Situation Awareness, projection and the problems of degraded modes in ATM maintenance activities

By Professor Chris Johnson

Chris Johnson is Professor of Computing Science at Glasgow University in Scotland. He heads a research team that focuses on the identification and analysis of systems failures across safety related industries. Over the last decade he has worked with organisations as diverse as NASA, the US Army and the UK National Health Service. He has worked on ATM related projects for more than a decade and is currently investigating the importance of safety culture in the systems engineering teams that are often called upon to 'fix things' when failures occur.

In the early 1990s, the US military were involved in a remarkable series of experiments intended to find out how good we are at anticipating when we need to sleep. In these experiments, army personnel who had been on night duty were asked to predict the likelihood of falling asleep in the next two minutes. The majority, who did fall asleep, failed to predict that this would happen. In other words, fatigue prevented them from accurately estimating their need for sleep.

In the same way, maintenance staff and systems engineering teams often go to extraordinary lengths to maintain underlying infrastructure. Often, those who are most directly involved in maintenance operations are the least able to accurately identify the risks and hazards that can arise during those procedures. This desire to support ATM operations can compromise safety unless it is carefully monitored.

Over the last two years, I have coordinated a survey of best practice in how ANSPs deal with what are termed 'degraded modes of operation'. These degraded modes are defined as occurring whenever ATM services continue to be provided without the support of critical components of the underlying systems infrastructure. Many service providers use minimum equipment lists to identify when such situations occur. However, in many cases systems engineering teams will struggle to support operations even though items on these lists may be temporarily unavailable. In extreme cases, loss of services has reached an unacceptable level.

The aim of the Degraded Modes project has been to identify the reasons why individuals and teams struggle to maintain levels of service even when critical elements of their operational infrastructure have been lost through system failures, maintenance activities or scheduled updates. This is an important topic because 'coping strategies' have been identified in the causes of both the Linate and Überlingen accidents. In both accidents, we were surprised that so many people worked so hard to maintain levels of service when they might have suspended operations in order to preserve system safety.

At Linate, there was a breakdown in communication between the groups responsible for the maintenance of the infrastructure and the operational staff. The gradual degradation of taxiway signage, the loss of critical runway lighting systems and the failure to update the analogue ground movement system gradually removed critical infrastructure support from the ATCOs. The ANSV investigators[9] found that these latent failures made the degraded operating modes more serious under reduced visibility; they found it 'remarkable' that the radar and lighting systems had not been improved in the months and years before the accident. Such observations are symptomatic of communications problems between maintenance management and teams of operational staff who must continue to maintain levels of safe service in the face of failures. At Linate it was particularly difficult for aircrews to use existing documentation to gain an accurate understanding of the operational environment.

Crucial markings between taxiways were indicated by yellow signs indicating the name of each route and by lines leading in the appropriate directions. However, the yellow line indicating the path of one taxiway had been partially obscured by black paint to cover an old path that had been modified. In consequence, the Jeppesen charts used by the crews did not provide accurate information about the state of the taxiways.

Similarly, the BFU report into the Überlingen accident[10] argues that the degraded infrastructure at ACC Zurich had a profound impact on the causes of the accident. "The radar system was being operated in the fallback mode and the optical Short Term Conflict Alert was not available; the telephone system was not working properly; the technicians working in the control room added to the controller's stress; operating two workstations with two different sectors from radar screens set to different scales was an additional strain and would probably not have been accepted by a supervisor although traffic flow was low; the ATCO could not use a headset as he was operating radios of two workstations.

Back to Content

The regulatory authority had already voiced concern about SMOP (Single Manned Operation Procedures). The general work conditions during the night shift and the additional strains of the night of the accident did not meet the requirements for SMOP" [page 92 of the English language version of the report].

Most of the previous work on 'degraded modes' of operation has been on operational teams of ATCOs, as they maintain service provision under degraded modes of operation. The novel aspect of our present project is that it focuses on the systems engineering teams that are responsible for maintaining the integrity of the underlying ATM system infrastructures. In particular, we have identified the problems in 'projection' or the anticipation of the impact that systems engineering changes will eventually have on operational staff. For example, we interviewed one team in an ACC where engineers had two backup banks of processors. The active system was labelled by a placard warning technical staff not to take this unit off-line as it would directly compromise service provision. During one maintenance period, an engineer moved the placard so he could access the fallback processors. His co-worker then mistakenly shut down the active system. The systems engineering team and safety management group responded by placing both processor banks in separate locked cages. All was well until, a problem arose with the primary unit and the key for the cage could not be brought down to the maintenance staff in time to prevent a 'contingency' from occurring. In both of these incidents, there was a failure by maintenance teams to anticipate or project the consequences of their actions in moving the placard and in restricting access to the processors.

Key recommendations:

A key finding from our work is that we do not need to reinvent a series of novel or expensive techniques to address some of the problems created by degraded modes of operation for systems engineering teams. In contrast, we argue that techniques, which are already used to train operational staff, should be extended to support technical and engineering activities:

Simulation and problem-based training tools for systems engineers.

Many of the incidents that have been reported to the project could usefully be incorporated into simulation exercises for systems engineers that enable them to develop appropriate planning and communication skills, just as the same scenario and problem based training techniques are already used for operational staff. These techniques are already widely used by some ANSPs but are completely unheard of in other ECAC states.

Low-Cost Operational Risk Reviews.

In many of the incidents that we have reviewed an initial risk assessment identified the hazards that might arise during maintenance and systems engineering operations. However, these assessments were seldom revised as problems arose during the performance of complex engineering tasks. In some cases, this meant that the risk information was barely worth the paper that it was written on. Other organisations, in particular the US Army, have developed simple easy-to-use risk assessment forms that encourage maintenance teams to consider the consequences of their actions as they work on an engineering problem.

Closer Integration of Operations and Systems Engineering.

There is a growing divide between systems engineering and operational staff in some ANSPs. This divide includes, but is not limited to, pay differentials and terms of service; it also includes differences in background and in education. This divide is corrosive to safety culture. Some engineering teams have described ATCO's as the 'David Beckham's of ATM' who

'hang up their headphones and go home while we work late'.

Conversely, operational staff criticise engineering teams who care more about the performance of their networks than they do about the problems of Air Traffic Management. It is difficult to underestimate the importance of this divide. Future plans for Single European Skies rely on more extensive integrated systems that will require significant maintenance if degraded modes of operation are not to have an adverse effect on safety.

[9] For a synopsis of the report and link to the original ANSV report see http://www.skybrary.aero/index.php/MD87%2C_WX_RI%2C_Milan_Linate%2C_2001

[10] For a synopsis of the report and link to the original BFU report see http://www.skybrary.aero/index.php/B757%2C_LOS%2C_Uberlingen_Germany%2C_2002

Back to Content