Taking a Closer Look at Flight Crew Handling of Complex Failures
Ten Case Studies

Reitsma, Jelmer; Fucke, L.; Borst, Clark; van Paassen, Rene

Publication date
2017

Document Version
Accepted author manuscript

Published in
19th International Symposium on Aviation Psychology (ISAP 2017)

Citation (APA)
Reitsma, J., Fucke, L., Borst, C., & van Paassen, R. (2017). Taking a Closer Look at Flight Crew Handling of Complex Failures: Ten Case Studies. In P. S. Tsang, & M. A. Vidulich (Eds.), *19th International Symposium on Aviation Psychology (ISAP 2017): Dayton, Ohio, USA, 8-11 May 2017* (pp. 560–565)

TAKING A CLOSER LOOK AT FLIGHT CREW HANDLING OF COMPLEX FAILURES – TEN CASE STUDIES

J.P.Reitsma[*], L. Fucke[†], C.Borst[*], M.M.van Paassen[*]
[*] *Delft University of Technology, 2629 HS Delft, the Netherlands*
[†] *Boeing Research and Technology Europe, Madrid, Spain*

Non-normal events, in particular system failures with serious operational impact are rare in flight operations. These events are not always easy to handle by flight crews. The aim of the performed study is to determine where in this process potential issues may lie. Ten incident reports are studied using a newly developed operational issue analysis framework. The framework is used to determine whether and how the current interfaces communicate the initial *functional* impact and functional impact delayed in time. Additionally, results from pilot interviews are presented which identified three phases of non-normal event handling: fault detection, fault management and strategic planning. Analysis of the ten cases shows that current alert systems are mainly supporting the first two phases while the strategic planning phase, requiring higher level functional information integrated into the operational context as well as failure impact later in time, is relying almost entirely on pilot knowledge and reasoning.

Flight deck alerting systems have changed considerably in the past decades. The dials and warning lights used in the first generation airplanes were replaced by a centralized alphanumerical alert readout device, which presents descriptive text messages that are categorized by system and criticality (Veitengruber, 1978). More information and automation is provided than ever before. Although computerization changed the way alerts are presented, the fundamental concept of alerting has not changed and alert messages still largely refer to states of physical components or functions that were previously performed by a physical component. Several recent studies indicate that non-normal events are not always handled as desired, and procedures do not always provide sufficient guidance (Burian, et al., 2005). Difficulties can arise especially during failures involving interconnecting and automated systems (Singer & Dekker, 2000). The unchanged alerting approach, the shift of the pilot's role to an exception handler and manager of automated resources (Sarter, 1997) and the increased complexity of airplanes (Hasson & Crotty, 1997), may introduce various human performance issues. Current alerting systems present malfunctions to the flight crew as a list of messages that present physical information describing the status of individual systems, often physical components such as pumps, computers or valves. Lintern, Waite and Taller (1999) argue that the human-performance issues are not caused by the amount of presented information nor the complexity of the systems, but are mainly caused by the type of information that is presented. Multiple researchers confirm that flight decks lack functional information (Dinadis & Vicente, 1999) and that this lack of functional information can make handling non-normal events more taxing.

This paper will report on the results of an exploratory study with the goal to identify potential human-performance issues related to the current alerting systems and investigate where improvements could be possible. For this study 10 non-normal events were analyzed on how the current alerting systems present functional impact of a failure and what human performance issues might hinder understanding of the impact of the failure on the airplane.

Method

The Operational Issue Analysis (OIA) framework was developed to analyze incidents and accidents regarding potential human performance issues. The basic principle of the framework will be explained at the hand of Table 1.

Table 1

Operational issues analysis (OIA) framework.

			Human Performance Hinders					
			Detection			Understanding		…
Function	**Impact**	**Representation**	#1	#2	#3	#4	#5	
Generate Electricity	Lost	´Standby Bus Off’		x		x		
Distribute Fuel	Degraded	Fuel weight values	x	x	x			
…	…	…						

First, the initial functional impact of a system failure is determined from the incident reports and captured in the first two columns as presented in Table 1. The functions are obtained from a high-level functional decomposition, which enables the comparison across different alerting systems and airplane system architectures. A functional impact can be classified as either a loss, a degradation, a redundancy reduction or no impact. The function-specific flight deck effects that may indicate an impact are gathered and they are presented next to the functional impact. It can happen that a functional impact is not represented by any flight deck effect. The number of impacts without an indication is counted. The presented indications are then analyzed regarding the presence of any potential human performance hinders. The human performance hinders were obtained from the published Boeing in-house Cockpit-operations Reliability Evaluation Worksheet (CREW) (Fucke, et al., 2011). This worksheet is built around the Rasmussen’s decision step ladder model. The CREW worksheet lists helps and hinders for all of the decision making steps. The OIA framework uses only hinders related to the first three steps, i.e. detection, understanding and prioritization, a total of 25 hinders. The latter decision making steps require more detailed procedural information, which is outside the focus of this study.

Next, the framework is used to determine how a functional impact delayed in time is communicated. This is done by evaluating each cascading failure step in the same fashion as before. This provides an indication whether the crew is able to detect repercussions at an early stage based on the presented flight deck effects.

The ten cases studied were selected from the Aviation Safety Reporting System (ASRS) and incident reports based on the following criteria: a system failure occurred in-flight on moderate to highly integrated airplanes and the malfunctions caused a severe operational impact delayed in time. The failures originate from a variety of systems.

Additionally, five experienced flight training instructors were interviewed to understand how non-normal events should be handled, what to consider during the event and what challenges are most typically encountered in operations and flight crew training. The results from the pilot interviews were used to assess validity of the findings of the operational issue analysis.

Results

The cases used for the OIA are categorized based on the initially affected function when the failure occurred: multiple failure scenarios, i.e. multiple functions are affected at the same moment, cases in which the "distribute fuel" function was initially affected, cases in which the "electric power generation" function was affected and cases in which the "hydraulic power generation" function was affected. The selected cases occurred on a variety of airplane models with varying system architectures. First is determined how many of the functional impacts are represented by any flight deck effect (FDE), which will be presented as a percentage of the total affected functions in Table 2. If there is an indication, the indication is evaluated on the number of hinders present. Finally, the cascading steps are analyzed and the percentage of impacts delayed in time that are communicated by a flight deck effect is calculated. The results are presented per category in Table 2, from which the following main observations can be extracted.

Table 2.
Hinders identified in showing the initial functional impact and impact delayed in time.

Case	Cases	Initial impacts with FDE per initially affected function [%]	Average # of hinders per initially affected function	Impacts delayed in time with FDE [%]
Multiple functions	2	51%	5	51%
Electric power generation	2	100%	1	-
Hydraulic power generation	2	100%	0	82%
Fuel distribution				
- (with alert)	1	100%	1	2%

- (without alert)	3	100%	8	2%

Not all initial functional impacts are presented by the interfaces. This was observed in particular for the multiple failure scenarios in which some impacts were not presented even though they were severe. The fact that the flight crew was surprised when detecting an uncontrollable engine (ATSB, 2013) (NTSB, 2010) and when there was no response after commanding reverse thrust, indicates that the impact of the failure was presented incompletely (NTSB, 2010). Furthermore, in one case the crew was not able to detect a loss of the fire extinguishing system (ATSB, 2013). The only way these effects could have been detected is by using detailed system knowledge.

Fuel leaks are hard to detect on planes that do not have an appropriate fuel alert**.** The crew can detect the initial impact on the fuel function, if no message is presented, only by comparing fuel on board figures with the flight plan, which requires mental effort, takes up additional time, is performed in large time intervals and is perceived as a lower priority in case other alerts are present, e.g., when symptoms appear in a different system. For example oil-related messages drew the attention of the crew away from routine tasks (GPIAA, 2004). The high number of average identified hinders in these cases confirm this. The planes that have a message in place such as 'FUEL DISAGREE' (ASRS #1184574), handled a fuel leak without difficulty. Hence, these cases are presented separately in Table 2.

The level of degradation can be difficult to determine. In the several cases, failure messages that include for example, 'monitoring fault', 'L/G CTL 1 FAULT' do not provide clarity if the system is still functioning. This might be because the messages present only physical states, e.g. 'HYD B+Y SYS LO PR','BRAKE TEMP'. The transformation to a higher level function needs to be done by the crew in order to determine if the system is still functioning.

Mode indications rely heavily on the pilots' system knowledge. The crew has to understand what functions are still supported in a specific mode. As an example the messages 'ALT LAW (PROT LOST)' and 'EMER ELEC CONFIG' shall be provided. In these cases, the crew may be required to remember what is covered by these modes and what is not, which increases mental effort. Difficulties exist in determining what is affected after an electric bus failure, since a lot of systems are dependent on these buses and often no clear overview is available to the crew.

The amount of presented messages during multiple failure scenarios can be overwhelming. In one case it took 50 minutes to obtain a clear overview on what systems were inoperative (ATSB, 2013). Hence it can be concluded that it can be difficult to obtain a clear overview of all the affected functionalities during failure scenarios that affect multiple sub-systems.

As Table 2 shows, determining the degradations delayed in time are almost entirely based on flight crew reasoning and procedural information. No indications are present that project future failure effects. These indications may be valuable for resource systems such as equipment cooling and depleting batteries, since they have a severe impact on connected systems.

Identifying the consequences of a system failure turns out to be challenging and often relies on flight crew reasoning. Examples of these are; difficulty in determining how the landing distance of the plane was affected while considering degraded braking capability and the higher approach speed (ATSB, 2013) (NTSB, 2010). Reduced range due to an extended landing gear (SUB, 2001). Additional fuel burn due to APU operation and a therefore limited range (ASRS #925795, ASRS #854044). And finally, the crosswind limitation due to hydraulic failure (ATSB 2001). This indicates that deriving functional, context specific information about the airplanes capabilities from alert messages can be difficult. The process of determining which parts of the mission can be performed without change and which not is one of the most challenging tasks the crews face. This was confirmed in the pilot interviews we performed.

Discussion

Some identified human performance issues could potentially be addressed by introducing new messages as was seen by the fuel cases. On the other hand, an increasing number of messages may also hinder detection and understanding.

The interviews and investigation reports show that handling of a non-normal event can be split up in three phases; ‘manage the moment’, ‘fault management’ and ‘strategic planning’ phase. The last phase is relatively unsupported by the current interface, this can be concluded from the observation that the impact delayed in time is not presented. This finding was confirmed in the interviews. Basic impacts on the mission can be difficult to extract from the alert messages, e.g. range or landing distance. This process is mainly based on the system knowledge and experience of the flight crew. While the majority of the tasks on the flight deck fall into the rule-based realm this process remains highly knowledge-based. The integration of the system effects into the operating context is complex. This can lead to interpretation errors, which can in turn lead to undesired consequences.

Making a diversion decision for example depends largely on aeronautical decision-making and can be very complex due to the many factors involved. Even clear procedural guidance stating that a diversion is needed, e.g. ’Land at nearest suitable airport’ can be challenging to follow, as a lot of factors have to be considered to determine whether an airport in fact is suitable and what configuration is needed or available for landing. What the effects are of a changed configuration has to be determined by the crew, requiring additional interaction with on-board systems, performance tables and additional reasoning. In addition go-around performance may have to be considered, which leads again to an increase in workload.

As we determined in our pilot interviews, operational issues can often be detected using a step-by-step story-telling approach, in which each flight phase is briefed based on what the effects are and how to handle the plane differently from normal operating procedures. Obtaining information about failure effects, weather, performance data, level of available automation, airport navigational aids or other services, is often tedious and can take a lot of time.

While it is understandable that providing improved support of the strategic planning phase can be challenging due to the ever changing environment in which an aircraft operates, it may be worthwhile looking into better integration of a failure effect with the environment by making full use of the current computing capabilities and ways of information exchange. This may simplify information integration and decision-making, lead to a reduction in workload and the ability to evaluate more options. Further, this could reduce the potential of undesired consequences by moving some tasks from the knowledge-based to the rule-based realm. Also, by providing a better overview of failure consequences, unnecessary diversions might be reduced. These have a significant economic impact in flight operations.

Further, with advancing automation it is likely that the fault management phase may become less important altogether as automation will take over more and more of the associated reconfiguration tasks. A more integrated support of the strategic management tasks therefore appears to merit a priority.

Concluding Words

To date, transforming physical state information into functional availability as well as integration with the operational environment requires a high level of reasoning and system knowledge from the flight crews and hence considerable training. The current alerting and checklist systems may not always represent the operational effects of a system failure in a way that lends itself to ad-hoc understanding. This can lead to undesired consequences. Improvements can potentially be made by providing increased interface support for information gathering and integration process. Automated processing of state information and relating it to the operational context can likely reduce the complexity of handling non-normal events.

References

ATSB (2001). Airbus A340-300, B-2380 Sydney, NSW 1 November 2000. *Investigation report 200005030.* Canberra, Australia: Australian Transport Safety Bureau (ATSB).

ATSB (2013). In-flight uncontained engine failure Airbus A380-842, VH-OQA. *Investigation report AO-2010-089.* Canberra, Australia: Australian Transport Safety Bureau (ATSB).

Burian, B.K., Barshi, I., & Dismukes, K. (2005). The challenge of aviation emergency and abnormal situations. *NASA Technical Memorandum, 213462*. Moffett Field, CA: NASA Ames Research Center.

Dinadis, N., & Vicente, K. J. (1999). Designing functional visualizations for aircraft systems status displays. *The International Journal of Aviation Psychology,* 9(3): 241–269.

Fucke, L., Mumaw, R. J., Kennedy, R. J., & Nicholson, R. K. (2011). Assessment of risk from human performance on the flight deck - Driving sound design decisions. *6th IET International Conference on System Safety*, (pp. 1–5). doi: 10.1049/cp.2011.0247

GPIAA (2001). All Engines-out landing due to fuel exhaustion, Air Transat, Airbus A330-243 marks C-GITS, Lajes, Azores, Portugal, 24 August 2001. *Investigation report 22/ACCID/2001.* Lisbon, Portugal: Gabinete de Prevenção e Investigação de Acidentes com Aeronaves (GPIAA).

Hasson, J., & Crotty, D. (1997). Boeing's safety assessment processes for commercial airplane designs. *16th DASC. AIAA/IEEE Digital Avionics Systems Conference*, vol.1(4.4): 1–7. doi: 10.1109/DASC.1997.635076

Lintern, G., Waite, T., & Talleur, D. A. (1999). Functional interface design for the modern aircraft cockpit. *The International Journal of Aviation Psychology*, 9(3): 225–240.

NTSB (2010). B752 Electrical Failure, Chicago IL, 22 Sept 2008. *NTSB Report CHI08IA292.* Washington, DC: National Transportation Safety Board (NTSB).

OTK (2009). Serious incident at Helsinki-Vantaa airport due to tread separation and hydraulic failure, 22 june 2009. *Investigation report C2/2009L.* Helsinki, Finland: Onnettomuustutkintakeskus (OTK).

Sarter, N. B., Woods, D. D., & Billings, C. E. (1997). Automation surprises. *Handbook of human factors and ergonomics*, 2:1926–1943.

Singer, G., & Dekker, S. W. A. (2000). Pilot performance during multiple failures: An empirical study of different warning systems. *Transportation human factors,* 2(1): 63–76.

SUB (2000). Flugunfall mit dem Motorflugzeug Type Airbus A310 am 12. Juli 2000 am Flughafen Wien-Schwechat, Niederösterreich. *Investigation report GZ. 85.007/0001-FUS/2006.* Vienna, Austria: Sicherheitsuntersuchungsstelle des Bundes (SUB).

Veitengruber, J. E. (1978). Design criteria for aircraft warning, caution, and advisory alerting systems. *Journal of Aircraft,* 15(9): 574–581.