Institution: University of Glasgow
Unit of Assessment: B11 – Computer Science and Informatics
Title of case study: Shaping Policy, Legislation and Regulation in European Air Traffic Management
1. Summary of the impact

The European Air Traffic Management system currently handles around 26,000 flights daily, with ultimate responsibility for the lives of almost 800 million passengers and crew every year. Professor Chris Johnson's research has directly influenced policy, legislation and regulation across Europe's air traffic control, including the current guidelines on software development in Air Traffic Management, which were incorporated into European law in 2008. He has led the way in harmonising computer infrastructure standards across different agencies throughout the EU, building defences against cyber-attacks and playing a vital role in improving passenger safety.

2. Underpinning research

Professor Chris Johnson's (Professor of Computing Science, University of Glasgow, 1994-present) research initially focussed on the use of formal methods to analyse the causes and consequences of failures in critical infrastructure. These included assets such as transportation networks that are critical to the functioning of society and the economy. Rather than proving that a specification meets particular design requirements, his research took an innovative approach by analysing the potential consequences when specifications failed to meet safety requirements. For example, identifying numerous mismatches between the software requirements and the environmental assumptions that led to the loss of the Mars Polar Lander and Deep Space 2 missions. One area of his underlining research used both linear interval and branching temporal logics to develop simulations of infrastructure failures and their interdependencies. These formal tools and the associated executable temporal logics extended by Professor Johnson in his Prelog toolset can be used post-hoc to support accident analysis for a known failure, but can also be used pre-hoc to support prospective risk assessment. Much of this work was conducted jointly between Professor Johnson at the University of Glasgow and C. Michael Holloway's group at the NASA Langley Research Center, beginning in 2003. In 2011, collaboration between Professor Johnson, Mike Fodroci (Head of Safety for the International Space Station) and Andrew Herd (Senior Software Engineer at the European Space Agency), aimed to identify whether recent funding cuts across the human space programme might lead to safety concerns – for instance, in crew and ground-team training on the International Space Station. Both these projects resulted in joint publications. Johnson has also applied these techniques in joint work with US Air Force Space Command, comparing concerns with the North American WAAS satellite augmentation system and the EGNOS, European infrastructure. These systems have been approved to integrate GPS signals into safety-critical applications.

This research, initially developed for the space sector, has also been applied in three recent European Railway Agency projects (2011-12) with the aim of increasing the consistency of accident investigations across member states. Although formal modelling informed elements of this work, a greater emphasis was placed on semi-formal tools for member states with very different resources. This built on Professor Johnson's previous research into the impact of bias on causal analysis in incident and accident investigations. For example, he pioneered some of the very few comparative studies (2012) in which teams of investigators from different agencies (including the US National Transportation Safety Board, Norwegian Oil and Gas Industry, Brazilian Space programme and the French aviation industry) have used different modelling techniques on the same scenarios to determine whether differences between the tools or individual investigators can bias the technical recommendations of accident reports.

In 2012, Professor Johnson's underlying research returned to its formal roots – extending Boolean Logic Driven Markov Processes (BDMPs) to consider the safety impacts of cyber-attacks. In many contexts, cyber-attacks have a limited impact; servers can be taken off-line and subjected to a forensic analysis. However, in ATM, separation must be maintained even if malware is detected in

some portion of the computational infrastructure. BDMPs provide quantitative means of assessing the different probabilities of a successful cyber-attack in the presence of routine (non-malicious) system failures. Professor Johnson's work with BDMPs has identified vulnerabilities in the existing safety procedures that have been developed as a guide for the new generation of space-based European navigation systems.

3. References to the research

C.W. Johnson, Michael P. Fodroci, A. Herd and M. Wolff, Promoting Resilience in Human Space Flight at a Time of Fiscal Pressure. In L. Ouwehand (ed.), *Proceedings of the Fifth Conference of the International Association for the Advancement of Space Safety*, Paris, France, NASA/ESA, 2011, Report SP-699, ISBN 978-92-9092-263-6 (with European Space Agency and NASA's Head of Safety for the International Space Station). *

C.W. Johnson, Using Assurance Cases and Boolean Logic Driven Markov Processes to Formalise Cyber Security Concerns for Safety-Critical Interaction with Global Navigation Satellite Systems. In J. Bowen and S. Reeves (ed.), *Proceedings of the 4th Formal Methods for Interactive Systems Workshop 2011*, Limerick, Ireland, 2011. (keynote talk) EGNOS is the first satellite based augmentation system to be approved for use in European safety-critical systems; it provides ways to improve the reliability, continuity etc of GPS). *

Summary of work on incident investigation linked to support for UK CAA and German DFS: C.W. Johnson, Computational Concerns in the Integration of Unmanned Airborne Systems into Controlled Airspace. In E. Schoitsch (ed.), *Proceedings of SAFECOMP 2010, 29th International Conference on Computer Safety, Reliability and Security*, Springer Verlag, 142-154, (doi:10.1007/978-3-642-15651-9_11) LNCS 6351, 2010.

C.W. Johnson, B. Kirwan and T. Licu, The Interaction Between Safety Culture and Degraded Modes: A Survey of National Infrastructures for Air Traffic Management, *Risk Management*, (11)3:241-284, ISSN 1460-3799, 2009 (doi:10.1057/rm.2009.10) (with Head of Safety/Security in European Aviation Network Management and Senior European Human Factors Engineer).

C.W. Johnson and I.M. de Almeida, An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03, Safety Science, (46)138-53, 2008 (work on Brazilian space programme showing comparisons between accident analysis techniques). (doi.org/10.1016/j.ssci.2006.05.007)

C.W. Johnson and C.M. Holloway, A Longitudinal Analysis of the Causal Factors in Major Maritime Accidents in the USA and Canada (1996-2006). In F. Redmill and T. Anderson (eds.) *The Safety of Systems: Proceedings of the 15th Safety-Critical Systems Symposium*, Springer Verlag, London UK, 85-104, ISBN 978-1-84628-805-0, 2007 (with NASA Langley, showing comparative approach between investigators looking across a wide range of incidents and accidents). *

C.W. Johnson and C. Shea, The Contribution of Degraded Modes of Operation as a Cause of Incidents and Accidents in Air Traffic Management. In A.G. Boyer and N.J. Gauthier (eds.) *Proceedings of the 25th International Systems Safety Conference*, Baltimore, USA, International Systems Safety Society, Unionville, VA, USA, 616-626, 2007.

* best indicators of research quality

4. Details of the impact

Through his chairmanship (2009-11) and on-going membership of the Scientific Advisory panel for the Single European Sky ATM Research Programme (SESAR), Professor Johnson has helped to address the technological and operational dimension of the Single European Sky initiative. SESAR directs the research of industrial aerospace participants (e.g. Boeing, European Aeronautic Defence & Space) to ensure that air traffic management (ATM) for Europe is modernised to meet

present and future needs. In 2013, SESAR received an additional €2 billion to continue its work into the Horizons 2020 programme with the Scientific Advisory panel directing the €100 million basic research programme.

The European ATM system currently handles around 26,000 flights daily with forecasts indicating that air traffic levels are likely to double by 2020. The EU's approach to management of this growth and addressing related safety concerns was to organise airspace into functional blocks defined by traffic flow rather than national borders. Such a project was not possible without common rules and procedures at European level. The Single European Sky initiative was launched by the European Commission in 1999 to introduce common rules and procedures that would facilitate such an approach. The Eurocontrol agency manages the European ATM network and effectively looks after the operational side of the Single European Sky, while SESAR supports developments in technology and procedure.

Formulating consistent infrastructures standards across Europe

Between 2008-13, SESAR involvement took Professor Johnson to over 18 member states to assist their ATM engineering teams. The focus of the work has been to transfer best practice and contribute to consistency across Europe; in particular, Professor Johnson has supported the use of rapid risk assessment techniques in everyday configuration tasks for ATM software. The technical focus of this work has been to use accident and incident investigation methodologies to identify patterns of failure across Communication Navigation Surveillance technologies. The consequences of these failures are an increasing cause for concern, considering the key role that computational systems play in maintaining separation in congested airspace around hub airports, such as Heathrow.

Contributing to the development of European policy and legislation

As the only academic member of the European Committee on Contingency Planning in Air Traffic Management, Professor Johnson used his research expertise to develop guidelines for the mitigation and recovery from major incidents in ATM; meeting requirements for Commission Regulation (EU) No 1035/2011. Professor Johnson also authored guidelines to support the European Regulatory Requirement on Software Engineering in Air Traffic Management (ESARR6), which provide ATM safety regulatory bodies and service providers with a uniform and harmonised set of requirements to ensure that the risks associated with the use of software in safety related ground-based ATM systems are reduced to a tolerable level. These guidelines were incorporated into European law under Regulation (EC) N° 482/2008 on 30 May 2008 and enacted following software related fatal accidents involving ATM infrastructures at Linate and Charles de Gaulle (both stemming from problems with Digital Surface Movement Radar System) and Uberlingen (involving software re-sectorisation in Area Control Centre Zurich). Professor Johnson's research into the use of formal and semi-formal techniques for incident investigation prior to 2008 played a key role in identifying the technical causes of these accidents. In particular, the Uberlingen ECF diagrams presented in his 2003 Handbook on Accident and Incident Investigation were used by EUROCONTROL (the European Organisation for the Safety of Air Navigation) to review the success of the European Strategic Safety Action Plan (2002-06 but influencing all subsequent legislation). Europe has not suffered any fatal accidents stemming from ATM software failures since 2008, although the frequency of lower consequence incidents is increasing with the complexity of the underlying software infrastructures.

In 2013, Professor Johnson was the only academic to be invited to the UK working group on risk assessment for cyber security in ATM, reporting to the Cabinet Office. Also in 2013, he was asked to direct the European research programme on cyber security within ATM as part of the €100 million portfolio of SESAR research, responsible for directing the scientific assessment of projects within the programme.

5. Sources to corroborate the impact (indicative maximum of 10 references)

European Guidelines for Contingency Planning for Air Navigation Services (including Service Continuity), Brussels, Edition 2, 2009. Acknowledgement of Johnson's work on pg 5.

Degraded Modes Safety for Operational Engineering, October 2009. Joint initiative between Professor Johnson and EUROCONTROL to increase consistency of systems safety engineering across member states, document distributed to engineers and senior management in more than 22 states. Johnson's contribution is summarised on pg 22, refers to his work on rapid risk assessment and mishap analysis following Linate and Überlingen.
SESAR press release on behalf of the Commission with names and biographies of the international experts on the Scientific Advisory Panel, including reference to Professor Johnson as founding President of the group.
Public version of the policy report prepared for SESAR and the Commission on major ATM disruptions: Chris Johnson and Alain Jeunemaitre, Risk and the Role of Scientific Input for Contingency Planning: A Response to the April 2010 Eyjafjallajökull Volcano Eruption, In A. Alemanno (ed.) Governing Disasters; The Challenges of Emergency Risk Regulation, HEC Paris, France. 2011. ISBN 978 0 85793 572 4 [available from HEI]

The following individuals can provide evidence of the impact of Professor Johnson's work:

- Head of the Safety Unit, Network Management Directorate, EUROCONTROL, Brussels, Belgium.
- Senior Research Engineer, Software System Safety Engineering Team, NASA Langley, Virginia, USA.
- Director, Corporate Safety & Security Management, DFS Deutsche Flugsicherung GmbH, German Air Traffic Management, Langen, Germany.
- Safety Expert for Satellite Systems, US Air Force 50th Space Wing, Air Force Space Command HQ.
- Senior Information Security Officer, European Network Information Security Agency, Heraklion, Greece.