Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Environnement,
de l'Energie et de la Mer

BEA
Bureau d'Enquêtes et d'Analyses
pour la sécurité de l'aviation civile

International Society of Air Safety Investigators
Annual Seminar, Reykjavik
October 17-20, 2016

Reverse-Engineering the Causal Links Reveals Safety Analysis Issues

Paper

by **Sébastien David** and **David Romat**

On 24th May 2011, a Dassault Falcon 7X operated by Jet Link AG suffered a pitch trim runaway during the descent phase to Kuala Lumpur Airport (Malaysia). The pitch attitude and load factor reached 42 degrees nose-up and 4.6 g respectively. In reaction to the loss of controllability in pitch, the reflex inputs of the PF, who banked the aircraft up to 98 degrees to the right to lower the aircraft's nose, were consistent with nose-high recovery techniques. This reaction, applied and adapted from an excessive pitch attitude recovery technique attributed to training which the PF received during his military career, was decisive in temporarily recovering control of the aeroplane by changing the nose-up pitching movement into a turn, despite the THS being in full nose-up position. During the maneuver, the crew also had to handle two dual input situations as the PNF made simultaneous inputs on his sidestick. Nevertheless, the crew managed to temporarily stabilize the aircraft's attitude with the horizontal stabilizer in full nose-up position. Parameter analysis and crew accounts tend to show that the dual input visual, tactile, and sidestick priority control alerts enabled the crew to identify the dual input phases and act appropriately. Approximately two minutes after the beginning of the runaway, a monitoring function automatically switched to a redundant control channel, which returned the horizontal stabilizer to normal operation.

To ensure the highest level of safety, Dassault-Aviation and the EASA agreed to ground temporarily the Falcon 7X fleet until the event was investigated. The fleet was composed at the time of the accident of 112 aircraft having accumulated more than 75,000 flight hours.

Moreover, this serious incident occurred two days prior the 37th G8 summit that was held in Deauville (France) during which the same type of aircraft (among others) was expected to be used to facilitate the transport of the leaders and delegates participating to this event.

Aéroport du Bourget
Zone Sud – Bâtiment 153
10 rue de Paris
93352 Le Bourget Cedex
France
Tél. : +33 1 49 92 72 00
Fax : +33 1 49 92 72 03
www.bea.aero

An AD released on 16 June 2011 allowed re-starting flight operations with a limited flight envelope after implementation of Dassault modifications. Flight operations with full flight envelope resumed on 29 August 2011.

On the other hand, since the event occurred in Malaysian airspace, the BEA informed the Malaysian civil aviation authorities who delegated the investigation to the BEA. In accordance with the provisions of ICAO Annex 13, Accredited Representatives and advisers from Switzerland (State of Registry and of Operation of the aeroplane), the United States (State of Manufacture of an equipment involved in the runaway), and Malaysia (State of Occurrence) participated in the investigation. The investigation lasted over four years to determine all lessons learned from the event. The Final Report was published early in 2016 and is available on BEA website[1]. Operational aspects of the event give "positive" lessons[2] but they are not detailed in this paper.

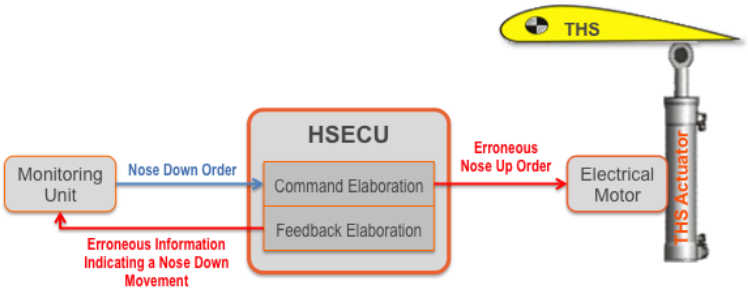
Origin of the failure

The investigation revealed that a soldering defect on one pin of an onboard unit component was the triggering event of the THS runaway. This soldering defect stems from a manufacturing defect that was not detected during the manufacturing process. It was caused by insufficient heat during the soldering process because the plated through-hole had not been properly insulated from the rest of the circuit board. Part of the soldering heat was therefore absorbed, preventing the creation of a proper solder.

The equipment involved was the Horizontal Stabilizer Electronic Control Unit (HSECU), which drives the main electrical motors of the THS actuator. Its design and manufacture were subcontracted by Dassault-Aviation to Rockwell-Collins. The micro-cracks on an induction coil solder caused the HSECU to generate incorrect nose-up commands to the motor controlling the horizontal stabilizer and to transmit nose-down values to monitoring systems indicating a change in the opposite direction to that in which the motor was actually moving.

[1] https://www.bea.aero/uploads/tx_elydbrapports/hb-n110525.en.pdf

[2] Application of excessive pitch attitude recovery technique and management of dual inputs situations.



Consequently, the nose-down orders computed by the flight control computers were consistent with the feedback elaborated by the HSECU. Hence the monitoring function, which by design relied only on HSECU information to detect an HSECU-induced THS runaway, did not trip.

Scope of the investigation

The identification of the faulty electrical connection that led to the in-flight upset was not the end-point of the investigation. As a general point of view, the design of the aircraft must adequately control undesired events to ensure the safety of aircraft and systems. It is accomplished by a series of analyses that has a specific function to identify hazards and then to control the probability of an accident occurring from the hazard or to reduce the severity of an accident. Those analyses can therefore be of considerable interest for safety investigations in identifying latent failures and possible causes of each failure mode. That's the reason why failure to detect design vulnerabilities and associated consequences despite this system safety analysis process was also investigated.

In other words, one aspect of the investigation was to determine why the effects of a soldering defect had not been properly anticipated and addressed during design. The objective was therefore to look for answers to the following questions:

- How were the consequences of this inductive coil soldering defect evaluated in the safety analysis conducted during aircraft design?
- What was the validation process of this assessment?
- Why the decisions taken during the safety assessment process had an impact upon the aeroplane design and therefore upon the serious incident?

The ICAO Manual of Aircraft Accident and Incident Investigation (doc 9756, Part III, Investigation) indicates that investigations *"often identify design or systems issues that are related to accident causation"* and

that *"many safety recommendations do address design improvements"* but that safety analysis process are seldom investigated. This last point was confirmed in the framework of the Dassault Falcon 7X investigation when looking at Final Reports addressing similar issues. Furthermore, without judging beforehand, system safety assessment documents on complex systems like fly-by-wire control system can be considered as protected or "confidential" ones. Therefore, requests from investigation authorities may suffer some reluctance from aircraft design organizations and equipment manufacturers. That was the case with the HSECU manufacturer who took several months to send requested answers and documents.

Safety assessment process

Before describing the analysis of the investigation, some key elements are given dealing with the safety assessment process.

Approved design organizations applying for type certificates must demonstrate compliance with applicable technical conditions and submit to EASA the means by which compliance is demonstrated. As the primary certification authority, EASA (like FAA for US programs) is involved in the early stages of the type certification process, particularly to validate the selected means of compliance and the certification documents presented as proof. The agency is not obligated to verify all documents, carry out any inspections, conduct or be present for any tests to check the validity of compliance. EASA and the design organization define the documents to be reviewed by the authority depending on the project to be certified.

During the certification of the Dassault Falcon 7X, THS runaway was considered as a catastrophic failure condition[3]. It results from the regulatory requirements[4] that aeroplane systems and associated components, considered separately and in relation to other systems, had to be designed so that this failure condition was extremely improbable and did not result from a single failure. Compliance with those requirements had to be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis had to consider:

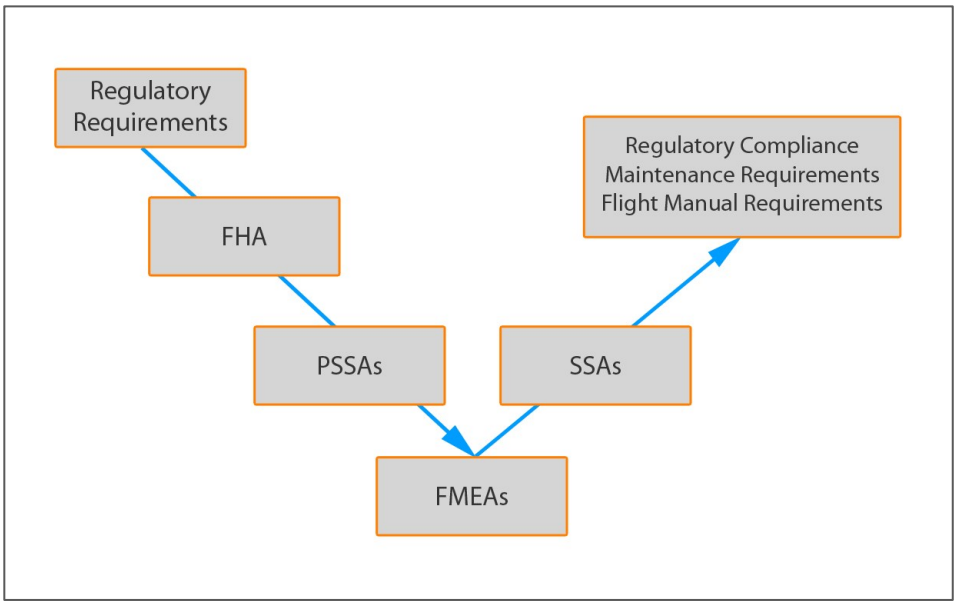
- Possible modes of failure, including malfunctions and damage from external sources;
- The probability of multiple failures and undetected failures;
- The resulting effects on the aeroplane and occupants;
- Crew warning cues, corrective action required and the capability of detecting faults.

[3] Failure condition which would prevent the continued safe flight and landing of the aeroplane.

[4] JAR 25.671 and JAR 25.1309. FAR regulations include the same requirements.

The analysis is the result of a highly complex safety assessment process and comprises many different types of analysis, including:

- FHA (Functional Hazard Assessment): These are preliminary engineering assessments that are frequently updated as the aircraft and system designs evolve. They list the main functions of the primary flight control system and identify failure conditions associated with each of these functions. The severity of each failure condition is also evaluated in FHAs, as well as the corresponding safety objective in terms of probability.
- PSSA (Preliminary System Safety Assessment): For each failure condition identified in the FHAs, the safety objective is cascaded down to the equipment level, on the same principle as fault trees.
- FMEA (Failure Modes and Effect Analysis): At equipment level, a structured and inductive analysis is performed to evaluate for each individual component the effects of its failure modes on the system. The FMEA is used to feed the PSSA to get the final System Safety Analysis (SSA).
- SSA (System Safety Assessment): SSAs take into account the results of FMEAs and other safety assessments and contain the definitive list of system failure conditions and associated probabilities. The purpose of SSAs is therefore to check compliance with safety requirements.



Investigation of the safety assessment process

As indicated above, the potential effects of a hardware component failure should be identified and detailed in the FMEA for the item in question. The HSECU FMEA, performed by Rockwell Collins as Dassault-Aviation subcontractor, identified a defective electrical link (similar to the soldering defect) on the faulty component (an induction

coil) as a potentially latent failure[7]. Its effects were considered as not visible on the HSECU.

The imprecise assessment of the effects of component failures in the FMEA of the HSECU prevented the proper evaluation of these effects in the safety analysis of the whole THS control system.

The System Safety Assessment (SSA) of the primary flight control system conducted by Dassault-Aviation took into account the results of the HSECU FMEA performed by Rockwell-Collins after verifying certain failure modes. Beyond the effects of the induction coil failure, considered as “potentially” latent, the number of similar results in this FMEA led to a failure to mention the HSECU in any of the failure conditions identified in the SSA for the Falcon 7X flight control system.
Those SSA results were not challenged by Dassault-Aviation despite the highest verification and validation level that were in place throughout the design of this critical system. The approval of the primary flight control SSA by the certification authority did not allow catching this error either.

The SSA results for the primary flight control system consequently affected the development of the monitoring functions associated with the THS control system. In the situation of the event, the monitoring functions of the THS control channel were actually depending on the HSECU itself to detect an HSECU malfunction. This architecture did not ensure that the control unit would detect a malfunction or that reconfiguration to another control channel could take place via an independent method. This type of architecture nevertheless met regulatory requirements (at the time of the design of the aeroplane), which were not explicitly requiring independence between monitoring and control channels. This enabled a single failure to cause THS runaway, considered as catastrophic. It has to be noticed that after the serious incident, Rockwell-Collins updated the HSECU FMEA using the same methodology. This new FMEA gave results totally different from the FMEA that was valid before the event. Dassault-Aviation also modified THS monitoring so that a THS runaway caused by an HSECU failure can be detected independently by monitoring units in all situations.

[7] As well as the majority of failures described in this FMEA.

Conclusion

The investigation therefore revealed that for a complex system like the primary flight control system, the safety assessment process is vulnerable to errors or inaccuracies. They can arise at various stages of the process:

- Imprecise assessment of the effects of the failure types identified in the FMEA, validation of the FMEA and in general, the varying results of FMEAs even when using the same methodology (human and equipment manufacturer organizational factors)
- Lack of mechanisms for detecting potential critical errors in equipment manufacturer FMEAs during the aircraft safety assessment and certification process.
- Design organization's capability of managing and supervising design when equipment (especially critical equipment) is designed by partners or subcontractors;
- Limitations in the SSA verification process by the aircraft manufacturer and in the approval process by EASA;
- Limitations of the safety analysis, like FMEAs, which were developed few decades ago for traditional hardware system and not for advanced avionics and computer-based fly-by-wire systems.

The BEA addressed safety recommendations to EASA and FAA aimed at filling gaps that may occur during aircraft design in the safety analysis process. But drafting safety recommendations for complex topics involving widely used industry standards, advanced avionics and numerous organizations was not easy. That's the reason why those safety recommendations raised the weaknesses identified during this investigation and confirmed by other ones, by asking EASA and FAA, in coordination with SAE and EUROCAE, to propose and develop additional or alternative means. The weaknesses involve:

- The FMEA methodology for electronic equipment and software;
- The insufficient or inadequate means to check the independence of system control and the monitoring of said system.

The time allocated to this investigation made it possible to go beyond what is commonly investigated. Thanks also to the cooperation with the aircraft manufacturer, light was shed on vulnerabilities in the complex process of system safety analysis, which will hopefully help avoid similar issues and improve overall flight safety.

Speakers:

Sébastien David, BEA Safety Investigator
sebastien.david@bea.aero

Sébastien David is a BEA senior safety investigator and coordinator of investigator training and investigation techniques. He graduated in 1997 as an aeronautical engineer from the French National Graduate School of Civil Aviation (ENAC). He joined the BEA Engineering Department in 1998 to work initially on flight recorders readouts and performance studies. During his career with the BEA, he has participated in many major investigations as IIC or accredited representative, as well as head of working groups, for example for the Human Factors group during the investigation of the Air France A330, flight AF447 accident. He has been type-rated on the Dassault Falcon 7X and has a Masters degree in Human Factors.

David Romat, BEA Safety Investigator
david.romat@bea.aero

David Romat is a BEA senior safety investigator. He graduated in 2005 as an aeronautical engineer from the French National Graduate School of Civil Aviation (ENAC). He joined the BEA Engineering Department in 2008 and has been in charge of flight recorders readouts and aircraft systems analysis. David has participated in many major investigations as Systems group leader, such as the Germanwings A320 flight 4U9525 or the Swiftair MD83 flight AH5017