows the implementation of the mitigating SRs provided the required safety assurance through the application of the formal risk assessment process (IAA ANSP, 2008a), this also showed the boundary of an unsafe situation where ATCO workload was considered too high. The derivation of SRs included trade-offs in the form of traffic restrictions, see Table 2 below.

"the risk assessment, it puts in the mitigating measures. You maintain the mitigating measures you come up with, ...until such time as, as you had assurance that, that it was fixed. You maintain the mitigating measures."

Table 2. List of SRs derived from the HAZOP process.

SR1:	Flow Restrictions to be monitored to evenly split traffic between North and South Sectors and to restrict overflights.
SR2:	That Flight Progress strips be available for all arrival traffic in the planning controller position for use as the alternate holding tool in the event of C2K entering emergency mode. Note: After Simulation using Flight Progress Strips safety requirement SR2 was considered not appropriate.
SR3:	Engineering Procedures to be followed when replacing a concentrator including testing on training rig prior to installation on ONL LAN.
SR4:	Engineering Procedures to be updated and followed when monitoring TMCS in regard to FDDI (significant alerts).
SR5:	ENG Manager will ensure that Engineers shall not perform any tasks on the ONL network (for which they have not been declared formally competent by the ENG Manager) outside the scope of defined SMC tasks. Individual Engineers shall be informed by Staff Notice of their individual responsibility not to perform any tasks on the ONL network outside the scope of defined SMC tasks (for which they have not been declared formally competent by the ENG Manager).
SR6:	Engineers involved in maintenance activities on the Network to be trained in any new procedures.

SR7:	A clear explanation of the recent ONL failures is to be published and all staff to be made aware.
SR8:	Engineering mitigations SR 3-6 to be put in place.
SR9:	An Emergency failure mode checklist for use in ATCO positions is to be published.
SR10:	All operational staff will be briefed on SR's 3-10 inclusive and a formal record of individuals briefed will be held by Operations.
SR11:	AON to be issued regarding the mandatory display of ASSR Codes
SR12:	That C2K malfunction Hold management AON be reissued with updated checklist and all staff be briefed on the changes made.
SR13:	Coordinator position to be staffed at all times between 06:30 and 23:30.
SR14:	That the Staff involved in previous failures to be formally de-briefed individually.

4.2.4 Newtonian reasoning to explain a complex system (navel gazing)

> "it's a bit like eh, this building being on fire and somebody reporting, 'Well while the building was on fire my PC was flashing, why do you think it was flashing?' When you know really, the bigger problem is the building was on fire."

A lot of time was spent analysing the loss of radar coupling, what could be called an "emergent property" (Cook, 2000), rather than accepting it as a by-product. The manufacture could only say it was most likely caused by the network interface card (NIC) failure because that was the only thing happening at the time. The loss of radar coupling impacts the radar symbol display to the ATCO, a normal label for an aircraft contains a callsign, altitude, ground speed along with additional flight plan information e.g. aircraft type, departure airport, arrival airport, cleared flight level. A de-coupled label only shows a four-digit code, aircraft altitude and ground speed, a single label displaying only this information is normally acceptable for a brief period, but to have all labels on a radar screen to suddenly display this basic information has a major impact on the ability to provide an ATC service.

> "we spent forever kind of exploring this as kind of navel gazing and stuff like that"

Chasing a Newtonian reductionist explanation for this coupling issue in a complex system also added to the uncertainty of the event and perhaps wasted time. The investigations revealed that "it was a traffic flooding situation, so (data) packets were getting dropped. But there was no deterministic outcome which packets got lost or didn't".

> "too much time was spend diagnosing this "rogue" behaviour, rather than looking for an explanation, just focus on either a mitigation or a fix"

Given that hazard analysis is designed around a known failure mode, and not around a "rogue" state there is limited value in chasing for an explanation or looking for additional "side effects". If it can occur, then focus on the mitigation.

4.2.5 Root Cause Analysis & Fix

NATS

From when the Engineering Technical Incident Cell (ETIC) group was convened at 15:05, until the nature of the failure was confirmed at 15:22, there was ongoing dialogue between the ATS engineers and a group of SFS Subject Matter (SME) ATCOs who had worked as part of the controller team involved in the SFS project implementation. These controllers were expert in the use of the system from an ATCO/ Ops perspective and it was this unique group that assisted in the initial diagnosis that SFS had failed and not NAS. It was fortuitous that this group of SME ATCOs/ Supervisors were in the building at the time, and they had responded to a Tannoy announcement recalling staff on breaks to the ops room.

One of the SFS project Controllers who responded that day helped investigate the initial uncertainty by using "a separate terminal to try and send messages to NAS and… got a response", as a result they were convinced "that actually it wasn't a NAS issue." And "within a very short period of time, that conversation turned into it's definitely an SFS problem. NAS is fine.".

> "it was just by chance you had like 3 or 4 best people you could have to come and help. And that proved to be really quite helpful."

By 20:30 on the evening of the failure there was enough knowledge of the causal factor of the failure to know if was related to the number of atomic functions, and terminals in watching mode assigned within the system (Walmsley et al., 2014, p. 34). This response echoes what Woods describes as "resilience as rebound from trauma and return to equilibrium" (Woods, 2015).

> "when people said, can you guarantee this is never going to happen again? The answer is, I can guarantee you this particular issue won't happen again, but I can't guarantee you that you won't see another system failure somewhere along the line."

IAA

> "we want another failure" I said, "You are joking?" and he said "No, from an engineering perspective that's how we do it."

In order to identify the nature of the failures in Dublin an FDDI LAN analyser was installed, and an expert consultant was flown in to set it up and monitor the system traffic. The idea at the time was that a repeat of the failure was required to be able to conclusively identify the root cause of the problem. There needed to be some method to capture a reoccurrence of the event and exclusively determine what was the cause of it, the analyser provided that method.

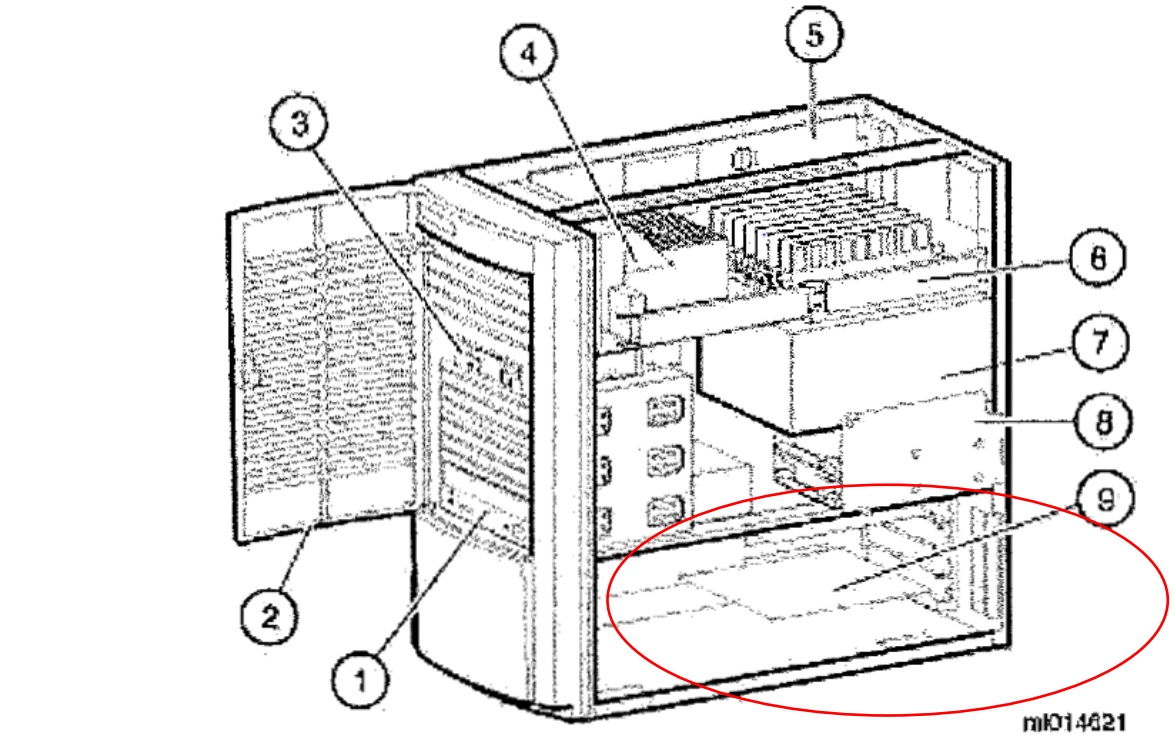
“It simply can’t fail” “But it must”!!!

The next day the system failed 3 times which resulted in the operations manager and the controllers further losing trust in the system. Ops responded by temporarily shutting the airspace. Operational controllers involved were badly shaken by the events. But it was these events that allowed a diagnosis of the faulty NIC card. The root cause was identified. Following theses failures, the faulty NIC card was replaced, and no further changes were made to the system. The equipment was fixed. The system was stable and didn’t fail again. Figure 13. below shows a workstation server with NIC card location.

> “We had said yes it is safe to go back into operations, we found the problem. What about the correlation? Well, we think its most likely associate with this card and the network effect traffic, well can you give proof conclusive? Eh no we can’t be conclusive yet”

Despite the NIC replacement and a stable system, the flow restrictions remained in place until the 1st August some 3 weeks later. During this time there was an inquest as to why there was a loss of coupling and the manufacturer spent a lot of time trying to diagnose why there was unexpected loss of correlation experienced at some positions, what was described as "rogue" behaviour. On counterfactual reflection there is a belief that a return to normal operations could have occurred sooner.

Figure 13. Cairde 2000 workstation showing NIC location (9) – (IAA SRD, 2009)



(9) = expansion slot card (e.g. Network Interface Card location)

Fault Finder Anecdote:

A critical member of the technical team was on a family holiday in Kerry, and he was needed back onsite in Dublin to help correct the issue, but his flight was unable to depart due to the ATC flow control restriction. Ironically without him returning to Dublin to help diagnose the fault, the flow control restrictions would remain in place. Needless to say the restriction on that flight was lifted and the airline/ passenger dialogue and the resultant telephone conversation between the airline and ATC went something like, “I’m sorry sir but you have to go to the back of the queue as the flight is delayed 3 hours due an air traffic control failure in Dublin”, “Eh, yes I know, I’m eh, needed back in Dublin to help fix it.” This was met with a blank stare from the airline representative, “Ring them and see”, the

subsequent phone call went something like this “Yes, he’s here now, can we get our slot lifted?” “slot cancelled” was the ATC reply.

Faulty NIC card anecdote:

“And subsequently the card was used in (the manufacturers factory), I don’t know where the card is now, but the card was subsequently sent to (the manufacturers factory) to test for the fix for dealing with removing the single point of failure. So, the card was actually used, so (the manufacturer) had developed a piece of code that in the event that beaconing occurred again, the server would shut itself down automatically and prevent the FDDI crash. This, the only way we could test it was with this card. So, the card was actually used.”

4.2.6 The Human Bridge

> “However, it is clear that the presence of several additional senior, qualified and experienced personnel who actively contributed to the initial failure diagnosis, supervision and management of the operational recovery in LAC was key, but possibly owed more to accident than design.”
>
> (Walmsley et al., 2015, p. 40)

In both failure events the role of the human in bridging the gaps between the failure of the system, the operation, and management was significant. In NATS the onsite presence and availability of “3 or 4 best people you could have to come and help” played a vital part in process clarifying the precise nature of the failure. As mentioned above in 4.2.5 there was ongoing liaison process between the ATS engineers and a group of SFS SME ATCOs, and between this group and supervisor, and as the situation progressed also with the Silver and Bronze crisis teams.

> "…just went and did a test that… would prove whether NAS was up or not... and came back and said, I think it's up. I've done this. And the engineers sort of said, well, yeah, you know, that's the right thing to do. Um, it looks like it's not a NAS problem. It must be an SFS problem. Um, and within a very short period of time, that conversation turned into it's definitely an SFS problem. NAS is fine."

This breakthrough provided the Ops supervisor with clarity that it was an SFS failure and not NAS "That was good news in some ways, but kind of we still didn't know quite what the prognosis was going to be.". It took human (SFS SME ATCO) expert knowledge to bridge the socio/ technical gap, which started the process to navigate out of uncertainty.

For the IAA ONL failure it took expert human assistance to intervene and install an FDDI analyser which enabled the identification of the root cause. The skill set required to do this was unique, the manufacture had to reach out for this assistance from a specialised consultant who was not a direct employee. Once the "root cause" of the ONL failure was identified and the assurance evidence presented by the manufacture to IAA, again consultant human intervention was sought to provide independent validation of the failure probability values given.

Within ATM in Europe a system is often considered as comprising of "people, procedures and equipment". When equipment fails then it's a people and procedures issue.

> "That's when you manage the system. That's when you manage the failure. So, it goes back to your question how do you restore a system, the people and procedures must be able to manage it. They must be able to manage it."

Procedures and processes in the guise of “checklists” played a role in both failures. Throughout aviation checklists play an integral role in day-to-day operations in aircraft and in ATC centres. However,

> “… nothing ever happens in the way it's supposed to. So, you know, kind of the experiences that I've had, very few, if hardly any, that I can think of were grab the checklist, do this, do that, do the other. It's always something else that comes into the mix that kind of rocks your boat or shakes your foundation of what you're supposed to do.”

The Walmsley report identifies checklists as contributing to a degree of uncertainty (Walmsley et al., 2015, p. 40), and the creation of SRs 9 & 12 (Table 2) in the ONL case were devised to improve the availability of appropriate documentation to ATCOs at the time of the failures.

The use of checklists in some unusual situations in ATC would appear limited as highlighted by Walmsley et al.;

> “The checklists also give guidance on steps that would be necessary to enable a recovery of the failed systems, but are silent on when such preparations need to be made and what flexibility exists to defer the more acute actions, such as clearing sectors of traffic, until more is known about the timeline for the technical recovery. They also lack guidance on the likely effect actions taken ‘locally’ may have on the wider aviation system and any options for tailoring responses to the conditions to minimise adverse impacts.”
>
> (Walmsley et al., 2015, p. 40)

This is further endorsed by interviewee comments;

> “So, it's really quite hard to get controllers to, to understand the complexity of systems. So, they just go, give me a checklist, I'll do this. What they don't get is when it actually happens, it will be quite a bit more than that simple checklist that you will have to assess and understand and know what to do with.”

> “most of my learning of how to cope in unusual circumstances has been by encountering unusual circumstances.”

There is a dependence on the ability of the human to bridge these limitation gaps. ATCOs are partially prepared for this by training for unusual situations and mentoring through on the job training (if any unusual situations are encountered).

> “That’s when you manage the system. That’s when you manage the failure. …the people and procedures must be able to manage it. They must be able to manage it.”

> “nothing can replace first-hand knowledge of the people who are going to, if the technology is removed, then it’s the people and procedures, if their training, and it’s their confidence,”

5. DISCUSSION

In this chapter several concepts observed during this research are remarked on and some of the themes and processes identified in Chapter 4 are expanded with researcher comment given. The research question is reprised from the introduction to restate the purpose of the research.

Research question: What processes support the decision to allow a return to full capacity when recovering from degraded operations in ATM?

5.1 Systems/ Complexity Theory

When the SFS primary system shutdown experienced an “exception”, the operation of SFS was transferred to the secondary standby system whose purpose was to provide redundancy. When the standby system experienced the same “exception” it also shutdown.

The ONL SRD failure report concludes that;

> “The root cause of Cairde 2000 emergency mode failures has been identified as a fault on a single network interface card together with a weakness in the FDDI LAN failure recovery mechanism. As a result of the failure causing an overload on the operational FDDI LAN, the system exhibited abnormal behaviour not consistent with the expected performance of C2K.”
>
> (IAA SRD, 2009).

It is not possible to always predict how a complex system will fail, both the SFS and the ONL events were double failures triggered by a single latent condition, i.e. system design flaws. Both failure events were consistent with what Dekker refers to as Complexity Theory

(Dekker et al., 2011) and safety (uncertainty), was presented as an emergent property (Cook, 2000; Leveson, 2011).

In both cases the primary root cause was confirmed by a process of going over the system logs and conducting a back-and-forth analysis of the overall system state and looking at individual components. This is problem solving journey is consistent with what Rasmussen refers to as "coping with complexity" (Rasmussen & Lind, 1981). The time pressures of a live ATM don't always allow for this type of detailed analysis in a dynamic environment. Returning to ATM operations should acknowledge the complexity of the system.

5.2 Retro Fitting Resilience to Existing Systems

> "there's absolutely no tolerance for an interruption of the service from an ATM provider"

So how do we mitigate for failure of a complex system? How do we prevent interruptions to service provision? The obvious initial answer proposed by both engineering interviewees when faced with the question, and by far the more costly, is to have a completely independent ATM system acting as a back-up. To implement this would require commissioning and staffing a second separate ATM system fed with up-to-date flight plan information, online H24 available for a seamless transfer of operations. Throughout the many weeks of ONL uncertainty, it was decided not to migrate operations to the back-up system as it would not have been able to handle the same volume of traffic that the degraded main C2K ATM system could.

There are opportunities to compensate for equipment failures by training for them and employing resilient human performance capabilities combined with the use of a dedicated set of resilient mitigating procedures. ATCO refresher training for abnormal situations is available and defined as;

> "Refresher training includes abnormal situations which, according to the definition includes circumstances which are neither routinely nor commonly experienced and for which an air traffic controller has not developed automatic skills and, more importantly, now also includes degraded systems training."
>
> (EUROCONTROL, 2017)

The inclusion of "degraded system training" is of course a welcome improvement and enables ATCOs to have some exposure to degraded modes, but it does not prepare for system "uncertainty", nor what Lanir outlines as "fundamental surprise" (1986). Typically, degraded modes training prepares ATCOs to respond to a specific element of the system that has failed and by applying the appropriate checklist. Because an ATC simulator is a controlled environment where every exercise is scripted, any simulated failure is carefully planned in accordance with expected system degraded performance i.e. failure modes as envisaged by the system designers. It doesn't address "uncertainty", or emergent properties.

> "if you don't really put the effort into making training realistic, it just becomes read a checklist and know where it is when you need it. You don't get the actual real thing, you've got the checklist. You've got 1000 other inputs that you weren't expecting, and you've got to make the most of that."

There are limitations of ATC simulators, they are primarily designed to simulate air traffic situations in a normal system state, and not to mimic operational failures. Unusual situation simulations, and degraded mode simulations account for a small part of simulator training exercises. In some refresher training cases, systems failures are covered by classroom power point presentations and a walk through of contingency checklists rather than dedicated simulation exercises. This can be because of simulator constraints in simulating degraded modes, or due to time pressures.

"There's no checklist for what happens. None of these failures ever go as prescribed."

If we practice for failure, uncertainty, and fundamental surprise, then we will be better able to manage it in a live operational environment. A proactive strategy for consideration is to develop a dedicated training module to specifically allow front-line operators to practice recovery from abnormal degraded system operations, to simulate unexpected system failure states, and to allow the front-line operators practice situation specific mitigations in an uncertain environment. Dedicated unusual situation training to provide the ATCOs with a resilient skill set to navigate uncertainty.

The development of "emergent" unusual system behaviour modules for ATCO training could be built around experience of actual system failures based on the accounts of the system failures that have occurred across Europe where unexpected system behaviour was experienced. Simulator scenarios where the participant is subjected to "fundamental surprise" by system behaviour could be developed and practiced allowing participants experience the phenomenon and to develop mitigations. This could be further enhanced by adopting an inclusive approach with the active involvement of engineering staff.

One of the enabling factors in the diagnosis of the system fault in the NATS case study involved the analysis by the human bridge e.g. the SFS SME ATCO in assessing what the system was doing. The deliberate fostering of an inclusive relationship between the human actors in the system i.e. the controllers and the ATS engineers, was enhanced by having ATS engineers situated in the ACC. This helped bridge the system gaps creating some resilience during the failure event. Including ATS engineers in specific practice simulations exercises and the debriefing sessions would help prepare both ATCOs and ATS engineers to work collectively during system failures. The more inclusive the preparations for dealing with abnormal situation more resilient our current system would become.

Additionally, the role that mangers play in the decision-making process is essential in a collaborative decision-making process. A collaborative decision-making process was well established at NATS with the interaction between managers and the SMEs from both ops and engineering proving crucial. There is a reliance on the technical experts to provide, in some cases, a simplified account of the system state and the failure to allow the management team to make an appropriate decision. In many cases there is a disconnect between organisational "management" crisis training and controller abnormal situation exercises, there is no cross participation. Resilience is not about reducing incidents, resilience engineering is about enhancing the capabilities of people and organisations that allow them to adapt effectively and safely under varying circumstances (Bergström & Dekker, 2019). Opportunities exist for more inclusive contingency practice exercises to enable business continuity.

5.3 Regulatory Considerations

"Managing risk is separate to regulatory assurance"

Uncertainty, or certainty for that matter, in the provision of ATC must of course take account of regulatory requirements. In the NATS case study pre-developed and approved NATS management System/ SMS processes included responsibilities which were defined and available for use i.e. the structure of the Gold, Silver & Bronze teams. They were well established and embedded with training for crisis participants as a prerequisite. These processes were less clear in IAA. In the extended period of uncertainty in the IAA case study, the application of the HAZOP process and the associated formal risk assessment was the organisational response to the uncertainty, in what could be considered "Resilience as graceful extensibility" (Woods, 2015). During the failure period there were formal meetings between the ANSP and the Regulator where the ANSP outlined how safety was being managed. The HAZOP process provided the ANSP with SMS safety assurance that the traffic scenarios implemented were of an acceptably safe level as defined in the SMS, "decisions to increase traffic levels were supported by safety assurance documentation (in the form of risk assessment and mitigation measures documented via the IAA's HAZOPs process)." (IAA SRD, 2009, p. 43).

"it's the safety management process that manages the failure not the regulation"

During uncertainty the focus is obviously on system recovery, and that the operation is safe. Ultimately however, confirmation that your safety argument is still valid is required. All changes within the ATC "functional system" (European Union, 2017) require a safety assessment, a safety argument, to ensure that the change is safe. This requirement is contained in COMMISSION IMPLEMENTING REGULATION (EU) 2017/373 (European Union, 2017). While this "373" regulation only came into effect in 2020, the preexisting regulation required similar safety assurances. For IAA there was a system safety case with stated system safety performance values. The overall probability for the total failure of the Flight Plan Information within the Cairde system of was a value of $5.3 * 10^{-7}$. per hour of operation. Once the failures occurred the safety argument became invalid, the theoretical numerical values were breached. Without a valid safety argument, the SMS risk assessment process provided safety assurance. To revalidate the safety case argument, the manufacture had to provide an assessment that both the ANSP accepted, and ultimately the regulator. As an additional measure, as mentioned above, the ANSP sought external validation of this.

During the brief NATS period of uncertainty there was a reliance on the pre-approved contingency procedures which were part of the unit's procedures. For IAA they employed the approved SMS HAZOP procedure and applied it to an uncertain situation to enable a resilience "graceful extensibility when surprise challenges boundaries" (Woods, 2015) and to manage the event. It formed a crucial part of the IAA ANSP demonstrating safety risk management of the failures and following the 2008 ONL failure the IAA conducted an SMS review of the processes to apply to a high impact safety event and the SRM HAZOP was adopted as a formalised process to apply in such events.

Similarly, to the chasing for an explanation of the “rogue” system behaviour being equated to “navel gazing” and the assertion that the focus should be on a mitigation or a fix, during uncertainty the situation should be managed by SMS SRM procedures.

Of course, the poignant issue worth noting is that SMS processes are subject to regulatory acceptance prior to introduction, but these procedures should refer to their application during high impact events and periods of uncertainty. Risk assessed and controlled steps taken with the SMS can provide a level of safety assurance required to navigate the situation through a resilient approach. The line between where regulation ends, and SMS begins can be blurred and could possibly introduce tension between the two functions. Thankfully the IAA ANSP had a good working relationship built with the Regulator which proved beneficial in demonstrating safe management of the situation.

5.4 Return to Full Capacity

During the 2008 ONL failure HAZOP process the safe boundary of risk acceptance was nudged multiple times as the six weeks progressed (see Figure. 12 above). As the boundary was nudged, the HAZOP process became about supporting the frontline operator rather than increasing traffic levels. The failure event was described by those ATCOs who had experienced it, and the focus became on providing the support necessary to enable the controllers to cope with another failure. Mitigations were developed to restore controller confidence, dedicated briefings on how the failures were manifesting themselves, checklists for failure events, support tools to manage traffic e.g. back up traffic lists, etc.

The initial response for each failure was the front-line controller using contingency procedures. The events were traumatic for the controllers involved with an instant increase in

workload dealing with the failure. The contingency procedures they applied imposed an immediate reduction in air traffic to compensate.

In Swanwick after the initial ATCO response and the implementation of crisis management procedures, and from that point forward, there was a collaborative decision-making process invoked across the organisation, from the Ops supervisor, the ETIC, Bronze, Silver and Gold groups. There was a documented and trained for crisis management operation in play across the organisation and from 15:55 onwards there was a gradual easing of restriction and an increase of air traffic until 20:30 until the final restrictions were lifted.

It was a practiced crisis plan which provided for a coordinated response, but there was a sentiment expressed that there could have been a return to operations sooner, during the time period when Silver team were waiting for a clearer understanding of the situation approximately between 15:45 and 18:00. Silver adopted a measured response that took account of communications processes across the operations, engineering, and management groups. This sentiment is worthy of consideration in discussion. From the time NAS to SFS recovery was completed at 15:45 and electronic coordination was restored there was a subtle lag between Silver team and the Ops room.

> “We don't know why it broke so it could break again. But we know that the troops, if you like, the controllers, had all experienced it failing at a reasonable level of business and have coped with it. Now you've got to take on board the fact that some of those might have been traumatized by that event. Still unsure. Lots of talk about it, but actually going from 100% down to like 20% is quite a traumatic experience.”

The sentiment is expressed from the perspective that given the ATCOs had just dealt with the failure, and while it may be unclear what the root cause was, and that it could fail again, the ATCOs knew what to expect if it did. There was an ongoing consultation process between the Ops Room Supervisor, the local area Supervisors and the ATCOs to take account of that sentiment and their confidence.

Between the 15:45 and 18:00 period in Swanwick the feeling in the Ops room was that it was an SFS failure, it had been restored, controller confidence was dented but now there was very little traffic and there was a feeling that there could have been an increase in traffic sooner.

> "you've got loads of, of workload capacity to actually manage an unusual event if it happens. So, so you can make a quite a reasonable judgment that says we can go a bit higher"

A comparison from the IAA event can be made to a similar sentiment expressed about "first-hand knowledge" and consultation of the ATCOs who experienced the failure event.

> "nothing can replace first-hand knowledge…. the first-hand knowledge of the people going to have to deal with the failure. Which would have been the controllers…"

At times of uncertainty, it's the relationships between people that count. With pressures to increase traffic it's the front-line operators i.e. the controllers, the supervisors and the ATS engineers who must be consulted to gain an understanding of their state of confidence and understanding of the level of uncertainty, and if they can manage it. If the system is uncertain and subject to rogue behaviour or unintended consequences, and if the

procedures can't take account of the, possibly unknown, emergent properties, then what can the human deal with?

5.5 Research (& Researcher) Learning

In the course of this research, I learned a number of unexpected things. Initially the ONL prolonged period of uncertainty seemed to be a more interesting event, but the NATS failure event proved to be equally, if not more, fruitful and offered some fascinating insights. The amount of cross over between the two events was unexpected given to different environments, timeframes, external and organisational pressures. Perhaps in hindsight this is not unexpected as both organisations perform the same function albeit in different environments.

The maintenance of a safe space between Rasmussens boundaries and the operating point is key to navigating uncertainty in a dynamic ATM environment (Cook & Rasmussen, 2005). While the front-line operators (ATCOs, Ops Supervisors & ATS Engineers) are key to negotiating the production boundary, it needs a protection counterbalance. But a counterbalance capable of dynamic movement (in line with Rasmussens model), not a hard and fast line, or position. The counterbalance role must assume some, or perhaps all, of the responsibilities of service provision. Either way it's about risk, the level of risk, and the acceptance of risk. An inclusive ATCO/ ATS Engineers/ Supervisor & Management approach can help with creating a more resilient system capable of graceful extensibility and sustaining adaptability (Woods, 2015, 2018).

6. CONCLUSION

In this chapter the conclusion is delivered below.

6.1 Conclusion

This research looked at managing uncertainty and recovery processes following failure of a complex sociotechnical system. The objective of this research is to see what operationally deployed processes supported the resumptions of ATS while emerging from, or still in, an uncertain degraded system state. A qualitative case study approach using semi-structured interviews was adopted. Failure event report documentation was reviewed with face-to-face interviews.

The emergence of safety strategies displayed in dealing with uncertainty contained elements of a resilience system. The trade-offs required to achieve the safety processes necessary to resume service provision demands were fine tuned to edge, closer to the edge of an unfamiliar safety boundary (for both events) in a dynamic setting with multiple adjustments as both systems returned to service. Operating close to the edge and flirting with boundaries can result in a tightly coupled ATM system becoming brittle where any sudden surge in demand can pushing beyond acceptable limits (Cook & Rasmussen, 2005).

While the current popularity of resilience as a design prerequisite for new systems doesn't address the requirement to achieve resilience in current operational systems, there are opportunities to adopt some practices and strategies that can enhance resilience. The interplay between boundaries and actors is key to navigating uncertainty in a dynamic ATM environment. While the front-line operators (ATCOs, Ops Supervisors & ATS Engineers) are key to negotiating the production boundary, there needs to be protection counterbalance strategies i.e. proactive risk management and continuous performance monitoring of the people and procedures.

Several items are proposed in Chapter 5 for consideration; complexity considerations, retro fitting resilience i.e. dedicated abnormal degraded system operations training module to specifically allow front-line operators to practice for failure, uncertainty, and fundamental surprise, & inclusive training strategies and regulatory considerations, these discussion items are intended to be of use to those tasked with navigating uncertainty in degraded Air Traffic Management operations in preparing for such events.

REFERENCES

Airport chaos 'could be repeated'. (2008, September 19). Irish Examiner. https://www.irishexaminer.com/news/arid-30378381.html

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science*, 37, 109-126 https://doi.org/10.1016/s0925-7535(00)00045-x

Amalberti, R. (2013). Navigating safety: Necessary compromises and trade-offs - theory and practice. *Springer Briefs in Applied Sciences and Technology*, *9789400765481*. https://doi.org/10.1007/978-94-007-6549-8

Ando, B. (2014, December 12). *Flights disrupted after computer failure at UK control centre*. BBC News. https://www.bbc.com/news/uk-30454240

Armstrong, D., Gosling, A., Weinman, J., & Marteau, T. (1997). The place of inter-rater reliability in qualitative research: An empirical study. *Sociology*, 31(3), 597-606. https://doi.org/10.1177/0038038597031003015

Ávila-Cabrera, J. J. (2016). The subtitling of offensive and taboo language into Spanish of Inglourious Basterds: A case study. *Babel. Revue internationale de la traduction/International Journal of Translation, 62*(2), 211-232. https://doi.org/10.1075/babel.62.2.03avi

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative Research Journal*, *18*(4), 383–400. https://doi.org/10.1108/QRJ-D-18-00035

Bergström, J., & Dekker, S. (2019). The 2010s and onward: Resilience engineering. In *Foundations of Safety Science* (pp. 391-429). Routledge. https://doi.org/10.4324/9781351059794-11

Bergström, J., Van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety*, *141*, 131-141. https://doi.org/10.1016/j.ress.2015.03.008

Bieder, C. (2022). *Safety Management Systems and Their Origins: Insights from the Aviation Industry* (1st ed.). CRC Press. https://doi.org/10.1201/9781003307167

Casey, C. (2008, July 13) Regulator has stake in failed system. Times Media Limited https://www.thetimes.co.uk/article/regulator-has-stake-in-failed-system-dz86kdjbmfp

Chaturvedi, S. R. B. H., & Shweta, R. C. (2015). Evaluation of inter-rater agreement and inter-rater reliability for observational data: an overview of concepts and methods. *Journal of the Indian Academy of Applied Psychology, 41(3)*, 20-27.

Cook, R. I. (1998). How complex systems fail. *Cognitive Technologies Laboratory, University of Chicago. Chicago IL*, 64-118.

Cook, R. I. (2000). How Complex Systems Fail Cognitive technologies Laboratory. *New York*, 1–5.

Cook, R., & Rasmussen, J. (2005). "Going solid": a model of system dynamics and consequences for patient safety. *BMJ Quality & Safety,* 14(2), 130-134. https://doi.org/10.1136/qshc.2003.009530

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage publications.

Dearden L. (2015, May 27). *Belgian airspace closed: Air traffic control failure grounds all flights causing 'chaos' at Brussels airport and diversions around Europe*. The Independent https://www.independent.co.uk/travel/news-and-advice/belgian-airspace-closed-air-traffic-control-failure-grounds-all-flights-causing-chaos-at-brussels-airport-10278525.html

Dekker, S., Cilliers, P., & Hofmeyr, J. H. (2011). The complexity of failure: Implications of complexity theory for safety investigations. *Safety Science,* 49(6), 939-945. https://doi.org/10.1016/j.ssci.2011.01.008

de Tourtoulon, A. (2012). *Trust Me I'm The Pilot.* Fastprint publishing.

Ericsson, K. A., & Simon, H. A. (1980). Verbal reports as data. *Psychological Review*, 87, 215–251. https://psycnet.apa.org/record/1980-24435-001

Ericsson, K. A., & Simon, H. A. (1993). *Protocol analysis: Verbal reports as data* (2nd ed.) Cambridge, MA: MIT.

EUROCONTROL. (2017). ATC Refresher Training Manual (Edition 1.0). https://learningzone.eurocontrol.int/ilp/pages/mediacontent.jsf?catalogId=4451312&mediaId=5383232

European Union. (2017, March). *COMMISSION IMPLEMENTING REGULATION (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011.* EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0373

Failure of radar causes chaos at Dublin airport. (2008, July 10). Irish Independent News. https://www.independent.ie/regionals/herald/failure-of-radar-causes-chaos-at-dublin-airport/27878289.html

Flin, R. (2006, April). Managerial Resilience and Safety: Vasa to NASA. In *SPE International Conference and Exhibition on Health, Safety, Environment, and Sustainability* (pp. SPE-98541). SPE. https://doi.org/10.1201/9781315605685-20

Flannery, M. C. (2009). The value of pigeons. *The American Biology Teacher*, 71(7), 430-434. https://doi.org/10.2307/20565347

Hand, J. (2023, September 3). *Nats air traffic control fault: Experts reflect on three days of chaos*. BBC News. https://www.bbc.com/news/uk-66685349

Hoffman, R. R., Crandall, B., & Shadbolt, N. (1998). Use of the critical decision method to elicit expert knowledge: A case study in the methodology of cognitive task analysis. *Human factors*, 40(2), 254-276. https://doi.org/10.1518/001872098779480442

Hollnagel, E., Laursen, T., & Sørensen, R. (2022). A day when (Almost) nothing happened. *Safety Science*, *147*(April 2020). https://doi.org/10.1016/j.ssci.2021.105631

Hollnagel, E., & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC press. https://doi.org/10.1201/9781420038194

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd.. https://doi.org/10.1201/9781315605685-1

Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative Market Research: An International Journal*, *3*(2), 82–90. https://doi.org/10.1108/13522750010322089

IAA ANSP. (2008a). *Dublin Hazop ONL LAN 080801*. IAA.

IAA ANSP. (2008b). *Report into the ATM System Malfunction at Dublin Airport, Issue: 19th September 2008*. IAA.

IAA may face cost of airport radar chaos. (2008, July 12). Business Post. https://www.businesspost.ie/legacy/iaa-may-face-cost-of-airport-radar-chaos/

IAA SRD. (2009). *REGULATORY INVESTIGATION FINAL REPORT Cairde 2000 System Malfunctions, Issue: 1*. IAA.

ICAO - International Civil Aviation Organization. (2005). *Annex 2 – Rules Of The Air.* (10th ed.). https://store.icao.int/en/annex-2-rules-of-the-air

ICAO - International Civil Aviation Organization. (2018). *Annex 11 – Air Traffic Services*. (15th ed.). https://store.icao.int/en/annex-11-air-traffic-services

IFATCA – International Federation of Air Traffic Controllers' Associations. (2022). *100 Years Air Traffic Control 1922-2022 an incomplete history, "The ALDIS Lamp"*. https://www.atc100years.org/the-aldis-lamp/

Kirka, D. & Katz, G. (2014, December 12). *London hit by air traffic control computer failure*. The Associated Press. https://phys.org/news/2014-12-london-air-traffic-failure.html

Klein, G. A., Calderwood, R., & Macgregor, D. (1989). Critical decision method for eliciting knowledge. *IEEE Transactions on systems, man, and cybernetics*, 19(3), 462-472. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=31053

Kontogiannis, T., & Malakis, S. (2018). *Cognitive Engineering and Safety Organization in Air Traffic Management*. CRC Press. https://doi.org/10.1201/b22178

Kontogiannis, T., & Malakis, S. (2019). A system dynamics approach to the efficiency thoroughness tradeoff. *Safety Science*, *118*(June), 709–723. https://doi.org/10.1016/j.ssci.2019.06.011

Kontogiannis, T., Malakis, S., & McDonald, N. (2017). Integrating operational and risk information with system risk models in air traffic control. *Cognition, Technology and Work*, *19*(2–3), 345–361. https://doi.org/10.1007/s10111-017-0409-3

Ladkin, P. B. (2015, May 28). *Report into air traffic control failure shows we need a better approach to programming*. The Conversation. https://theconversation.com/report-into-air-traffic-control-failure-shows-we-need-a-better-approach-to-programming-42496

Lanir, Z. (1986). Fundamental surprise. *Eugene, OR: Decision Research, 424*.

Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety science*, *49*(1), 55-64. https://doi.org/10.1016/j.ssci.2009.12.021

Lund University. (2022, April 22). *Research ethics and animal testing ethics*. Retrieved December 14, 2023, from https://www.staff.lu.se/research-and-education/research-support/research-ethics-and-animal-testing-ethics

Malakis, S., Kontogiannis, T., & Smoker, A. (2023). A pragmatic approach to the limitations of safety management systems in aviation. *Safety Science, 166*, 106215. https://doi.org/10.1016/j.ssci.2023.106215

McDermid, J. A., & Whysall, P. J. (2015, October). Disruption to UK air traffic management on 12th December 2014: Analysis and lessons learnt. In *10th IET System Safety and Cyber-Security Conference 2015* (pp. 1-6). IET. https://doi.org/10.1049/cp.2015.0291

More delays expected at Dublin Airport. (2008, July 11). RTE News https://www.rte.ie/news/2008/0710/105558-air/

Neeley, T. B., & Dumas, T. L. (2016). Unearned status gain: Evidence from a global language mandate. *Academy of Management Journal*, *59*(1), 14–43. https://doi.org/10.5465/amj.2014.0535

Orban, O. (2017, October 1). Air Traffic Control delays in Germany after brief closure of Karlsruhe UAC. Aviation24.be https://www.aviation24.be/air-traffic-control/dfs/air-traffic-control-delays-germany-brief-closure-karlsruhe-uac/

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety science*, 102, 79-100. https://doi.org/10.1016/j.ssci.2017.10.005

Patrick, J., & James, N. (2004). Process tracing of complex cognitive work tasks. *Journal of Occupational and organizational Psychology*, *77*(2), 259-280. https://doi.org/10.1348/096317904774202171

Perrow, C. (1999). *Normal accidents: Living with high risk technologies*. Princeton university press. https://doi.org/10.1515/9781400828494

Pitas, C. (2014, December 13). Computer fault identified as UK flight chaos abates. Reuters. https://www.reuters.com/article/us-britain-airlines-closure-idUSKBN0JQ1M620141212/

Radar malfunction causes chaos at Dublin Airport. (2008, July 10). This Is Tucson. https://tucson.com/news/radar-malfunction-causes-chaos-at-dublin-airport-authorities-warn-of-more-trouble-thursday/article_001f86e8-5dc2-5248-a48b-4b89de0ab9b8.html

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rasmussen, J., & Lind, M. (1981). Coping with complexity. *HG Stassen (Ed.)*.

Rasmussen, J., Nixon, P., & Warner, F. (1990). Human error and the problem of causality in analysis of accidents. *Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences*, 327(1241), 449–593. https://doi.org/10.1093/acprof:oso/9780198521914.001.0001

Raynard, R., & Svenson, O. (2019). Verbal Reports and Decision Process Analysis. In Schulte-Mecklenbeck, M., Kühberger, A., & Johnson, J. G. (Eds.), *A handbook of process tracing methods for decision research* (2nd ed.). (pp. 271-273). Routledge. https://doi.org/10.4324/9780203875292

Reason, J. (1997). *Managing the risks of organizational accidents.* Ashgate. https://doi.org/10.4324/9781315543543

Saran, C. (2015, May 26). NATS failure down to bug from the 90s and redundant code. ComputerWeekly.com. https://www.computerweekly.com/news/4500246924/Nats-failure-down-to-bug-from-teh-90s-and-redundant-code

Seale, C., Silverman, D., Gubrium, J. F., & Gobo, G. (2003). Qualitative research practice. *Qualitative research practice*, 1-640.

Singh, K., Maiti, J., & Dhalmahapatra, K. (2019). Chain of events model for safety management: data analytics approach. Safety science, 118, 568-582. https://doi.org/10.1016/j.ssci.2019.05.044

Smith, J., & Noble, H. (2014). Bias in research. *Evidence-Based Nursing*, *17*(4), 100–101. https://doi.org/10.1136/eb-2014-101946

Snook, S. A. (2011). *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Princeton University Press. https://doi.org/10.2307/j.ctt7sf5p.4

Statt, N. (2018, April 3). *The EU's air traffic control system failed, and up to 15,000 flights may be grounded*. The Verge. https://www.theverge.com/2018/4/3/17193814/eu-eurocontrol-brussels-system-failure-flight-plans-airlines-delays-grounded

Subotic, B., Schuster, W., Majumdar, A., & Ochieng, W. (2014). Controller recovery from equipment failures in air traffic control: A framework for the quantitative assessment of

the recovery context. *Reliability Engineering and System Safety*, *132*, 60–71. https://doi.org/10.1016/j.ress.2014.06.010

Swiss airspace re-opens after ‘technical malfunction’. (2022, June 15). Reuters. https://www.swissinfo.ch/eng/business/swiss-airspace-reopens-after-air-traffic-control-problems/47675112

'Technical issue' briefly cripples Swedish air traffic (2016, May 19). The Associated Press. https://phys.org/news/2016-05-technical-issue-briefly-cripples-swedish.html

Vaughan, D. (2021). *Dead reckoning: Air traffic control, system effects, and risk*. University of Chicago Press. https://doi.org/10.7208/chicago/9780226796543.003.0001

Vijayan, V., & Smoker, A. J. (2021). Exploring goal conflicts and how they are managed in a biomedical laboratory using Rasmussen's model of boundaries. Applied Biosafety, 26(S1), S-43. https://doi.org/10.1177/1535676020919624

Walmsley, R., Anderson, T., Brendish, C., McDermid, J., Rolfe, M., Sultana, J., Swan, M. & Toms, M. (2015). NATS System Failure 12 December 2014–Final Report Independent Enquiry. *Final Report dated*, *13*. https://www.caa.co.uk/media/r42hircd/nats-system-failure-12-12-14-independent-enquiry-final-report-2-0-1.pdf

Wicaksono, H., Rahman, F., & Sahib, H. (2020, October). The ineffective way of using gun light to deliver light sign for aircraft with total radio failure or receiver failure. In *IOP Conference Series: Earth and Environmental Science* (Vol. 575, No. 1, p. 012179). IOP Publishing. https://doi.org/10.1088/1755-1315/575/1/012179

Woods, D. D. (1993). Process tracing methods for the study of cognition outside the experimental psychology laboratory. In G. A. Klein, J. Orasanu, R. Calderwood, & c E.

cY N. N. J. Zsambok (Eds.), *Decision making in action: Models and methods* (pp. 228–251). Ablex.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability engineering & system safety, 141*, 5-9. https://doi.org/10.1016/j.ress.2015.03.018

Woods, D. D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. *Environment Systems and Decisions*, 38(4), 433-457. https://doi.org/10.1007/s10669-018-9708-3

Woods, D. D. (2023). Resolving the Command–Adapt Paradox: Guided Adaptability to Cope with Complexity. Chapter 8 in Le Coze, J.-C. & Journé, B. (Eds.), *Compliance and Initiative in the Production of Safety: A Systems Perspective on Managing Tensions & Building Complementarity*. Springer Briefs in Safety Management, Dec. 2023.

Woods, D. D., & Cook, R. I. (2002). Nine steps to move forward from error. Cognition, technology & work, 4, 137-144. https://doi.org/10.1007/s101110200012

Yi, J., Ma, C., & Zhao, J. (2022). Advances in Resilience Engineering for Air Traffic Management Applications. *Journal of Physics: Conference Series*, *2364*(1). https://doi.org/10.1088/1742-6596/2364/1/012028

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications Ltd. https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

Yu, M., Erraguntla, M., Quddus, N., & Kravaris, C. (2021). A data-driven approach of quantifying function couplings and identifying paths towards emerging hazards in

complex systems. *Process Safety and Environmental Protection*, *150*, 464–477. https://doi.org/10.1016/j.psep.2021.04.037

APPENDIX A – Case Study 1. ONL Radar Data Architecture Diagram