COMBATTING MANAGERIAL COMPLACENCY IN SPACE MISSIONS

C.W. Johnson

Department of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson, Email: Johnson@dcs.gla.ac.uk
+44 (0)141 330 6053 (Tel.), +44 41 330 4913 (Fax).

ABSTRACT

Human factors techniques have made significant contributions to the safety of space missions. Physiological models help to monitor crew workload and performance. Empirical studies inform the design of operator interfaces to maximize finite cognitive and perceptual resources. Further progress has been made in supporting distributed situation awareness across multi-national teams and in promoting the resilience of complex, time critical missions. Most of this work has focused on operational performance. In contrast, most space-based mishaps stem from organizational problems and miss-management. In particular, this paper focuses on the dangers of complacency when previous successes are wrongly interpreted as guarantees of future safety. The argument is illustrated by the recent loss of NASA's Nuclear Compton Telescope Balloon; during a launch phase that 'no-one considered to be a potential hazard'. The closing sections argue that all senior executives should read at least one mishap report every year in order to better understand the hazards of complacency.

1. INTRODUCTION

Nothing breeds complacency like success. The longer we operate without suffering an incident or accident, the more likely we are to reduce the safeguards that previously assured success. There are further pressures in space engineering–public and politicians often fail to understand the technical and engineering risks associated with many missions. They assume that past achievements guarantee future success. In contrast, a wide range of hazards continue to threaten missions that have previously avoided major failures. It is, therefore, critical that we combat the insidious effects of complacency during many space missions. This paper argues that management teams should be encouraged to read mishap reports so that they are continually reminded of the risks that continue to threaten successful operations.

2. NASA'S COMPTON TELESCOPE BALLOON

On 29th April 2010, a 'High Visibility' Mishap occurred during the launch of the Nuclear Compton Telescope (NCT) at Alice Springs International Airport in Australia (NASA, 2010). Personnel from a contractor were attempting to launch a balloon-borne gamma-ray telescope, which was designed to study astrophysical sources of nuclear line emission with high spectral and spatial resolution. Weather conditions seemed favorable and ten pilot balloons were successfully launched. The crew, therefore, assembled the payload and began to inflate the balloon with helium. The Site Director (SD) received the necessary clearances from Melbourne Air Traffic Control and gave the Launch Director (LD) permission to release the balloon.

The scientific instruments were protected prior to launch by suspending them from a crane. The aim was then to release the payload as soon as the balloon had sufficient lift to complete the launch. In order to do this, the balloon had to be directly over the crane and package at the moment of release. Otherwise, there is a risk of dangerous oscillations damaging the equipment. The crane can be driven under the balloon to achieve a better relative position for the release.

On the day of the incident, the balloon began to move further ahead of the crane on the launch vehicle. The LD told the driver to turn left in order to gain ground. He then pulled the lanyard but could not release the payload from the crane. They accelerated again to catch up with the balloon before making a second attempt. However, they reached the airport perimeter fence and were forced to terminate the launch. The LD was now concerned that spectators might be injured so began further attempts to move the launch vehicle, the payload and the tethered balloon to a safe position. During this process, the payload broke free from the launch vehicle and the balloon dragged it with the wind. The balloon and payload broke through the airport fence and hit a vehicle. The driver was taking photographs of the launch and managed to jump from the roof immediately before impact. A command was then issued to abort the mission by separating the payload. As a result, the balloon came to rest one quarter of a mile downwind from the site. The physical damage was compounded by media coverage. Television broadcasts showed the mishap around the globe and video footage was uploaded to the Internet within hours of the incident.

3. HUMAN FACTORS IN SPACE MISHAPS

This incident has been chosen to illustrate the arguments in this paper because it is typical of many mishaps in

which no injuries occur but that nevertheless provide significant insights into the future safety of space systems.

The loss of the NCT illustrates some of the human factors problems that cause or complicate many mishaps. A key concern for the subsequent enquiry was to determine how spectators came to be downwind of the balloon during the launch. After the decision was taken to terminate the initial release, the Launch Director (LD) could see that spectators were at risk because groups were in the likely path indicated by a tethered pilot balloon. He used his hand-held radio to try and have them moved. The request was relayed to the Site Director (SD) who then asked his deputy to relocate the crowds. The deputy told the occupants of two vehicles to move. An off-duty contractor also heard the command over his radio; he was watching the launch with the spectators. He volunteered to move some of the public to what he considered to be a safer position. However, some of the people that he approached told him that they had just been moved **to** the area that they were now being asked to leave. The investigation board concluded that "specific direction regarding safe locations was not provided to the individuals who relocated spectators, and the resulting actions actually relocated spectators into the eventual path of the balloon and launch vehicle" (NASA, 2010). Similar communications problems have been identified across a range of space missions (Orasanu et al, 2004, Johnson et al, 2010). The introduction of Crew Resource Management techniques from aviation into the space domain has provided ways to improve team integration and training. However, these methods have not been widely applied and communications problems remain a significant factor in many incidents and accidents.

The NCT launch incident illustrates the importance of mishap reports as a tool for reinforcing basic concepts in safety engineering. In particular, the accidental release of the balloon illustrates the complexity of human decision-making in crisis situations. Key personnel must be provided with appropriate Standard Operating Procedures (SOPs) to guide time-critical intervention when things begin to go wrong. The NCT incident also illustrates the importance of drills and exercises to prepare for the application and refinement of these SOPs. For instance, the contractor had successfully completed previous launches even after initial attempts had failed. This created a form of complacency in which there was no expectation that the operation might not succeed at all. Partly in consequence, there were no published guidelines on when repeated attempts to launch the balloon might create unacceptable risks either for mission success or for the safety of the public. The decision to abort the launch was left entirely to the judgment of the Launch Director (LD). In consequence, the LD felt he could still chase the balloon down when the first attempt failed to release the payload. This decision was "entirely reliant on human observation and decision-making" (NASA, 2010). This might be justified if adequate training was provided. However, the launch teams were not required to rehearse a range of contingency operations or anomalous situations. No specific training was provided to deal with anomalies or failed launch attempts. This can again be traced back to the perceived success of previous operations; why would such training be necessary given that few problems had arisen in previous operations?

The subsequent enquiry argued that the incident illustrated a flawed approach to human factors concerns during balloon launches. Rather than developing, documenting and training for agreed operating procedures, the contractor relied on the teams' experience of successful operations; "which left much susceptible to human error or lack of understanding of what to do in contingency or anomalous situations" (NASA, 2010). These concerns were exacerbated by the manner in which higher levels in the programme within NASA had delegated responsibility for critical aspects of launch operations. There was no higher-level guidance on the identification and marking of potential hazard areas during a launch. This was left to the contractor who was assumed to have gained sufficient expertise during previous launches. Unsafe areas were often identified in an informal way using prominent land marks. It was difficult to identify changes in a hazard area as the balloon and launch vehicle moved around the site as the wind changed direction. This led to confusion about the 'safe areas' when the LD and SD tried to move spectators during the NCT launch. The contractor's staff relied on distributed, real-time decision making to maintain public safety. This created significant concerns because there was no centralized responsibility for monitoring the changing threats during a launch. Human factors studies have identified a host of concerns that arise from the coordination and complexity of distributed decision making in safety-critical operations (Bearman et al, 2010, Salmon et al, 2009).

4. THE OPIUM OF SUCCESS

The subsequent mishap board looked beyond the traditional focus of many previous human factors studies. They found that the incident was caused by flawed underlying assumptions. In particular, they identified "a problematic historical mindset and an ineffective organizational structure" that failed to aggressively look for potential risks (NASA, 2010). The program had focused narrowly on the hazards from the over flight of populated areas. This 'complacency'

stemmed, in part, from many years of successful balloon launches. It was argued that these successes had been used to justify reductions in the technical safeguards that might otherwise have protected the launch team and the members of the public around Alice Springs. The myopia was traced back to organizational problems in the program, including the lack of independent safety assurance. Similar comments have been made by previous mishap boards on both sides of the Atlantic (Johnson, 2003). The lack of independent oversight for safety concerns remains the most significant weakness in the organization of space safety.

The complacency identified in previous paragraphs, stemmed in part from the longevity of balloon launches at the incident site. Familiarity can erode caution. NASA had completed more than 50 successful releases from Alice Springs, since 1981. Other organisations had been launching from the area many years before this.

The NCT launch was only one of three missions that had been planned between March and May of 2010. A few weeks before the incident, the Tracking and Imaging Gamma Ray Experiment (TIGRE) had been successfully launched. It had continued operating for more than two days before being 'terminated' and recovered as planned. The subsequent inquiry into the loss of the NCT argued that 'reliance on past success has become a substitute for good engineering and safety practices. Interviews have indicated a consistent theme that the balloon program success rate has been sufficiently high, so therefore there have not been problems to correct or additional scrutiny required' (NASA, 2010). Complacency poses the greatest risks for projects that have a relatively strong safety record.

5. LACK OF FORETHOUGHT

A number of factors combined to create unusual and unanticipated circumstances during the NCT launch. The public had rarely, if ever, been downwind during previous operations. In consequence, the team had little experience of how best to deal with the hazards when initial attempts failed to release the balloon. One reason for this was that the area downwind of the first launch site was not open to the public. However, as the crane manoeuvred it "just so happened that the layout of the balloon on this day was such that publicly accessible points were in the proximity downwind" (NASA, 2010).

A common theme amongst many mishap reports is the 'lack of imagination' shown by engineers when considering the potential adverse consequences of their actions (Johnson, 2003). This is a particular problem when finite design resources are focused on a small number of hazards. During balloon launches attention is often focused on mitigating the risks to other forms of aviation. Hence, the majority of the safety documentation prior to the mishap at Alice Springs addressed the potential hazards to aviators. This arguably detracted from other less obvious hazards, especially to ground personnel during launch operations.

In many cases, risk assessments have been undermined by superficial or cursory hazard analysis. This leads to double jeopardy – not only is it more likely that an incident will occur because safeguards are not implemented – but it is also more likely that the emergency response will be inadequate once an incident does occur. For instance, the Campaign Manager on site during the NCT launch realised that a spectator's vehicle had been hit by the payload and that people may have been injured. He, therefore, took prompt action to summon emergency personnel. However, he was unaware that the 911 number used in the United States would not work. Australian emergency services use the alternate 000 number. He was, therefore, unable to place the call. It was fortunate that airport emergency personnel were able to respond after the Tower notified them of the impact.

The complacency that undermines emergency planning can also compromise wider opportunities to learn from incidents and accidents. After the investigators arrived in Alice Springs, they learned that parts of the payload had already been taken to the local scrap yard. Senior management at the site had not been sufficiently well briefed about mishap investigation requirements to protect all of the necessary evidence – although steps had been taken to safeguard the launch vehicle; "because of the actions of the personnel in the recovery and removal of the wreckage from the mishap site to a holding location within the area, the physical evidence had to be declared as contaminated by the field investigator" (NASA, 2010).

6. ORGANISATIONAL COMPLACENCY

It is important to reiterate that complacency need not stem from deliberate negligence, rather it is the result of multiple, conflicting objectives. Safety is only one of many requirements that must be met by the engineering of complex, space missions. Over time, previous successes can undermine the priority placed upon particular defences including hazard analysis and risk assessment. This complacency is far more likely to occur when the responsibility for safety is lost across complex organisational structures. In the case of the NCT mishap, the Balloon Program Office (BPO) was part of the Wallops Flight Facility (WFF) within the Goddard Space Flight Centre. The BPO managed all balloon activities and reported to the Astrophysics Division within NASA's Science Mission Directorate at

NASA Headquarters. However, the launch was conducted by the New Mexico State University, Physical Sciences Laboratory's Columbia Scientific Balloon Facility (CSBF) under contract to the BPO. However, the CSBF Launch Director (LD) and Campaign Manager (CM) operated in cooperation with a Site Director (SD) working within the University of New South Wales Alice Springs Balloon Launch Facility.

The subsequent mishap investigation identified significant concerns about the ways in which safety was managed across the various interfaces between these organisations. As we have seen, the launch director ordered his driver to make a left turn of more than 90 degrees in order to catch up with the balloon. This hard turn significantly increased the stress on the release mechanisms. This provides a further example of 'unthinking complacency'. The contractor had no guidance on the operating parameters for the launch hardware. They had no instructions about types or durations of manoeuvres that could be safely performed under particular meteorological or terrain conditions.

The mishap investigation board argued that the BPO should have provided greater guidance and technical oversight for the balloon launch process. The significance of this observation should not be underestimated. The implementation of the launch was left to the discretion of the contractor under a performance-based contract. Similar financial arrangements are helping to integrate commercial space operations into a range of NASA missions. The lack of safety oversight that led to this incident provides an important warning for the future (Johnson and Robins, 2011).

The Mishap Investigation Board also identified limitations in the management of safety between other areas of the Wallops Flight Facility (WFF), the Balloon Programme Office and its contractors. The WFF Safety Office was responsible under the NASA Range Safety Manual 2002 Rev B[1] for developing a balloon safety plan that considered ground hazards at the launch site. However, it was argued that the Safety Office had not developed a rigorous hazard analysis. Instead, the existing documentation focussed on a small range of concerns mainly related to pyrotechnic hazards and payload risks. There was little consideration of the problems that might arise during launches in areas where there was sandy or broken terrain. These conditions hindered the NCT launch at Alice Springs when the vehicle lost traction at crucial times during the attempt to catch up with the balloon. Similarly, the existing safety documentation did not adequately consider the risks created by perimeter fencing especially when some launch trajectories placed strict limits on the area available to complete any manoeuvres.

Further concerns focused on the underlying management relationships between the parties involved in the incident. The WFF had not ensured that senior personnel in the Balloon Programme Office were in close contact with their counterparts in the contractors management team. In consequence, the BPO did not ensure that the contractor was following existing procedures and policies. The programme office had a good overview of the ground safety plan and the existing risk assessments; however, they did not monitor what was actually happening on the site. These problems were compounded by a lack of safety leadership at higher levels because these launches were *'out of sight, out of mind'*. The safety leadership did not ensure the flow down of NASA requirements to protect the public. The board found that the WFF Safety Office and senior management were unaware that public safety was at risk during a balloon launch. Again this illustrates wider concerns when projects are increasingly managed by individuals without the technical background to interpret safety concerns across complex space missions.

The lack of organisational oversight is partly explained by funding concerns. Previous successes can persuade management to reduce funding that otherwise have been used to address safety concerns. There was a perception prior to the mishap that too many additional cost burdens would have 'killed' the balloon programme. One consequence was that higher levels of safety management lacked the resources and the motivation to thoroughly consider launch risks given that there had not been any major incidents immediately prior to this mishap.

7. OVER-RELIANCE ON PROCESSES

Complacency can also be institutionalised when common operations are enshrined in procedures that seem to guarantee success. In other words, engineers will often assume that no hazards can arise so long as they follow the same steps they used in successful operations. In this case, the contractor's team followed NASA's standard 'dynamic launch' process for large stratospheric balloons, described in Section 2 of this paper. As we have seen, the standard approach focused on the platform architecture and launch procedures rather than on common techniques for hazard mitigation. In consequence, the 'standard' approach provided little protection for spectators and staff when problems began to occur during the launch.

[1] http://sites.wff.nasa.gov/code803/docs/RSM2002%20revB.pdf

It is also clear that important elements of the 'standard' dynamic launch technique were undocumented. The contractor had not provided its personnel with detailed guidance about the use of this technique; "after reviewing all of the procedural documentation, no prescribed process was found for launching the balloon and there was minimal information provided in the documentation for on-the-job training". These omissions extended to the provision of guidance for contingency planning. In consequence, although the dynamic launch process had provided considerable success in the past it was extremely fragile. As we have seen, it was vulnerable to human error and communications problems across the launch team as they struggled to retrieve the balloon and at the same time maintain public safety.

8. RELIANCE ON DOCUMENTATION

Complacency is sustained by the mistaken belief that documentation guarantees the safety of complex systems. In many cases, it is clear that documentation significantly undermines safety by wasting finite resources on 'tick box' exercises that have little relationship to operational practices. For instance, the safety plans developed by the contractor and the programme office did not consider the hazards to spectators during a launch. This in turn reflected a failure to meet the requirements of RSM 2002, cited in previous sections as well as NASA guidance documents NPR 8715.3 and NPR 8715.5. The investigation also argued that the contractor had failed to meet the requirements in their contract NAS5-03003. In particular, clause 4.1.2 stated that written procedures are required for any hazardous procedure and given that the launch process involves many hazards, it requires written procedures. It was argued that the Balloon Program Office should have ensured that the contractor complied with section 4.1.2 by confirming that procedures were written to cover the launch process. There were further limitations with the WFF ground safety plan. For instance, the kinetic potential and mechanical energy in the hanging payload was not recognised as a potential hazard. Similarly, the risk assessment did not account for the potential harm that could be caused by the balloon or parachute after an aborted launch.

Many mishap boards have argued that accidents would have been avoided if only personnel had followed procedures and guidance. **In contrast, more may be gained by asking why procedures and guidance are so hard to follow.** Contractors and employees face enormous problems in applying the mass of guidance that has been developed for space missions (Johnson, 2003). The NCT mishap board found that many of these guidance documents were poorly written, including the balloon ground safety plan. One reason for this is that senior safety management did not review the documentation; "there is much ambiguous language in the documentation, hazards are not covered completely, there is no provision to protect the public except in the over flight phase, and it does not completely cover all phases of balloon operations".

Complacency is hard to sustain when others within an organisation have recognised the potential risks in a space-related mission. In particular, NASA Agency Range Safety Program had conducted an audit of balloon launches in 2002. However, several of the actions that had been identified from this review were still open, without corrective actions. In particular, one item found that the "Balloon Program payloads are potentially hazardous to the public and should be managed consistent with other hazardous, uninhabited programs". The board criticised the lack of follow-up for these concerns that should have been elevated to the highest level of NASA to ensure the safety of the public at launch sites.

9. ALTERNATIVES TO PARANOIA?

Previous sections have argued that the NCT mishap was compounded by inadequate hazard analysis. This, in turn, stemmed from organizational causes that can be traced back to a culture of complacency reinforced by a feeling that previous successes guaranteed future safety. However, such insights are of little value unless they provide longer term operational benefits. Even if the existing hazard analyses had been extended to consider the risks to spectators, there is no guarantee that they would have prevented the mishap from occurring. In particular, there were several unusual aspects of the NCT failure. For instance, the launches took place under a permit that was issued by the Australian Civil Aviation Safety Authority (CASA). The permit approved heavy balloon operations around Alice Springs airport without explicitly mentioning the extent of the area. The fenced perimeter provided one demarcation; hence the spectators were permitted to view the launch from outside that area. They could easily access the launch site using public roads. However, the fences were not designed to provide protection from the hazards associated with NCT operations. The CASA permit was also ambiguous because both the fenced area and the zone where the spectators had gathered were both airport property; "While at first glance it appears that this permit is intended to establish a safe area to protect the public, the ambiguity of the boundaries of the area and the lack of specific reference to people in the area during the launch indicate that it does not address public safety". It is hard to imagine that the hazards created by such ambiguity might have been anticipated by a more sustained risk assessment prior to the mishap.

A number of other 'one off' factors illustrate the problems in anticipating many mishaps. There was no independent range safety officer at the launch site. The Campaign Manager (CM) fulfilled some of these responsibilities. However, his main concern was to ensure mission success. He also had responsibility for coordinating elements of the release, by deciding when to drop the restraining collars on the balloon. These other preoccupations prevented him from focusing on safety. The Launch Director had a similar division of responsibilities. He could halt the operation if he felt the situation was unsafe – earlier attempts to launch the NCT had been postponed because of adverse weather. However, he was also responsible for meeting the overall mission objectives; "he lacked independence as well and his primary responsibility was to direct the launch vehicle to track the balloon and launch at the appropriate time".

Similar one-off circumstances can be found in most major mishaps. They can be difficult or impossible to anticipate and often have a significant impact on the course of an incident or accident. However, they cannot easily be described as the 'root cause'. In the NCT failure, higher levels of management might have taken a more active involvement in the oversight and direction of balloon operations prior to the incident. In order to encourage this active approach to safety management, we argue that all senior executives should read at least one mishap report every year in order to better understand the hazards of complacency in complex, space missions.

10. CONCLUSIONS

This paper has argued that human factors techniques have made significant contributions to the safety of space missions. Physiological models help to monitor crew workload and performance. Empirical studies inform the design of operator interfaces to maximize finite cognitive and perceptual resources. Further progress has been made in supporting distributed situation awareness across multi-national teams and in promoting the resilience of complex, time critical missions. Most of this work has focused on operational performance. However, most space-related mishaps stem from miss-management. In particular, previous sections have argued that complacency has undermined operational effectiveness when previous successes are wrongly interpreted as guarantees of future safety.

The closing sections of this paper have recommended that all senior executives should read at least one mishap report every year in order to better understand the hazards of complex, space missions. This cannot guarantee future incidents will not occur. However, the intention is to provide an annual reminder of the complex ways in which human error, systems failure and managerial decision making combine to undermine defenses that protected previously successful missions. Mishap reports also remind safety management of the need to prepare for emergency response in the aftermath of an adverse event. Paradoxically, successful teams are often the least prepared for incidents and accidents. These arguments have been illustrated by the recent loss of NASA's Nuclear Compton Telescope Balloon; during a launch phase that 'no-one considered to be a potential hazard'.

References

C. Bearman, S.B.F. Paletz, J. Orasanu and M.J.W. Thomas, The Breakdown of Coordinated Decision Making in Distributed Systems, Human Factors: The Journal of the Human Factors and Ergonomics Society April 2010 vol. 52 no. 2 173-188

C.W. Johnson, A Handbook of Accident and Incident Reporting, Glasgow University Press, Scotland, UK, 2003.

C.W. Johnson, A. Herd and M. Wolff, The Application of Resilience Engineering to Human Space Flight. In H. Lacoste-Francis (ed.), Proceedings of the Fourth International Association for the Advancement of Space Safety, Huntsville Alabama, ESA Communications, ESTEC, Noordwijk, The Netherlands, ISBN 978-92-9221-244-5, ESA SP-680, 2010.

C.W. Johnson and D. Robins, Myths and Barriers to the Introduction of Safety Cases in Space-Based Systems. In C.G. Muniak (ed.), Proceedings of the 29th International Systems Safety Society, Las Vegas, USA 2011, International Systems Safety Society, Unionville, VA, USA, 2011.

National Aeronautics and Space Administration (NASA), Mishap Report into the Nuclear Compton Telescope Balloon Launch in Alice Springs, Northern Territory, Australia, High Visibility Type B Mishap, Incident Reporting Information System (IRIS) Case Number S–2010–119–00007, Volumes I+II, Date of Mishap: April 29, 2010, Date of Report: September 7, 2010.

J. Orasanu, U. Fischer, Y. Tada, and N. Kraft, Team Stress and Performance: Implications for Long-Duration Space Missions, Human Factors and Ergonomics Society Annual Meeting Proceedings, Cognitive Engineering and Decision Making, pp. 552-556(5), 2004.

P.M. Salmon, N.A. Stanton, G.H. Walker and D.P. Jenkins, Distributed Situation Awareness: Theory,

Measurement and Application to Teamwork, Ashgate, Kent, UK, 2009.