Published July 2016

Report

Serious incident on **24 May 2011**
during descent to Kuala Lumpur Airport (Malaysia)
to the Dassault Falcon 7X
registered **HB-JFN**
operated by **Jet Link AG**

BEA
Bureau d'Enquêtes et d'Analyses
pour la sécurité de l'aviation civile
Ministère de l'Environnement, de l'Enérgie et de la Mer

Safety Investigations

BEA investigations are conducted in accordance with the provisions of Regulation No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation.

The BEA is the French Civil Aviation Safety Investigation Authority. Its investigations are conducted with the sole objective of improving aviation safety and are not intended to apportion blame or liability. BEA investigations are independent, separate and are conducted without prejudice to any judicial or administrative action that may be taken to determine blame or liability.

SPECIAL FOREWORD TO ENGLISH EDITION

This report has been translated and published by the BEA to make its reading easier for English-speaking people. As accurate as the translation may be, the original text in French is the work of reference.

Table of Contents

Glossary

ACMU	Actuator Control Monitoring Unit
ADIRU	Air Data Inertial Reference Unit
ADI	Attitude Director Indicator
AMJ	Advisory Material Joint
ANSV	Agenzia Nazionale per la Sicurezza del Volo
AP	Autopilot
APU	Auxiliary Power Unit
ATPL(A)	Airline Transport Pilot Licence
ATSB	Australian Transport Safety Bureau
BSCU	Brake System Control Unit
CAS	Crew Alerting System
CODDE	Crew Operational Documentation for Dassault Easy
CRM	Crew Resource Management
CS	Certification Specifications
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FCL	Flight Crew Licensing
FDC	Flight Data Concentrator
FFS	Full Flight Simulator
FHA	Functional Hazard Assessment
FL	Flight Level
FMEA (AMDEC)	Failure Mode, Effects Analysis
ft	Feet
HSEBU	Horizontal Stabilizer Electronic Backup Unit
HSECU	Horizontal Stabilizer Electronic Control Unit
HSI	Horizontal Situation Indicator
HSSU	Horizontal Stabilizer Sensor Unit
HSTA	Horizontal Stabilizer Trim Actuator
ICAO	International Civil Aviation Organisation

ICATEE	International Committee for Aviation Training in Extended Envelopes
IPT	Integrated Procedures Trainer
JAR	Joint Aviation Requirements
kg	kilo
kt	Knot
lbs	Pounds
LOCART	Loss of Control Avoidance and Recovery Training
MAIC	Maintenance and Avionics Interface Computer
MDU	Motor Drive Unit
MDU	Multifunction Display Unit
MEL	Minimum Equipment List
MFCC	Main Flight Control Computer
MMEL	Master Minimum Equipment List
NTSB	National Transportation Safety Board
PDU	Primary Display Unit
PF	Pilot Flying
PNF	Pilot Non Flying
PSSA	Preliminary System Safety Assessment
RMT	RuleMaking Task
SFCC	Secondary Flight Control Computer
SSA	System Safety Assessment
TCAS	Traffic alert and Collision Avoidance System
THS	Trimmable Horizontal Stabilizer
TOGA	Take Off / Go Around
VMC	Visual Meteorological Conditions

Synopsis

Pitch trim runaway in normal law, during descent

Aircraft	Dassault Falcon 7X registered HB-JFN
Date and time	24 May 2011 at approximately 19 h 55[(1)]
Opertor	Jet Link AG
Place	Malaysian airspace in descent to Subang Airport (Malaysia)
Type of flight	Public transport, non-commercial repositioning flight
Persons on board	Captain (PNF), co-pilot (PF), one member of a commercial air crew
Consequences and damage	None

[(1)] All times in this report are UTC, except where otherwise specified.

ORGANISATION OF THE INVESTIGATION

The serious incident 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 the HSECU), and Malaysia (State of Occurrence) participated in the investigation.

The investigation lasted over four years during which the exact determination of the circumstances and the retrieval of information from equipment manufacturer Rockwell-Collins proved to be difficult. Specifically, receiving replies could take several months. This was justified by the fact that the BEA's investigation into the organisational factors that led to the serious incident was unprecedented and the various elements required for replies took time to retrieve.

1 - FACTUAL INFORMATION

1.1 History of Flight

Note: the following information was compiled from data taken from the flight data recorder (FDR) and crew accounts.

On 24 May 2011 at 08 h 10, the crew of the Falcon 7X registered HB-JFN took off from Nuremberg (Germany) bound for Kuala Lumpur (Subang Airport) for a repositioning flight. The co-pilot was PF.

During the descent, the autopilot (AP) and auto-throttle were engaged and the calibrated airspeed was 300 kt. At approximately 19 h 55, the PF reduced the rate of descent on approaching the cleared altitude (11,000 ft). He selected a rate of descent of 1,300 ft per minute and activated vertical mode VS[2]. A few seconds later, when the aeroplane had passed below 13,000 ft, the horizontal stabilizer THS[3] went from neutral to maximum nose-up position (12 degrees) in fifteen seconds.

The AP remained engaged for the first eight seconds of THS deployment. The flight control laws counteracted the nose-up movement of the THS by a nose-down action on the elevators, which reached approximately two-thirds of their maximum travel before AP was disconnected[4]. The THS continued its nose-up movement. The aeroplane's pitch attitude and load factor increased.

The PF applied maximum nose-down input on the sidestick and placed the throttle levers in Take-Off position. The auto-throttle disconnected. The PF's nose-down input did not stop the nose-up movement of the THS, which reached its limit seven seconds after AP was switched off. The FCS displayed *"TRIM LIMIT"* on the PDU. Between disconnection of the AP and when the THS reached its stop, the calibrated airspeed dropped from 297 to 220 kt.

The increased pitch attitude during THS runaway was combined with a slight bank to the right and increased altitude. The PF made a leftwards input on the sidestick, causing the aircraft to bank 15 degrees to the left. The pitch attitude reached 25 degrees nose-up. Feeling that his pitch input was ineffective, the PF made a full rightwards input. He explained that he was trying to bank enough to decrease the pitch attitude, increase speed and regain pitch control. During the manoeuvre, the bank angle reached 98 degrees to the right.

Meanwhile, the Captain (PNF) made nose-down inputs and roll inputs contrary to those of the PF. These simultaneous inputs decreased the bank input of the PF and increased the pitch attitude, load factor and angle of attack once again. These simultaneous inputs triggered the *"DUAL INPUT"* alarm. The PF stated that he therefore asked the PNF to stop making inputs on his sidestick. He also took over priority of the controls by pressing the appropriate push-button on his sidestick for six seconds. The PF maintained the bank angle at 40 to 80 degrees to the right for about twenty seconds. After reaching 42 degrees nose-up, the pitch attitude gradually decreased to 10 degrees. The angle of attack and load factor fell quickly, from 22 to 5 degrees and from 4.5g to between 1.25 and 1.5g respectively. Meanwhile, the calibrated airspeed dropped from 300 kt to 150 kt.

[2] Mode to maintain vertical speed.

[3] Tail Horizontal Stabilizer, acronym used by Dassault.

[4] On disconnection of the AP, the pitch attitude was zero degrees and the load factor 2g, both rising.

The PF then made leftwards roll inputs until the bank angle was stabilised at about 50 degrees. The THS remained in full nose-up position, and the pitch attitude and calibrated airspeed remained stable for around forty seconds, at 10 degrees nose-up and 200 kt respectively. The PNF stated that he attempted to use the manual pitch trim and reengage the flight controls by pressing the *"FCS ENGAGE"* push-button on the upper panel.

Noticing no improvement, the PNF made roll inputs on his sidestick, in the opposite direction to those made by the PF, as well as full nose-down inputs. The simultaneous roll inputs of the two pilots gradually brought the bank angle to zero, which caused the pitch angle to increase once again to approximately 30 degrees, and the calibrated airspeed to drop to 125 kt. The crew stated that they heard the *"INCREASE SPEED"* alarm. This second dual input phase lasted approximately twelve seconds. The Captain then took over the controls. The attitude began to decrease and the altitude reached a maximum of 22,500 ft. When the attitude reached 5 degrees nose-down, the Captain made nose-up inputs. The attitude increased again and the Captain resumed making full nose-down inputs.

For a reason unknown to the crew, the THS began to move towards a level position, going from twelve degrees to one degree nose-up in fifteen seconds. The aeroplane pitch was once again able to be controlled via inputs on the sidestick. The crew made the decision to continue in manual flight mode. The approach and landing took place with no any further incidents.

2 minutes and 36 seconds passed between the start of THS nose-up movement and its return to balanced position. During this time:

- the load factor reached 4.6g;
- altitude increased from 13,000 to 22,500 ft;
- the calibrated airspeed went from 300 to 125 kts;
- the pitch attitude reached 41 degrees.

Following this serious incident, the Falcon 7X fleet was temporarily grounded[5]. It returned to service on 16 June 2011.

[5] By an urgent EASA Airworthiness Directive issued on 26 May 2011 (AD No.: 2011-0102-E).

1.2 Injuries to Persons

	Injuries		
	Fatal	**Serious**	**Minor/None**
Crew	-	-	3
Passengers	-	-	-
Others	-	-	-

1.3 Damage to Aircraft

Maintenance inspections following the incident detected no damage.

1.4 Other Damage

There was no damage.

1.5 Personnel Information

1.5.1 Captain

1.5.1.1 Captain

Male, aged 39.

1.5.1.1 Experience and qualifications

- ATPL(A) issued on 30 October 2010 in accordance with JAR-FCL1 requirements;
- practical exam for Falcon 7X type rating on 03 February 2011;
- valid Falcon 7X and Falcon 900 type rating;
- captain's training in June 2006;
- last base check on 03 February 2011;
- last line check on 15 May 2011;
- last CRM training in February 2010;
- medical certificate (class 1) issued on 09 December 2010.

Experience:

- 3,917 flying hours, including 134 on type;
- 125 hours in the last three months, all on type;
- 57 hours in the last thirty days, all on type;
- no hours in the last 24 hours.

1.5.1.2 Aviation career

- pilot instructor from 1994 to 2000;
- hired by Jet-Link AG as a co-pilot on Falcon 900s in July 2001.

1.5.2 Co-pilot

Male, aged 40.

1.5.2.1 Experience and qualifications

- ATPL(A) issued on 15 May 2008 in accordance with JAR-FCL1 requirements;
- practical exam for Falcon 7X type rating on 10 March 2011;
- valid Falcon 7X and Falcon 900 type rating;
- last base check on 10 March 2011;
- after the type rating practical exam, the co-pilot was in line training under supervision;
- last CRM training in February 2011;
- medical certificate (class 1) issued on 17 March 2011.

Experience:

- ❒ 2,685 flying hours, including 83 on type;
- ❒ 83 hours in the last three months, all on type;
- ❒ 57 hours in the last thirty days, all on type;
- ❒ No hours in the last 24 hours.

1.5.2.2 Aviation career

- fighter pilot on the Mirage 2000 from December 1994 to September 1999, and on the Mirage IV from September 1999 to September 2002;
- air Force Flight Safety Officer from 2002 to 2005;
- falcon 900 co-pilot with Netjets (business jet operator) from June 2008;
- hired in February 2010 by the owner of HP-JFN as co-pilot on the Falcon 900;
- transferred to Jet-Link AG, operator of HB-JFN.

1.6 Aircraft Information

The HB-JFN is owned by Wallenmount Ltd, based in Hong Kong and is operated by Jet-Link AG, a business jet operator based in Switzerland.

1.6.1 Airframe

Manufacturer	Dassault Aviation
Type	Falcon 7X
Serial Number	116
Registration	HB-JFN
Entry into service	March 2011
Certificate of airworthiness	Valid, issued by the Swiss Federal Office of Civil Aviation
Airworthiness examination certificate	Valid
Utilisation as of 24 May 2011	164 flying hours and 67 cycles

1.6.2 Engines

Manufacturer: Pratt & Whitney Canada
Type: PW307A

	Engine 1	**Engine 2**	**Engine 3**
Serial Number	PCE-CH 0367	PCE-CH 0366	PCE-CH 0368
Installation date	07 March 2011	07 March 2011	07 March 2011
Total running time	164 hours and 67 cycles	164 hours and 67 cycles	164 hours and 67 cycles

1.6.3 Weight and balance

The weight of the aeroplane at take-off was 69,243 lbs for a maximum authorised take-off weight of 70,000 lbs or 31,751kg. The estimated centre of gravity of the aeroplane at take-off was 27.5% from the mean aerodynamic chord (MAC), which was within operational limits (19.5 to 31.33%).

At the time of uncommanded THS runaway, the weight of the aeroplane was estimated by the operator to be 41,000 lbs and the centre of gravity 31.9% from the MAC, which was within operational limits (19.5 to 38.5%).

1.6.4 Maintenance

HB-JFN had been in Nuremberg from 19 to 23 May 2011 for maintenance operations. They consisted mainly of cabin and engine work and were carried out by Aero Dienst, a Part 145 approved maintenance organisation (DE.145.0059). Aero Dienst approved the aircraft for return to service on 23 May 2011.

1.6.5 Instrument panel

1.6.5.1 Displays

The Falcon 7X is equipped with the EASy (Enhanced Avionics System) avionics suite, which comprises four displays that provide flight information and a flight management system, and display system status and electronic checklists. The crew can configure these displays according to operational needs.

In standard configuration, the Primary Display Unit (PDU) contains:

- an Attitude Director Indicator (ADI) with critical flight information (attitudes, airspeed, altitude, etc.);
- a Horizontal Situation Indicator (HSI) that combines key flight information;
- the ENG-CAS window, which displays engine parameters and Crew Alerting System (CAS) messages;
- one window that can be configured to display trim positions (ENG-TRIM window), radio and radio navigation systems, and traffic information from the TCAS. At the time of the THS runaway, this window was displaying radio and radio navigation systems on the left-hand PDU and the ENG-TRIM window on the right-hand PDU. A few seconds after the Captain took over the controls, this window on his PDU switched to display on ENG-TRIM window.

The MDUs are more flexible and can be used by the crew to display any of the following, depending on flight phases:

- additional navigation and flight management information (maps, lists of turning points, aircraft performance, etc.);
- diagrams showing the status of systems and switches.

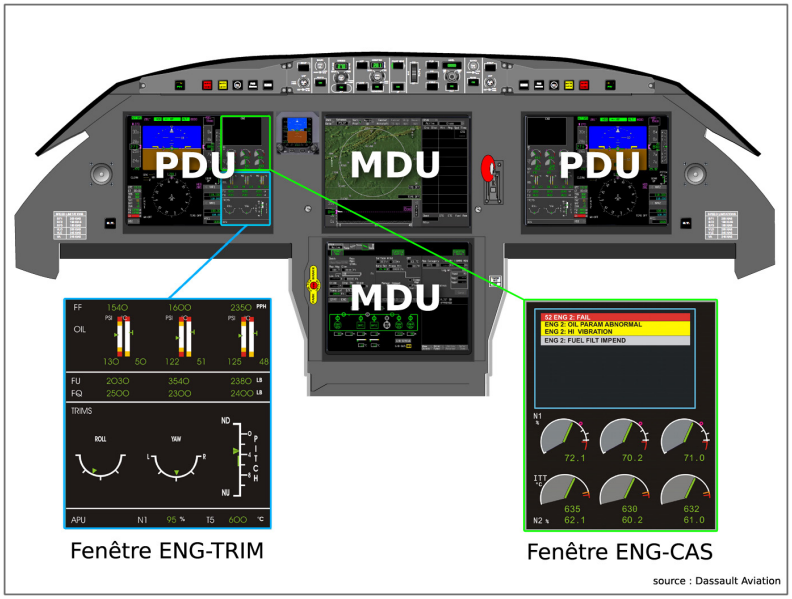


Figure 1 - instrument panel

1.6.5.2 Crew Alerting System

The CAS constantly monitors system status and alerts the crew by displaying a message in the ENG-CAS window and/or or generating an audio alarm depending on the severity of the failure.

During the incident, the amber *"FCS: TRIM LIMIT"* message was displayed. An amber message indicates a failure or abnormal event requiring the immediate attention of the crew and corrective action.

The CAS generates a *"FCS: TRIM LIMIT"* message when the pitch or roll order is 90% higher than the maximum order. The associated corrective action required of the crew is to:

- ❒ maintain an airspeed and controls for which the forces exerted on the flight controls are acceptable;
- ❒ check the state of control surfaces, fuel distribution, balance, and possible ice build-up to correct the movement of the horizontal stabilizer;
- ❒ and return to an airspeed and configuration that correspond to the flight phase.

When the *"FCS: TRIM LIMIT"* message is displayed, a Master Caution alert lights up and a *"Gong"* warning is triggered.

1.6.5.3 Dual input warning

The Falcon 7X has two separate sidesticks to control aeroplane pitch and roll. In the event of simultaneous input by both pilots, orders are algebraically commanded. A *"DUAL INPUT"* alarm is generated and the stick vibrates.

Each pilot is able to deactivate the other's sidestick at any time by pressing and holding down the priority (PTY) push-button.

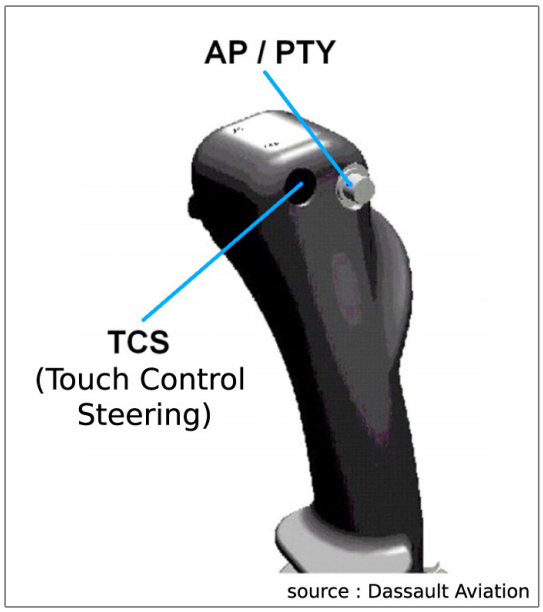


Figure 2 - sidestick

If the button is held down:

- a green PTY[6] indicator light comes on in front of the pilot whose sidestick is active;
- an amber arrow lights up in front of the pilot whose sidestick is deactivated, pointing to the side that has priority;
- a *"PRIORITY RIGHT"* audio alarm is generated if the pilot in the right-hand seat has priority, or *"PRIORITY LEFT"* if priority is on the left-hand side.

[6]PRIORITY.

Thus, when the co-pilot takes priority over the Captain, the following indicator lights are displayed on the left-hand side in front of the Captain, and on the right-hand side in front of the co-pilot:

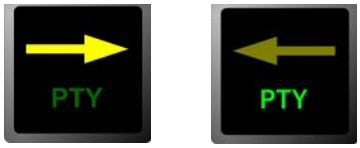


Figure 3 - priority indicator lights

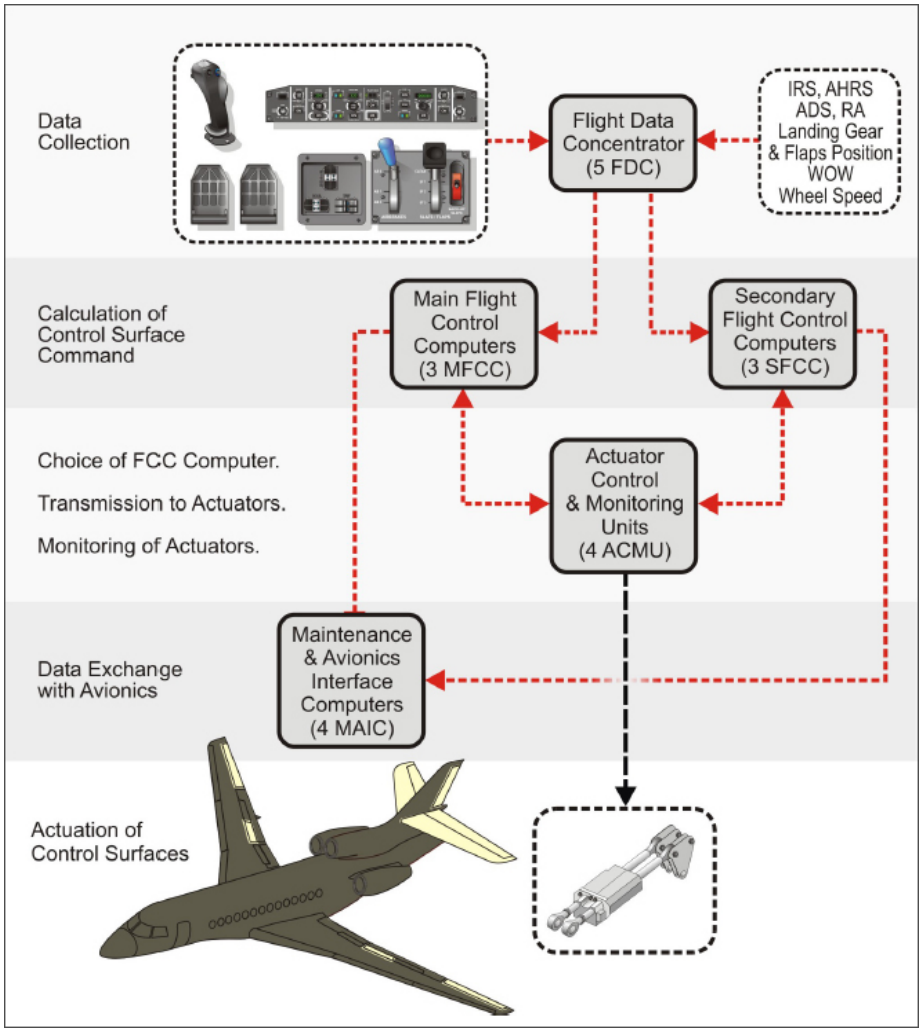
1.6.6 Pitch trim system

1.6.6.1 General architecture of the electrical flight control system

The Falcon 7X electrical flight control system operates with the following elements:

- five Flight Data Concentrators (FDC), which collect data from the aeroplane sensors and monitoring devices;
- three Main Flight Control Computers (MFCC) and three Secondary Flight Control Computers (SFCC), which receive information from the FDCs and generate turning commands for the control surfaces based the flight control laws that are available;
- four Actuator Control Monitoring Units (ACMU), which each receive orders from all the MFCCs and SFCCs, dismissing any inconsistent commands, then send the turning command to the associated control surfaces. The ACMU then slaves the servo actuators to the orders;
- four Maintenance and Avionics Interface Computers (MAIC), which receive data[7] from the MFCCs, SFCCs and other computers. Based on this information, the MAICs generate the information presented in the various synoptic displays and CAS messages.

[7] Particularly flight control law modes (Normal, Alternate, Direct Laws) and failure statuses from the various sensors / computers /actuators.



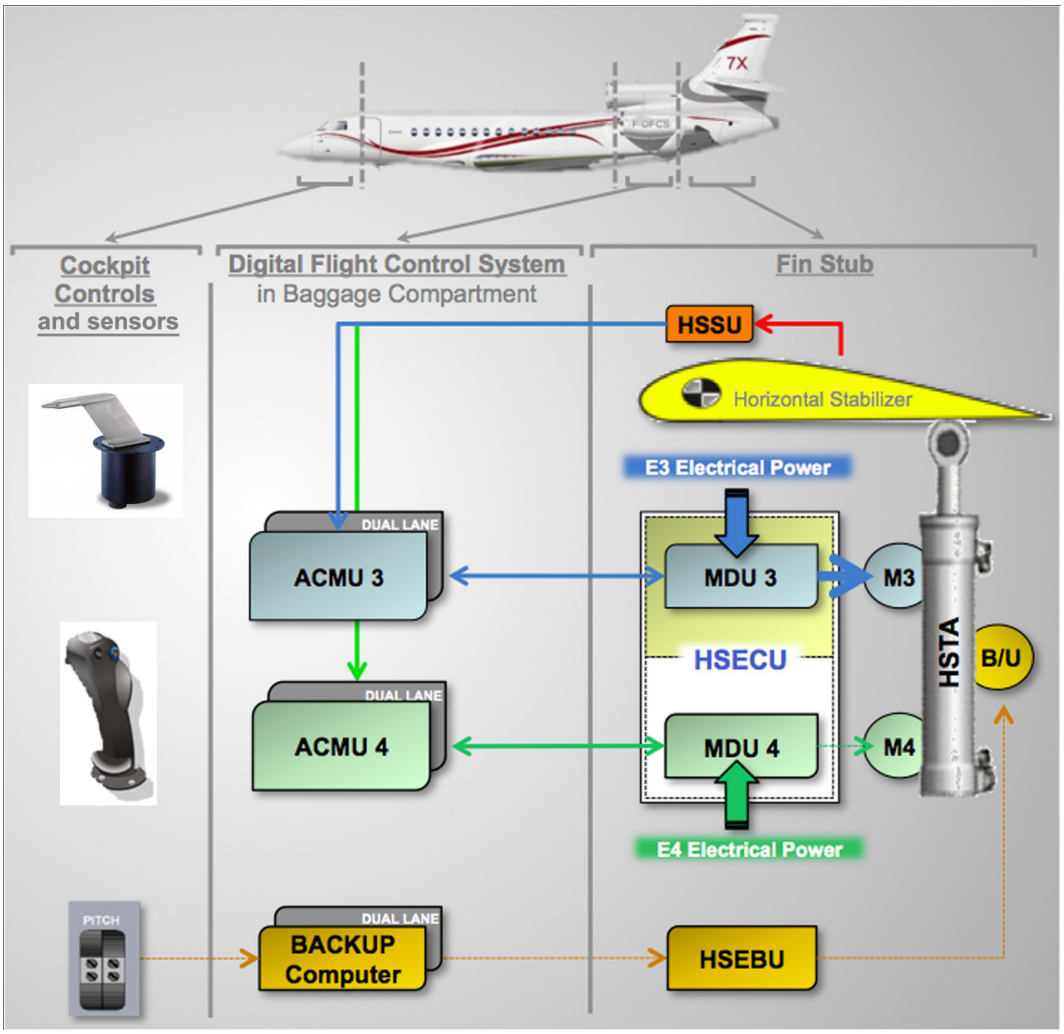
(source : Dassault Aviation)

Figure 4 - general architecture of the electrical flight control system

1.6.6.2 THS control

The THS is controlled via the following components:

- a Horizontal Stabilizer Trim Actuator (HSTA) that can be actuated by three electrical motors, M3, M4 and B/U (Backup);
- a Horizontal Stabilizer Electronic Control Unit (HSECU) with two control channels, MDU3 (Motor Drive Unit) and MDU4, which control M3 and M4 motors respectively;
- ACMU3 and ACMU4, which receive THS position commands from the MFCCs and SFCCs and generate the M3 an M4 rotation speed command. This command is then transmitted to MDU3 or 4. The ACMUs also monitor their associated MDUs;
- two double Horizontal Stabilizer Sensor Units (HSSU), which send this information to the ACMUs;
- a Horizontal Stabilizer Electronic Backup Unit (HSEBU) which controls the actuator backup motor (B/U);
- a BACKUP Computer, which receives commands from the manual trim control in the cockpit and transmits them to the HSEBU.



(source : Dassault Aviation)

Figure 5 - THS control

Three independent channels therefore control the pitch trim:

- channel 3, which is the active channel in normal operating conditions. In this case, MDU3 controls motor 3 based on commands from ACMU3. Motors 4 and B/U are not powered and auto-trim is active;
- channel 4, which is activated when a problem is detected on motor 3. The HSECU then switches over to MDU 4 which controls motor 4 based on the commands from ACMU 4. The auto-trim function remains active;
- the backup channel is used when a problem is detected on motors 3 and 4. In this case, the auto-trim function is lost. The THS is then controlled manually by the crew via the control in the cockpit.

In flight, if the auto-trim function is active, the crew cannot manually control the THS and only has access to the manual control if the auto-trim function is lost.

Commands from control channels 3 and 4 to the motors that actuate the THS are transmitted in the form of motor rotation speeds.

The checks used to change the control channel are carried out by the ACMUs, based mainly on:

- the position of the THS, transmitted by the HSSU, and
- the following information from the HSECU:
  - THS motor speed and direction of rotation;
  - motor temperature;
  - electrical current consumed.

A number of checks are designed to detect THS runaway depending on the cause of the malfunction (HSSU, ACMU or HSECU). The checks used to detect runaway caused by an HSECU malfunction consist in verifying the consistency between:

- the speed set point calculated by the ACMU and
- the motor actual rotation speed and direction transmitted by the HSECU.

Consumed current and motor temperature checks are also designed to trip if the THS becomes stuck (saturation, mechanical jam, mechanical limit).

Therefore the monitoring function carried out by the ACMU for the THS control channel thus depends on the parameters transmitted by the HSECU, which controls the THS.

1.6.7 Autopilot

AP can be switched off manually or automatically. It automatically disconnects in any of the following conditions:

- the TOGA push-button on the throttle lever is actuated;
- loads on one of the sidesticks exceed a certain threshold;
- an autopilot failure is detected;
- the flight control system high or low speed protections are activated;
- the roll or pitch angle exceeds 80 or ± 60 degrees respectively.

Thus, during the incident, based on the FDR parameters (see appendix 1), the only condition that could have caused the AP to automatically disconnect was the nose-down input of the co-pilot on his sidestick.

1.7 Meteorological Information

The crew stated that when the incident occurred, the aeroplane was flying in VMC with no turbulence.

1.8 Aids to Navigation

N/A.

1.9 Communications

N/A.

1.10 Aerodrome Information

N/A.

1.11 Flight Recorders

The aeroplane was equipped with two flight recorders[8], each able to record data from the last 25 flying hours and audio information from the last two flying hours.

The aeroplane electrical power supply was not shut off on the apron and audio recordings concerning the event were therefore not available.

FDR graphs are appended in Appendix 1.

[8] Both flight recorders are identical and were manufactured by Honeywell (P/N 980-6021-072).

1.12 Wreckage and Impact Information

N/A.

1.13 Medical and Pathological Information

N/A.

1.14 Fire

N/A.

1.15 Survival Aspects

N/A.

1.16 Tests and Research

1.16.1 HSECU inspections

The HSECU is manufactured by Rockwell Collins to meet Dassault Aviation technical specifications. It is integrated into the pitch trim control system by Dassault Aviation.

Functional tests and a visual inspection did not detect any HSECU malfunctions.

Note: visual inspections of the HSECU circuit boards did reveal that, due to their location, some components on adjacent boards were in mechanical contact with each other. It was later determined that these mechanical interferences did not cause the incident. However, Rockwell Collins did introduce a modification, as detailed in Section 5 of this report.

Tests carried out on HSECUs identical to those on the HB-JFN showed that when the HSECU circuit boards were powered at an internal voltage around +0.7 V, instead of a nominal voltage of -15 V, it reproduced a THS runaway similar to the incident.

Inspection of the -15V power supply pinpointed three failure modes that could have caused such voltage variations. Additional testing was carried out to detect whether one of these failure modes was present on the HSECU on the HB-JFN. It revealed that:

- the impedance[9] value of component L4 was unstable, varying between the nominal value 0.5 Ω and abnormal values of up to 300 kΩ when slight pressure was applied to the component;
- one of the solders of the induction coil had cracks at the base, causing loss of the mechanical joint and the component pin could potentially move in the printed circuit board. This type of solder is called a *"cold solder joint"*.

[9]The impedance of an electrical component is a measure of the opposition that the component presents to an electric current.

Figure 6 - solder defect on the L4 induction coil

After refitting the circuit board in the unit and turning on the power, the -15V power supply malfunction could not be reproduced despite several attempts.

X-ray inspection of the soldering defect revealed:

- that there was no alloy in 90% of the plated through- hole[10];
- micro-cracks between the component and printed circuit board pin.

[10]Hole in a circuit board into which the pin of a component is inserted and soldered.

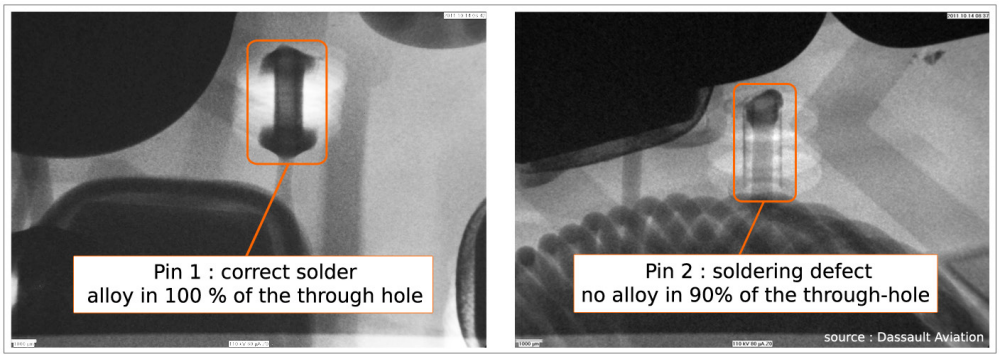


Figure 7 - X-ray of the soldering defect on the L4 induction coil

1.16.2 Cause of the pitch trim runaway

The soldering defect created impedance fluctuations in component L4, causing the HSECU internal power supply to output an incorrect voltage, both in terms of absolute value and sign (+/-).

Due to this soldering defect, the HSECU control channel generated and transmitted a constant nose-up command to the THS motor, while sending a rotation speed signal to the ACMU that indicated a nose-down movement of the THS, as illustrated in the diagram below.

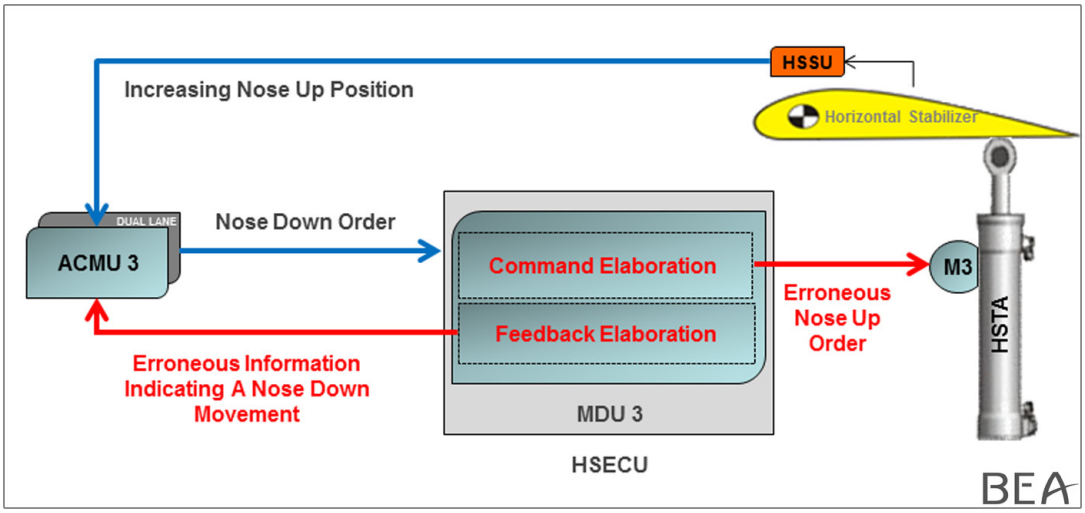


Figure 8 - Impact of the HSECU internal power supply malfunction

To counter the nose-up movement of the aeroplane, the ACMU sent a nose-down order to the HSECU while receiving from the HSECU a speed signal indicating nose-down movement of the THS, consistent with the order transmitted.

Consequently, the monitoring function based on the consistency between the speed set point sent by the ACMU and the speed signal fed back by the HSECU did not trip.

Further, the monitoring based on the consumed current did not trip either. Inspections of the HSECU revealed that this monitoring does not trip when the internal power (-15 V) is incorrect (in this case for voltages around +0.7 V). When it was designed, the possibility that a -15V power supply could output such voltage values was not taken into account.

When the THS actuator then reached its limit and continued to receive nose-up commands, the temperature of the M3 motor increased. When its activation limit was exceeded, the temperature monitoring function tripped. The ACMU then switched THS control to channel 4, which commanded a nose-down movement of the THS until it returned to a balanced pitch.

1.16.3 Origin of the soldering defect

The presence of micro-cracks on the solder of one of the L4 induction coil pins was caused by insufficient heat during the soldering process. This was because the plated through-hole was not being properly insulated from the rest of the circuit board. Part of the soldering heat was therefore absorbed, preventing the creation of a proper solder.

1.17 Organisational and management information

1.17.1 EASA and type certification information

1.17.1.1 Definitions

CS/JAR 25: Certification specifications for aeroplanes with a maximum take-off weight of over 5 700 kg.

Part 21: Acceptable means of compliance and guidance material for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations

Design organisations: Organisation responsible for designing products, parts and appliances, and modifications and repairs thereto. It must demonstrate its capability in accordance with provisions of Part 21. In particular, it must control and oversee all design aspects. The design organisation must establish a quality system for accepting parts or appliances produced by partners or subcontractors.

Production organisations: Organisation responsible for the manufacture of products, parts and appliances. It must demonstrate its capability in accordance with provisions of Part 21.

1.17.1.2 EASA information

The European Aviation Safety Agency (EASA) is the authority appointed by the European Commission to harmonise aviation safety standards in Europe and to oversee Member State design and production functions and tasks.

To this end, EASA issues type certificates and design organisation approval.

Approved design organisations applying for type certificates must demonstrate compliance with applicable technical conditions and submit to EASA the means by which compliance is demonstrated.

Approved production organisations must submit statements of compliance for all aircraft, parts, products or appliances. These statements are used to ensure that:

- each product, part or appliance complies with approved design data and that they can operate safely;
- each aircraft has undergone ground and flight tests.

EASA validates statements of compliance if, after inspection, it considers that the product, part or appliance complies with applicable conditions and is in condition for safe operation.

EASA 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 organisation define the documents to be reviewed depending on the project to be certified.

Three categories of documents were defined for Falcon 7X certification:

- **Category 2**: document submitted to EASA for approval after validation by the design organisation;
- **Category 1**: document accepted by EASA without verification and submitted to EASA for information purposes after validation by the design organisation;
- **Category 0**: document accepted by EASA without verification and not submitted to EASA after validation by the design organisation. The design organisation must provide this type of document upon EASA request.

1.17.1.3 Flight control regulatory requirements

Regulations applicable to flight control systems are specified in Paragraphs JAR 25.671 and JAR 25.1309. FAR regulations include the same requirements.

■ JAR 25.671[(11)]: Control systems: General

The aeroplane must be shown by analysis, tests, or both, to be capable of continued safe flight within the normal flight envelope, without requiring exceptional piloting skill or strength after the following failures:

- any single failure not shown to be extremely improbable, excluding jamming;
- any combination of failures not shown to be extremely improbable[(12)];
- any jam in a control position normally encountered during take-off, climb, cruise, normal turns, descent and landing unless the jam is shown to be extremely improbable, or can be alleviated;
- a runaway of a flight control to an adverse position and jam must be accounted for if such runaway and subsequent jamming is not extremely improbable.

[(11)] JAR 25.671 and special conditions applicable to the Falcon 7X.

[(12)] Probability of 1 x 10-9 or less per flying hour.

- JAR 25.1309[13]: Equipment, systems and installations

This paragraph applies to numerous systems and equipment, including the horizontal stabilizer system. It provides additional requirements to supplement JAR 25.671, including the following:

- (b): aeroplane systems and associated components, considered separately and in relation to other systems must be designed so that:
  - the occurrence of any catastrophic failure condition[14] which would prevent the continued safe flight and landing of the aeroplane is extremely improbable;
  - the occurrence of any other hazardous failure condition which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions is improbable[15];
  - any major failure condition is remote[16].
- (d): compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider:
  - 1. possible modes of failure, including malfunctions and damage from external sources;
  - 2. the probability of multiple failures and undetected failures;
  - 3. the resulting effects on the aeroplane and occupants;
  - 4. crew warning cues, corrective action required and the capability of detecting faults.

To demonstrate compliance with the abovementioned requirements, acceptable means (AMJ[17]) are also outlined in JAR 25. The following points from paragraph JAR 25.1309 are of note:

- These means are based on the principle that there should be an inverse relationship between:
  - the severity of the effects of a failure (five levels: no effect, minor, major, hazardous, catastrophic) and
  - the probability of its occurrence (probable, remote, extremely remote, extremely improbable). These probabilities are defined qualitatively and quantitatively. For example, any catastrophic failure condition should be extremely improbable.
- The Fail-Safe Design concept defines basic objectives pertaining to failures. For example, in any system or subsystem, the failure of any single element, component or connection during any one flight should not lead to catastrophic failure conditions.
- Since not all means of compliance with JAR 25.1309 (b) and (d) have been defined, the designer and certifying authority must agree on the means early in the analysis process.
- Various methods for assessing the causes, severities, and likelihood of potential failure conditions are available, including failure mode, effects and criticality analysis (FMECA or FMEA). FMEAs are structured, inductive analyses which can be used to evaluate the effects on the system and aeroplane of each possible element or component. The section specifies that when analysis is properly formatted, it will aid in identifying latent failures and the possible causes of each failure mode.

[13] JAR 25.1309 and special conditions applicable to the Falcon 7X.

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

[15] Probability of 1 x 10-7 or less per flying hour but greater than 1 x 10-9.

[16] Probability of 1 x 10-5 or less per flying hour but greater than 1 X 10-7.

[17] Advisory Material Joint.

1.17.1.4 Safety assessment process

The safety assessment process can be represented as a V cycle. The left-hand part of the V corresponds to the development, specifications and validation phase, and the right-hand part to the integration and verification phase.

For compliance with JAR25.1309, safety assessments during the system design phase include the following documents:

- FHA (Functional Hazard Assessment): These are preliminary engineering assessments that are frequently updated as the aeroplane and system designs evolve.
  - they examine the functions of the aeroplane and systems and identify functional failure conditions associated with each of these functions;
  - they determine the effects of all identified failure conditions and their severity.
- PSSA (Preliminary System Safety Assessment): This type of assessment evaluates system designs and applies safety objectives defined in the FHA to the relevant systems and equipment. They typically contain fault trees of failure conditions identified in the FHA and an estimate of associated probabilities of occurrence.
- SSA (System Safety Assessment): SSAs take into account the results of FMEAs (see below) 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.
- FMEA (Failure Mode Effects Analysis): FMEAs identify the following aspects for each component of equipment via the most exhaustive inductive approach possible:
  - the functions of the component;
  - the various failure modes of each component;
  - the causes of failures (type of failure for each component or function of the equipment);
  - the effects of each failure on the equipment or system;
  - the probability of each failure.

FMEAs are used extensively in industry to determine the failure conditions of equipment. They rely partially on the knowledge and experience of the equipment manufacturer personnel with failure modes and mechanisms.

EASA ensures that design organisations submit all the documents necessary for type certification. It checks and approves FHAs and SSAs. EASA does not systematically verify FMEAs and is therefore not necessarily in contact with equipment manufacturers during type certification of an aircraft.

1.17.1.5 Technical standards

Equipment manufacturers can refer to the following reference documents to prepare safety assessments:

- American military technical document MIL-STD-1629A of 24 November 1980;
- ARP4761 of December 1996;
- DO178B of December 1992.

MIL-STD-1629A

This document is a military standard that defines procedures for developing equipment failure analyses and evaluating the potential impact of their functional or material failure. It can be used to design, develop, evaluate and validate a programme.

ARP 4761

Technical standard ARP4761 is an SAE[18] publication that provides guidelines for preparing safety assessments for compliance with JAR/FAR 25.1309 regulatory requirements. It details the safety assessment processes for complex systems (FHAs, Preliminary SSAs, SSAs) and the methods that can be used (including FMEAs) to comply with the process. It particularly recommends using common mode analysis (CMA) to ensure independence between functions using the same information sources (signals, power supply, etc.) and to identify any common mode defects. It is cited as a reference in the means of compliance with Paragraph 25.1309 of the current version of CS25. This document specifically states in paragraph G.3.2.2 that : *«Determining all the failure modes of any but the simplest components (where industry data is available) is extremely difficult and sometimes impossible»*.

[18] Society of Automotive Engineers. Professional association founded in 1905 by industry professionals to develop and share technical standards, including ARPs, Aerospace Recommended Practices.

DO178B

This document was drawn up jointly by EUROCAE (European Organization for Civil Aviation Equipment) and RTCA (Radio Technical Commission for Aeronautics) and acts as a guide for the development of software to be certified. This document compiles best practices that have been applicable in the industry for many years. Rather than recommending a particular method or process, it sets objectives with which these processes must comply.

1.17.2 Dassault Aviation information

1.17.2.1 Falcon 7X type certification

EASA issued type certification for the Falcon 7X on 27 April 2007[19]. On the date of the incident the Falcon 7X fleet had logged approximately 75,000 flying hours.

The Falcon 7X meets certification specifications in force at the time of type certification, including JAR25 change 15[20] and special requirements issued by EASA.

[19] The Falcon 7X was also certified by the FAA.

[20] JAR25 change 16 for JAR 25.1309 (b) and special requirements for JAR25.671 (See 1.17.1.3).

In accordance with these regulatory requirements and certain standards, Dassault Aviation, (an EASA Part 21 approved design organisation) developed technical specifications for all of the aeroplane's equipment. The design of HSECU electronic controllers was subcontracted to Rockwell-Collins, which is not an EASA approved design organisation. This design activity was therefore conducted under the supervision of Dassault. Dassault and Rockwell-Collins therefore had frequent meetings and technical reviews during the HSECU design phase. They were approved for installation on the Falcon 7Xs and meet Dassault Aviation specifications.

1.17.2.2 Falcon 7X flight control system safety assessments

The Falcon 7X flight control system underwent an SSA based on a simulation tool (OCAS[21]) This method provides an integrated approach to safety assessments. This method was selected in consultation with EASA.

[21]Qualified in accordance with technical standard DO178B verification tools.

This tool was qualified according to technical document DO178B for conducting an in-depth PSSA and SSA of the Falcon 7X flight control system. This document is a Category 2 document (see 1.17.1.2) submitted for EASA approval after Dassault Aviation validation. It contains five documents:

- **Safety assessment of the primary flight control system**:
  - This is a summary of all failure conditions and the associated severity and probability of occurrence.
- **Book 1 - Safety assessment of the primary flight control system:**
  - This document explains the results of quantitative and qualitative safety assessments for each failure condition.
- **Book 2 - Minimal cuts set[22]:**
  - This document lists all the failures or combination of failures of the various systems or equipment with the associated probability of causing a given failure mode.
  - This document is used to show how probabilities are obtained for the different failure modes of the primary flight control system.
- **Book 3 - MMEL**:
  - This document makes the connection between the failure modes in question and the MMEL.
- **Book 4 - Comprehensive event list**:
  - This document lists all the failures taken into account in the safety assessments for each failure mode of the primary flight control system.
  - The probabilities of these failures are also included in this document.

[22]Minimal cut sets for a given failure.

1.17.2.3 Safety assessment related to primary control surface runaway in normal law

The following information is highlighted in the primary flight control system safety assessment documents:

SSA:

- This document identifies a failure condition relating to one primary control surface runaway unstopped by any of the aircraft systems (called "*one primary control surface runaway*"). The objective for this failure condition, which is considered to have catastrophic consequences, is to have an extremely improbable likelihood of occurrence.
- For the pitch trim system, this failure condition corresponds to what occurred during the incident flight, i.e. the THS in limit position, resulting in potential loss of control of the aeroplane.
- The probability of occurrence estimated using the OCAS tool for the SSA is lower than this objective (2.2×10^{-10}), which is in compliance with regulatory specifications.
- The SSA also indicates that in the event of primary control surface runaway:
  - the problem is not signalled in the cockpit;
  - there are no procedures available to crews.

Book 1:

- This document defines the failure mode for a primary control surface runaway. This results from the deployment of spoilers, the rudder, ailerons or the elevator. There is no mention of the THS.
- The causes of each case of runaway are listed in the document. Pitch trim runaway is not included.

Book 2:

- No HSECU failures appear in any of the failures or combinations of failures for the flight control system.

Book 3:

- Not applicable to the failure mode examined.

Book 4:

Among all the failures taken into account for the of the primary flight control system safety analysis, Book 4 mentions no HSECU failures.

Thus, on the date of the incident, the primary flight control system safety analysis by Dassault Equipment did not cover pitch trim runaway in normal law. The manufacturer explained this by the fact that during the safety analysis for Book 2, as HSECU safety systems are based on software driven by two digital channels of ACMU3 and ACMU4, it was difficult to quantify the probability of a unarrested THS runaway. Given the multiple safety systems in place, the unarrested THS runaway was expected to be detected early enough to switch on the redundant channel in order to stop the runaway immediately. Thus, the probability of THS runaway was considered "*extremely improbable*".

Furthermore, the results of the PSSA qualified the ACMU that controls the THS and the HSECU as critical equipment[23]. Therefore the most stringent measures (DO178 and DO254 Level A) were taken to prevent any equipment design error, particularly for validation and verification activities.

[23]Equipment for which a failure, malfunction or design error can have catastrophic effects. This equipment must have the highest Development Assurance Level (A) in accordance with the good practices at that time which later became ARP 4754 (Guidelines for Development of Civil Aircraft and Systems, published by the SAE).

1.17.2.4 Dassault Aviation FMEA implementation

Safety assessments developed by Dassault take into account the FMEAs conducted by equipment manufacturers. FMEAs are classified as Category 1 documents and were sent for information purposes to EASA, which therefore did not validate them (*see 1.17.1.4*). Before being sent to EASA in accordance with certification plan rules, the FMEAs were reviewed by Dassault teams based on information provided by the equipment manufacturers. The purpose of these reviews was not to conduct another detailed analysis of failure conditions, since this had already been performed by the equipment manufacturer.

Note: For the HSECU, the safety systems included in the ACMU circuit boards take into account failure modes identified in the HSECU FMEA.

1.17.2.5 Operational documentation

The documentation developed by Dassault Aviation for crews include:

- the aircraft flight manual;
- an aeroplane operating manual, the CODDE[24], which has three sections:
  - CODDE 1: Description of the aeroplane and its systems
  - CODDE 2: Operating manual
  - CODDE 3:
    QRH1: normal procedures
    QRH2: emergency and abnormal procedures
    ECL: Electronic checklist

[24]Crew Operational Documentation for Dassault Easy.

1.17.2.6 Falcon 7X type rating programme

The type rating programme mainly sets out to familiarise crews with using and operating the aeroplane in compliance with CRM principles.

It includes a high nose-up attitude recovery exercise during two of the eight Full Flight Simulator (FFS) sessions which take place during initial type rating training.

For simultaneous inputs, design principles (visual, tactile and audio alerts, sidestick button) and dual input management principles (coordination between the pilots) are initially presented during theory training. An exercise to demonstrate how the sidesticks operate during dual input is completed during one of the FFS sessions. Training includes a virtual exercise in which one of the pilots takes over the controls in the event of pilot incapacitation.

1.17.2.7 Pitch trim runaway

Dassault Aviation operational documentation (CODDE Volume 2) includes an operational technique for managing pitch trim runaway in Appendix 1. It only covers the case in which the manual pitch trim is used, which means that the auto-trim function had been lost beforehand.

The technique described by Dassault Aviation specifies that once the situation is detected, the PF or PNF must announce *"TRIM RUNAWAY"*. The PF must then counter the trim runaway with the sidestick and manual pitch trim.

Since the event, Dassault Aviation has updated this technique in its operational documentation[25] (*see Section 5 of the report*).

[25]CODDE Volume 2.

1.17.3 Rockwell-Collins information

1.17.3.1 General description

Rockwell-Collins is an equipment manufacturer without design organisation approval. The HSECUs were designed under Dassault Aviation's design approval in accordance with Part 21[26].

[26]Part 21.A.239© and 21.A.243.

1.17.3.2 Development and validation of failure mode effects analyses (FMEA)

A technical division at Rockwell-Collins is responsible for defining specifications and validating FMEAs.

This technical division determines the resources to be allocated to the FMEA development, verification and planning process. According to Rockwell Collins, the primary skills and responsibilities required of senior engineers involved the process are as follows:

- knowledge in systems development;
- knowledge of technical standards such as ARP4761;
- specialist in an RMS specific field or general background in several fields;
- strong knowledge of the equipment and systems department;
- ability to:
  - organise, analyse, design, test and document complex products and ability to integrate them into a system;
  - estimate and track the costs and projections of a project while managing the associated risks;
  - provide logical and detailed analysis of problems and situations.

FMEAs are developed according to A Rockwell Collins quality process that follows a procedure based on technical reference MIL-STD-1629A and internal guidelines. The procedure especially includes reviews and validation throughout the document development process. These reviews can involve Rockwell Collins engineers and clients' representatives and possibly certification authorities.

1.17.3.3 Analysis of HSECU failure modes

All HSECU circuits were analysed according to the Rockwell-Collins internal quality process. The *"FMEA Methods and procedures"* section of the FMEA, specifies that *"all efforts were made to determine of the potential failure conditions that could affect the performance or use of the HSTA"*.

The first version of the HSECU FMEA dates back to July 2004. The version in effect at the time of the incident was Version C dated February 2008. It was developed, reviewed, and validated by three people at Rockwell Collins:

- **preparation and development**: a systems engineer with six years' experience in safety assessments in the field of systems reliability, maintenance and safety;
- **check**: An electronics engineer with 25 years' experience designing electrical systems for flight critical applications;
- **check and Validation**: A manager with ten years' experience in systems reliability, maintenance and safety in the aeronautical industry.

Teams at Dassault Equipment used the FMEA and electronic circuit boards provided by Rockwell-Collins to verify that failure modes corresponded to those usually identified, and that the local effects or systems of these failure conditions appeared plausible. Once document consistency was verified, the HSECU FMEA was submitted to EASA.

1.17.3.4 Failure conditions and associated effects related to the serious incident

Failure effects are described in general terms. Several consequences are mentioned as having a possible latent effect[27] or which could alter the operation of the HSECU. The following is noted for the L4 induction coil:

Failure type	Cause of failure	Local effect(for the component)	Overall effect	Failure detection method (A: crew; B: on the ground)
Short circuit	Part damage, material property degraded, eroded	noise	Loss of power boost, noise	Vendor test/evaluate; box ATP
Open circuit	Part damage, material property degraded, eroded	Loss – 15 Volt power	Loss of speed and direction interpretation, no motor drive for actuator	A: Loss of the normal channel B: Vendor test/ evaluate; box AT
Change value	aging	Potential latent failure	Assy or system level parameters, tolerances affected; otherwise latent.	Vendor test/evaluate; box ATP

[27]The latent effects of an HSECU component failure are found on 162 out of 181 pages of Version C of the FMEA.

For component L4, the failure type "*fluctuating value*" means that its inductance[28] value (in henries) varies.

[28]Inductance is the ability of an electrical component to create voltage at its terminals proportional to the current passing through it.

In the case of the incident, the circuit was partially open due to the soldering defect. The failure type to be considered may correspond to an "*open circuit*" and "*fluctuating value*". In the first case, the table shows that the effect is loss of the normal channel (channel 3). The second case is a potential latent failure that has an overall latent effect or can affect HSECU tolerances.

Rockwell-Collins gives the following definitions for terms used in the FMEA:

- a *"potential latent failure"* of a component is a failure that is not specifically monitored and which can therefore occur without being detected;
- the overall effect "*tolerances affected or latent"* means that if values fluctuate, there are no adverse effects if values remain below the acceptable range defined in the design. However, if fluctuating values exceed design tolerances, the behaviour of the component is altered and it becomes a latent failure.

In general, the FMEA indicates that identified failures essentially result in loss of the normal channel, switching the control channel to a redundant channel, or else the failures are considered as latent.

1.17.3.5 Update of the FMEA following the serious incident

Rockwell-Collins used the same method and reference documents to amend the FMEA[29] after the serious incident. In the new version, no failures are considered as latent and the descriptions of failure effects for each component or function of the HSECU are more detailed. In total, the identified failures can generate 31 different consequences affecting HSECU operation.

[29]Version D dated November 2011.

The following is particularly noted for the L4 induction coil (differences with Version C of the FMEA are shown in red):

Failure type	Cause of failure	Local effect (for the component)	Overall effect	Failure detection method (A: crew; B: on the ground)
Short circuit	Part damage, material property degraded, eroded	-15VDC stuck at 0 V	Motor untimely driven at overspeed AND Erroneous Velocity Output to ACMU (stuck to 0).	A) Uncommanded movement of actuator, detectable by external position sensors B) Vendor test/evaluate; Box ATP.
Open circuit	Part damage, material property degraded, eroded	Loss of -15VDC power supply from U3	Motor untimely driven at overspeed AND Erroneous Velocity Output to ACMU (not stuck to 0) AND OverCurrent output untimely stuck low (no fault state).	A) Uncommanded Movement of Actuator, Detectable by External Position Sensors B) Vendor test/evaluate; Box ATP.
Change value	aging	Worst case considered is an additional impedance across L4 leading to increase of -15 above 0V (demonstrated by tests)	Motor untimely driven at overspeed AND Erroneous Velocity Output to ACMU (not stuck to 0) AND OverCurrent output untimely stuck low (no fault state.	A) Uncommanded Movement of Actuator, Detectable by External Position Sensors B) Vendor test/evaluate; Box ATP.

1.18 Additional Information

1.18.1 Safety assessment methods

1.18.1.1 Qantas-operated Airbus A330 accident in Australia, 7 October 2008[30]

While cruising at 37,000 ft, one of the aeroplane's three ADIRU[31] started outputting intermittent, incorrect values on flight parameters, and particularly angle of attack data, to other aircraft systems. Approximately two minutes later, in response to spikes in angle of attack data, the aircraft's flight control primary computers commanded the aircraft to pitch down. At least 110 of the 303 passengers and 9 of the 12 crew members were injured.

The safety investigation identified several lessons concerning system safety assessments. Some have aspects in common with the HB-JFN incident.

The following paragraphs contain information from the results of the investigation and several other reference documents.

1.18.1.2 System safety assessment: PSSA/SSA

Conventional system safety analysis techniques mainly rely on fault trees assembled via PSSAs and SSAs. These methods were initially developed for hardware systems and are not well-suited to more complex systems with software elements.

To mitigate this problem, formal methods consist in creating a mathematical or logic model of the system, then using it to automatically complete tasks such as generating fault trees.

This type of method was used for the safety analysis of the Falcon 7X flight control system. It enables teams responsible for designing the system and conducting safety analysis to use the same view of the system and reduce the risk of misinterpretation and misunderstanding.

However, results depend on how well the model represents the system and environment in which it works. In addition, the type of failure rarely takes into account transient phenomena or the temporal aspect of a failure. It can also prove impossible to use all the results that are generated due to their sheer number.

Whatever the method, the interest of fault trees is generally to estimate the probability of a hazardous event. Most safety analysis errors result from the failure to foresee all the ways in which the hazard could occur, especially for complex and new systems.

[30] The final report is available on the ATSB site at: http://www.atsb.gov.au/publications/investigation_reports/2008/aair/ao-2008-070.aspx

[31] Air Data Inertial Reference Unit.

1.18.1.3 Equipment safety analysis: FMEA

FMEA is an analysis method that appeared in the 1940s and remains widely used in the industry. However it has the following limitations:

- it only takes into account known or foreseen failure modes of basic components;
- it only covers failures or failure condition for one component at a time and does not take into consideration more complex failures involving multiple components;
- it provides no assurance that all consequences of a given failure condition will be identified;
- the quality and completeness of an FMEA depends on the analyst's ability to understand and anticipate the equipment behaviour while it is still in development;
- this method is designed to assess failures in electrical or mechanical components. It is not well suited for complex software elements, particularly due to the fact that "*failure*" is a difficult concept to apply to software (or part of it).

1.18.1.4 Alternative methods

Other methods consider failures to be the result of a system's inadequate control of disturbances to its operation. These disturbances can be caused by component failures, dysfunctional interactions between system components or external disturbances.

These methods are currently used on a limited basis.

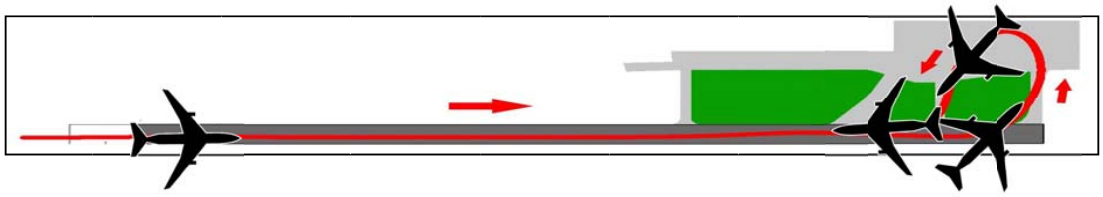
1.18.1.5 Human factors affecting safety analysis

An enormous amount of effort has been put into studying the human factors issues for crews, air traffic controllers and aircraft maintenance personnel. However the ATSB report found very little research that has examined the human factors issues affecting design engineers and safety analysts or the factors likely to lead to errors in design.

The ability to detect errors in design or judge whether a fault tree is complete can be affected by a range of different factors, such as experience, available knowledge, task complexity and the fact that omissions are relatively difficult to detect. The final result can also be affected by time-related pressure from the organisation's activity and industrial programme deadlines.

1.18.2 Alitalia-operated Airbus A321 accident, 9 April 2007

The crew was authorised to land in Naples (Italy) on runway 24 in calm wind conditions. The Captain decided to land using maximum reverse thrust without the use of automatic brakes due to the weight of the aeroplane and length of the runway. Upon touchdown, an alert sounded and a message appeared indicating failure of the automatic braking system even though the system had not been activated. The crew felt no significant deceleration and radioed control tower to report an emergency situation. Nearing the end of the runway, the Captain turned the aeroplane to the left using the nose gear steering. Sensing the direction of the aeroplane, the pilot of a helicopter in hover flight over a taxiway lifted off while another aeroplane stopped taxiing to avoid any risk of collision with the A321. The Captain then began a turn to the right and the aeroplane came to a stop on the landing runway, in the opposite direction.



The findings of the ANSV (Italian authority responsible for safety investigations) identified a soldering defect on one of the pins on a BSCU thermistor component, causing abnormal voltage variations and intermittent failure of the BSCU.

This accident is another example of the potential effects of a soldering defect. The investigation report does not mention anything about safety assessments.

1.18.3 Japan Airlines-operated Boeing 787-8 accident, 7 January 2013

While parked at Boston International Airport (USA), cleaning personnel discovered smoke in the aft cabin of the aeroplane. About the same time, a maintenance manager in the cockpit observed that the APU had automatically shut down. When the aft electronic equipment bay was opened, heavy smoke and flames were found coming from the lid of the APU battery case (same model as the Boeing 787 main batteries).

The NTSB identified an internal short-circuit that had caused an uncontrollable temperature and pressure increase in a single APU battery cell. This increase caused cascading thermal runaway within the battery, creating smoke and fire. The NTSB concluded that the accident resulted from the following:

- Boeing's failure to consider ways to mitigate the most severe effects of an internal short-circuit within an APU battery cell and
- the FAA's failure to identity the design defect during the certification process.

The following lessons concerning safety assessments were highlighted in the NTSB[32] investigation report:

- the failure condition in the APU battery at the time of the accident had not been identified by Boeing or its subcontractors during the Boeing 787 battery safety assessment process;
- the key assumption that cascading thermal runaway would not occur was not explicitly discussed or justified;
- a conservative approach considering that this assumption could be incorrect was not adopted, contrary to certification regulations;
- FAA reviews of safety assessments did not reveal the two abovementioned points.

[32] The final report can be found on the NTSB's website at the following link: http://www.ntsb.gov/investigations/AccidentReports/Reports/AIR1401.pdf

1.18.4 Pilot accounts

1.18.4.1 Captain

The Captain stated that at the time of the incident, the crew was busy preparing for descent and vertical modes to comply with air traffic control clearances. The cockpit was calm at the end of a nearly 12 hour flight and there were no notable meteorological phenomena.

When the attitude began to increase, the Captain wondered if the PF had commanded the movement. Seeing him making inputs on the sidestick, he realised that the PF was actually attempting to counter the movement. He states that he instinctively reached toward the central console, where the ''*TRIM EMERG*'' button is located on the Falcon 900. This button enables the pilot to take over manual control of the pitch trim. He also took the controls to see if he could regain control on his side, to no avail.

He stated that banking the aeroplane helped decrease its attitude as they tried to find a solution. He added that he had never received training to handle excessive pitch attitude.

In his opinion, the fact that there were no passengers made the job easier for the crew.

1.18.4.2 Co-pilot

The co-pilot stated that during descent, at approximately 12,500 ft, the aeroplane suddenly went nose-up and banked to the right without any precursor signs or CAS message. He explained that when the aeroplane reached an airspeed of approximately 130 kt, the *''INCREASE SPEED''* alarm was triggered. He attempted to counteract the nose-up pitch by making a full nose-down input on the sidestick. He stated that he banked the aeroplane fully to the right to reduce the angle of attack and that he pushed the throttle levers to increase speed. He indicated that during this phase, the Captain:

- tried to use the manual pitch trim;
- attempted to reengage the flight controls by pressing the "PFS ENGAGE" push-button on the upper panel;
- made inputs on the sidestick because the DUAL INPUT alarm was triggered. In reaction to the alarm, the co-pilot yelled at the Captain to stop using the sidestick.

According to the co-pilot, three messages appeared on the ENG-CAS window:

- FCS TRIM LIMIT;
- ALT MISCOMPARE;
- AFCS: ADS 3 MISCOMPARE

Not seeing any improvement in the situation, the co-pilot stated that he suggested that the Captain take over the controls to attempt to trim the aeroplane. The aeroplane went nose-up again, to a lesser extent than the first time, and reached an altitude of 24,000 ft. The subsequent decrease in airspeed once again triggered the INCREASE SPEED alarm. The Captain instructed the co-pilot to attempt to reengage the flight controls.

The co-pilot explained that when they recovered control of the aeroplane, the Captain decided to fly the aeroplane manually. During their approach, the crew notified the control tower at Subang airport of an emergency situation.

The French-speaking co-pilot indicated that the stressful situation generated by the uncommanded climb made it difficult for him to explain what was happening to the Captain, whose first language was English.

The co-pilot explained that he banked the aeroplane during the pitch trim runaway as a reflex and that his experience as a military pilot came in great use to him in responding to the situation. He stated that when the THS runaway occurred, the rapid increase in pitch attitude reminded him of a level toss bombing manoeuvre that he had used many times during fighter jet training. This manoeuvre consists in approaching a target in level flight, then raising the nose (approximately 5g and 30 degree pitch attitude) to release the bomb about 5 km from the target. The pilot must then bank the aircraft more than 90 degrees to decrease the attitude and leave the drop zone at a low altitude. During the manoeuvre, full thrust must be applied.

The co-pilot stated that he had never received any specific upset recovery training during his career as an airline pilot. He explained that upset situations can be covered during CRM training.

1.18.5 Recovery from unusual situations

1.18.5.1 Airplane Upset Recovery Training Aid

Many manufacturers, operators, training organisations and aviation authorities have worked together to create a training aid that provides techniques for recovering from upset situations[33].

To recover from this type of situation, pilots need to quickly understand the situation in order to respond appropriately.

[33] Airplane Upset Recovery, Training Aid, Revision 2, November 2008.

In a nose-high, wings-level upset, the manual advises the following:

- start by disengaging the autopilot and auto-throttle and recognize and confirm the situation;
- next, apply nose-down elevator to achieve a nose-down pitch rate. This may require as much as full nose-down input;
- if a sustained column force is required to obtain the desired response, carefully trim off some of the control force without using too much trim. Do not fly the aeroplane using pitch trim.

If at this point the pitch rate is not under control, there are several additional techniques that may be tried:

- pitch may be controlled by rolling the aeroplane to a bank angle that starts the nose down. Continuous nose-down elevator pressure will make the ailerons more effective. The angle of bank should not normally exceed 60 degrees. If airspeed decreases too much, full deflection of the ailerons and spoilers can be used;
- If altitude permits, it may be necessary to reduce thrust to prevent the angle of attack from continuing to increase for some aircraft with underwing-mounted engines;
- If control provided by the ailerons and spoilers is ineffective, rudder input by may be required to induce a rolling manoeuvre. Only a small amount of rudder input is needed to prevent loss of lateral control.

To complete the recovery, roll to wings level as the nose approaches the horizon. Recover to slightly nose-low attitude to reduce the potential for entering another upset. After checking airspeed, adjust thrust and pitch as necessary.

1.18.5.2 Aeroplane upset prevention and recovery training

In March 2014[(34)] the ICAO published a manual on upset prevention and recovery for civil aviation authorities, approved training organisations, airlines and their crews. Its purpose is to provide training methodologies to mitigate risks related to upset events by preparing crews to recognise, detect and avoid such occurrences, and training them to recover from them effectively. The guidelines are based on an analysis of accidents resulting from loss of control in flight. The manual's foreword indicates that between 2006 and 2011, aeroplane accidents resulting from loss of control were the leading cause of fatalities in commercial aviation.

[(34)] Unedited version that may still be modified.

The content of the manual is based on a training approach that combines:

- academic training;
- practical on-aeroplane training;
- flight simulation training device (FSTD) multi-crew training, at all stages of flight, and in representative conditions.

The manual also defines aeroplane upset as an aeroplane in flight unintentionally exceeding the parameters normally experienced in line operations or training:

- pitch attitude greater than 25 degrees nose-up, or
- pitch attitude greater than 10 degrees nose-down, or
- bank angle greater than 45 degrees, or
- within the above parameters but flying at airspeeds inappropriate for the conditions.

In March 2014, the FAA[35] modified the training criteria for airline pilots. The regulation stipulates that training programmes must comply with the changes no later than March 2019 to improve manually controlled flight in critical situations, including upset recovery.

[35] FAR 121.423

When the report was published, no other similar regulations were in existence for airlines in European Union member states. However in August 2013, EASA launched two Rulemaking Tasks (RMT[36].0581 and RMT.0582) titled Loss of Control Prevention and Recovery Training. The aim of these tasks is to develop regulations to ensure that pilots receive initial and recurring training on loss of control prevention and recovery. They integrate the latest ICAO publications and rely heavily on the international working group[37] initiatives and safety recommendations from investigation authorities

[36] RuleMaking Task.

[37] ICATEE (International Committee for Aviation Training in Extended Envelopes) and LOCART (Loss of Control Avoidance and Recovery Training).

1.18.6 Dual input events

The crew of the HB-JFN is not the only case of dual inputs. Several safety investigation reports state that despite the presence of visual, audio and, like on the Falcon 7X, tactile alerts (vibration in the sidestick), these types of actions[38] can still occur. They are mainly associated with situations where stress and surprise play a factor.

[38] Afriqiyah-operated A330 accident in Libya, May 2010, Air France-operated A320 incident in Israel, April 2012, etc.

They are also sometimes reported by the crew. The French Civil Aviation Authority (DGAC) database contains 145 dual input events between 2006 and 2013, none of which involve Falcon 7X aeroplanes. Most occurred intentionally during landing flare to correct inputs on the PF stick. Others took place during go-arounds, TCAS manoeuvres or turbulence.

In 2014, a new OSD[39] requirement was introduced, mandating that aircraft manufacturers submit certain data in order to improve the way in which specific design characteristics of each aircraft are taken into account in crew training and operation.

[39] Operational Suitability Data.

2 - ANALYSIS

2.1 Scenario

A soldering defect on an HSECU induction coil pin led this unit to generate incorrect pitch-up commands to the motor that controls the position of the THS and to transmit to its monitoring systems values indicating a nose-down variation. None of the aircraft systems detected these XXX erroneous values, resulting in deployment of the THS in full nose-up position during descent to Subang Airport.

The immediate effect of THS runaway was excessive pitch increase. The crew had no way of changing the position of the THS in normal law.

The reflex response and inputs of the PF were consistent with excessive pitch attitude recovery manoeuvres and stabilised the aeroplane despite the position of the THS. Maintaining a high bank angle helped stabilise the pitch attitude.

The Captain also made simultaneous roll inputs in the opposite direction to those of the PF twice, each time for approximately ten seconds. These simultaneous inputs decreased the bank, thus increasing the pitch attitude. The crew became aware of the dual inputs and handled the situation by taking over priority of the sidestick and transferring the controls.

Approximately two minutes after THS runaway occurred, the actuator control monitoring unit (ACMU) temperature monitoring function switched to a redundant control channel, which returned the THS to normal operation.

2.2 Hardware production

Micro-cracks on the induction coil solder caused THS runaway. This soldering defect stems from a manufacturing defect that was not detected during the HSECU manufacturing process. It was caused by insufficient thermal insulation between the plated through-hole and the rest of the circuit board.

The Alitalia-operated Airbus A321 accident in 2007 (see 1.18.2) is another example of the effects that result from a single soldering defect on the pin of a single component.

2.3 Safety analysis

2.3.1 Failure of a single component

The soldering defect on an L4 induction coil pin in the HSECU changed the impedance of the component, causing THS runaway (see 1.16.2). Uncommanded runaway of a primary control surface is considered as a failure that prevents safe flight and must therefore not occur as the result of the failure of a single element or component (see 1.17.1.3) or a as a result of a combination of extremely improbable failures.

The potential effects of a hardware component failure should be identified and detailed in the FMEA for the item in question. The HSECU FMEA identified a soldering defect on the L4 induction coil as a potentially latent failure. Its effects were not therefore considered as visible on the HSECU. Rockwell-Collins generally described the majority of failures as latent in its HSECU FMEA.

The imprecise assessment of the effects of component failures on the HSECU, and particularly the failure on the L4 induction coil, prevented the proper evaluation of these effects in the safety analysis.

2.3.2 FMEA limitations

The effects of a failure caused by a soldering defect on the L4 induction coil were poorly assessed in the HSECU FMEA. The effects of a fluctuating inductance value in the component were considered as "potentially" latent. However, they had significant effects on the behaviour of the HSECU, the flight control system and therefore the control of the aeroplane in flight.

FMEAs are tools that have long been used in aeronautical equipment design. They are prepared on the basis of technical standards (*see 1.17.1.5*) and the internal procedures of equipment manufacturers. However, the Qantas-operated Airbus A330 accident in Australia on 7 October 2008 (*see 1.18.1*) and this serious incident show that there are some limitations to the FMEA drafting, verification and validation process.

2.3.2.1 FMEA drafting process

In the case of the HSECU, it took three months of analysis to determine the effect of the failure of the L4 part on the behaviour of the THS control system. Following the incident, Rockwell-Collins completely updated the HSECU FMEA using the same methods and reference documents. The new FMEA has results that differ from the version in effect at the time of the serious incident (*see 1.17.3.4 and 1.17.3.5*). This shows the difficulty in estimating a priori the consequences of the failure of a part. Although the same procedures were used, the updated version shows that the results in this type of document vary and therefore present a degree of uncertainty, despite the fact that it acts as a basis for the system safety assessment process. Following the Qantas Airbus A330 accident in Australia on 7 October 2008, the ATSB also found that FMEAs did not systematically identify all the scenarios that could result in a given failure. Both these examples show that FMEAs have their limitations and prove that the system is not completely foolproof.

These limitations can be attributed to:

- Human factors such as dependency on analysts' experience, training and workloads;
- Organisational factors such as the human resources allotted to FMEA production or time-related pressure in the industrial development and certification process;
- Factors inherent to FMEAs, and particularly the fact that they only take into account known or anticipated failure modes, and do not cover failures involving several components. The FMEA process was developed in the late 1940s for the analysis of simple electrical or mechanical equipment and are at times poorly suited to analysing complex equipment, particularly with computers.

2.3.2.2 FMEA verification and validation

For type certification, design organisations have to detail the methods to be used to determine the acceptability of equipment designed by sub-contractors and the tasks performed by the latter. Thus, Dassault Aviation did not carry out an exhaustive re-check on the HSECU FMEA in order to compare with that of Rockwell Collins but carried out a general checks of these results based on the information at its disposal. Furthermore, EASA does not verify the content of FMEAs as they are not included in the documents requiring approval. In general, neither the design organisation nor EASA have the resources or technical expertise required to perform an in-depth verification and validation of the FMEAs for all of the equipment present on an aircraft. Consequently, only equipment manufacturers are able to check in detail and validate the results of the FMEA.

Consequently, the results of FMEAs can depend entirely on the internal procedures set up by equipment manufacturers, even where critical equipment for which a design error or unexpected malfunction could result in a catastrophic aeroplane failure. Thus, for the Falcon 7X HSECU, identified as critical equipment, the FMEA development, the check and validation process relied entirely on the experience of three people at Rockwell-Collins.

In this context, errors in the FMEA can result in safety assessments that show compliance with certification requirements even though they are erroneous. These *"latent"* design errors can have direct consequences on the operation of aircraft since they have a direct impact on system safety, operational and maintenance procedures, and crew and aircraft maintenance personnel training, potentially resulting in direct consequences on aircraft operation. This incident and the accident in Australia (*see 1.18.1.1*) both illustrate what can happen as a result of these latent errors.

2.3.3 Limitations of SSA and monitoring functions

The system safety assessment (SSA) of the primary flight control system conducted by Dassault Aviation took into account the results of the HSECU FMEA 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.

Uncommanded THS runaway in normal law does appear in the safety assessment summary report but not in the documents containing more detailed failure mode results (Book 1 and Book 2, *see 1.17.2.2*). This was not challenged by either Dassault Aviation or EASA, which approved the flight control system SSA.

The SSA results for the primary flight control system affected the development of the monitoring functions associated with the THS control system. Therefore, at the time of the incident, the THS control system had been designed so that the monitoring function of the ACMU depended entirely on the horizontal stabilizer electronic control unit (HSECU) to detect THS runaway caused by 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 enabled a simple failure to cause THS runaway, considered as catastrophic. This type of architecture nevertheless meets regulatory requirements, which do not explicitly require independence between monitoring and control channels. However the entire THS control channel is considered as a critical system because it carries numerous catastrophic failure modes such as uncommanded runaway of a primary control surface.

The highest design assurance level (DAL A) was assigned to THS ACMU modules and the HSECU. The highest verification and validation levels were therefore supposed to be in place throughout the design and safety analysis process. However they failed to identify the HSECU critical failure modes and did not anticipate THS runaway in normal law.

This serious incident therefore revealed that for a complex system like the primary flight control system, the safety assessment process is vulnerable to errors or problems that can arise at various stages of the process:

- development and validation of equipment FMEAs by an equipment manufacturer;
- design organisation's capability of managing and supervising design when equipment (especially critical equipment) is designed by partners or subcontractors;
- validation of an SSA by a design organisation;
- approval by the certification authority.

The accidents in Australia (*see 1.18.1.1*) and the United States (*see 1.18.3*) confirm that safety assessment processes cannot anticipate failure conditions with potentially catastrophic effects that are not identified during the design phase, especially for complex systems or new technologies.

2.4 Aeroplane upset recovery

Crews are rarely exposed to upset situations, whether in training or operation. To recover from aeroplane upset, pilots must be capable of quickly identifying and using the appropriate recovery techniques. In this instance, the co-pilot's previous experience in the French Air Force was decisive in temporarily recovering control of the aeroplane when its pitch attitude increased significantly following THS runaway in normal law. His reflex reaction was developed by repeating similar manoeuvres to increase pitch attitude on fighter jets. Furthermore, the operational technique described in Dassault Aviation documentation in effect at the time of the event was not well-suited when the auto-trim function was available and active.

The ICAO manual findings on loss of control and aeroplane upset situations (*see 1.18.4.2*) show that the co-pilot had the right reaction to the increase in pitch attitude although it is not common for airline pilots. In general, this assessment and currently insufficient content in pilot training fail to ensure that the skills required to recover from aeroplane upset are acquired and maintained. Providing crews with training on aeroplane upset recovery is being explored by organisations such as the OACI, EASA, and FAA, which agree that it is an initiative worth pursuing.

2.5 Dual inputs

The THS runaway generated two occurrences of dual inputs in less than three minutes, each lasting approximately ten seconds. These situations can be attributed to the surprise and stress caused by:

- the sudden and serious nature of the disturbance generated by the THS runaway;
- incomprehension of the situation, especially during the THS runaway phase;
- the crew's lack of exposure to the situation in training or operation;
- both pilots' lack of experience on aeroplanes with sidesticks.

The absence of audio recordings of the event prevented investigators from properly analysing how the crew handled these two instances of dual inputs. However, parameter analysis and crew accounts provided the following information:

- the way the crew handled the two dual input phases enabled one of the pilots to regain control within seven to eleven seconds;
- The dual input visual, tactile, and sidestick priority control alerts enabled the crew to manage both dual input phases. These alerts therefore enabled the crew to identify the dual input phases and act appropriately.

Simultaneous inputs on aeroplanes with sidesticks are not isolated events. Aeroplanes equipped with sidesticks are ergonomically designed to enable pilots to handle dual input situations (sidestick vibration, audio and visual alerts). However this incident highlights the lack of training that crews receive in this area. It is of particular note that the scenario used in type training (incapacitated pilot) is not representative of commonly encountered dual input situations. (see 1.17.2.6 and 1.18.5).

3 - CONCLUSION

3.1 Findings

- the serious incident occurred during a repositioning flight;
- The crew had the licences and qualifications required for flight;
- the aircraft had a valid airworthiness certificate. It had received regular maintenance in accordance with regulations;
- the aircraft weight and balance were within operational limits;
- the aircraft had taken off from Nuremberg without any known technical problems;
- a pin in an HSECU component had a soldering defect;
- this soldering defect was not detected during manufacture of the HSECU;
- during descent to the destination aerodrome, at an altitude of approximately 13,000 ft, the THS went from level to full nose-up position in fifteen seconds;
- the PF took over the controls and made full nose-down inputs;
- when the PF nose-down inputs proved ineffective, he performed a recovery manoeuvre by banking the aeroplane rightwards, initially to a 98° angle;
- the PF had performed this type of manoeuvre many times during his military career;
- this manoeuvre changed the nose-up pitch into a bank, enabling the PF to temporarily regain pitch control despite the THS being in full nose-up position, then trim the aeroplane and stabilise the airspeed;
- the THS actuator control monitoring unit triggered the change in THS control channel and the aeroplane pitch could once again be controlled via the sidestick;
- 2 minutes and 36 seconds went by between the moment when the THS nose-up movement began and its return to level position. During this time, the load factor reached 4.6g. The aircraft altitude went from 13,000 to 22,500 ft. The calibrated airspeed went from 300 to 125 kts. The pitch attitude angle reached 41 degrees;
- during the event the crew made dual inputs at two different times, for nine and twelve seconds respectively;
- these dual input phases were managed via visual, audio, and tactile alerts, and sidestick priority management systems;
- no significant events had occurred before the THS runaway;
- the effects of a failure caused by a soldering defect on the L4 induction coil were poorly assessed in the HSECU FMEA;
- the FMEA verification and validation processes used by the equipment and aeroplane manufacturers failed to detect the mistake;
- the highest design assurance level (DAL A) was assigned to THS ACMU modules and the HSECU;
- FMEAs were not among the documents requiring EASA approval during type certification of the Falcon 7X;
- the architecture of the THS control system was such that the control channel and HSECU monitoring function performed by the ACMU depended on parameters generated by the HSECU, which controls the THS.

3.2 Causes of the serious incident

A soldering defect on the pin of an HSECU component caused the unit to generate incorrect nose-up commands to the motor controlling the THS and to transmit to systems in charge of the monitoring of its functioning values indicating a change in the opposite direction to that in which the motor was actually moving. This single defect caused simultaneous failures on the THS control and monitoring channels that were not detected by any of the aircraft systems and were enough to cause THS runaway under normal law.

The following factors played a role:

- a manufacturing defect that was not detected before the HSECU was put into service;
- the imprecise assessment of the effects of the failure types identified in the HSECU FMEA, validation of the FMEA and in general, the varying results of FMEAs, which can depend on human factors and equipment manufacturer organisational factors;
- the lack of mechanisms for detecting potential critical errors in equipment manufacturer FMEAs during the aeroplane safety assessment and certification process. Neither the aeroplane manufacturer nor EASA conducted an in-depth verification of the FMEA;
- the limitations in the aeroplane manufacturer's SSA process during the verification and approval process by EASA despite the fact that the summary of the SSA mentioned THS runaway in normal law. However the detailed results did not include any combinations of failures that could cause the runaway and the HSECU was identified as critical equipment in which a malfunction or error in design can result in a catastrophic situation;
- for the event in question, the architecture of the THS control system had interdependent monitoring and control channels that prevented the HSECU malfunction from being detected and reconfiguration to a redundant control channel.

This event thus brought to light inadequate provisions intended to meet the regulatory certification requirement stipulating that the single failure of a component, system or appliance in flight must not cause runaway of a primary flight control to an unwanted position

There are no specific procedures or crew training for THS runaway in normal law, which in this case occurred in a sudden and considerable manner. Despite their surprise, the crew managed to recover and maintain control of the aircraft with the THS in full nose-up position:

- by immediately applying and adapting an excessive pitch attitude recovery technique attributed to training which the PF received during his military career;
- Through coordination between the two crew members, which enabled them to perform their assigned tasks effectively until the return to normal fight conditions despite simultaneous inputs on their sidesticks at two different times.

The tripping of a temperature monitoring function two to three minutes after THS runaway began enabled to switch to another control channel, and by getting pitch level back, to recover aircraft controllability till the end of the flight.

4 - SAFETY RECOMMENDATIONS

4.1 Additional Methods for FMEA

The investigation tends to show that the means required to detect errors that may be included in Failure Mode, Effects and criticality (FMEA) are inadequate, specifically when this relates to equipment that is considered as critical. This finding is also based on other accidents. It also shows the limits of FMEA which, though well adapted to simple systems and to material malfunctions for which it was designed some decades ago, seems to be less effective for electronic equipment or software.

This is why the BEA recommends that:

- **EASA, in coordination with FAA, SAE and EUROCAE[40], evaluate and propose alternative or additional methods to the FMEA for electronic equipment and software. [Recommendation 2016-002]**

- **FAA, in coordination with EASA, SAE and EUROCAE, evaluate and propose alternative or additional methods to the FMEA for electronic equipment and software. [Recommandation 2016-003]**

[40] Acronym of the EURopean Organisation for Civil Aviation Equipment, a European organisation that defines rules for the standardisation of systems used in civil aviation.

4.2 Independence between control and monitoring systems

Independence between control and monitoring systems, as well as checks on this independence, constitute key elements in the safety of a system. They are not explicitly required by certification specifications. Some errors that may exist in safety analyses are difficult or even impossible to detect based on the available technical standards, whether during checking and validation by the design organisation or during approval by the authorities responsible for certification. In the case of this serious incident, a simple brazing error led to undetected failures on both of the systems and thus to the runaway of a primary flight control surface to an undesirable position. This is why the BEA recommends that:

- **EASA, in coordination with FAA, SAE and EUROCAE, develop means or methods that make it possible to consolidate, during safety analyses, checks on the independence of system control and the monitoring of said system. [Recommandation 2016-004]**

- **FAA, in coordination with EASA, SAE and EUROCAE, develop means or methods that make it possible to consolidate, during safety analyses, checks on the independence of system control and the monitoring of said system. [Recommandation 2016-005]**

4.3 Training relating to taking over control of aeroplanes equipped with non-coupled control sticks

The investigation showed that training relating to taking over control of aeroplanes equipped with non-coupled control sticks, as it is undertaken at the moment during initial and recurrent training, does not guarantee continuing crew competence in this area. It thus seems to be required, in the context of OSD, to take into account the specific procedures relating to taking over control of aeroplanes equipped with non-coupled control sticks.

This finding was also made during the investigation into the accident that occurred on 29 March 2013 at Lyon-Saint Exupéry (France) to the Airbus A321 registered SX-BHS operated by Hermes Airlines and chartered by Air Méditerranée[41] and for which the BEA recommended that:

- ***EASA, in coordination with manufacturers, ensure that future training programmes defined in the context of OSD include initial and recurrent training relating to taking over control of aeroplanes equipped with non-coupled control sticks. [Recommandation 2015-024]***

[41] https://www.bea.aero/fileadmin/documents/docspa/2013/sx-s130329.en/pdf/sx-s130329.en.pdf

5 - MEASURES TAKEN SINCE THE INCIDENT

Following the incident, the equipment and aircraft manufacturers implemented a number of safety measures.

5.1 Measures taken by Rockwell-Collins

■ Safety assessment

Following the incident, the FMEA[42] was amended using the same method and reference documents. In the new version, the failure effects for each component or function of the HSECU are described in more detail. The following information is specifically included for the induction coil with the defective solder (the differences with Version C of the FMEA are indicated in red):

[42] Version D of November 2011.

Failure type	Cause of failure	Local effect (for the component)	Overall effect	Failure detection method (A: crew; B: on the ground)
Short circuit	Component damaged, equipment damaged, eroded	-15VDC fixed at 0 V	Runaway motor in overspeed AND inaccurate speed signal sent to the ACMU (fixed at 0).	A: Uncommanded movement of the actuator, detectable via external position sensors B: "vendor test/evaluate; ATP box"
Open circuit	Component damaged, equipment damaged, eroded	Loss of -15 VDC power supply	Runaway motor in overspeed AND inaccurate speed signal sent to the ACMU (fixed at 0) AND Overcurrent output fixed at low value (no fault).	A: Uncommanded movement of the actuator, detectable via external position sensors B: "vendor test/evaluate; ATP box"
Fluctuating value	ageing	The worst case scenario is additional impedance at the L4 terminals causing the voltage (-15) to rise above 0V (demonstrated under test conditions)	Runaway motor in overspeed AND inaccurate speed signal sent to the ACMU (not fixed at 0) AND Overcurrent output fixed at low value (no fault).	A: Uncommanded movement of the actuator, detectable via external position sensors B: "vendor test/evaluate; ATP box"

Rockwell-Collins amended the HSECU FMEA. In the new version, no failures are considered as latent and thirty-one different failure conditions are identified (in the version in effect at the time of the incident, only a switch of the control channel was considered).

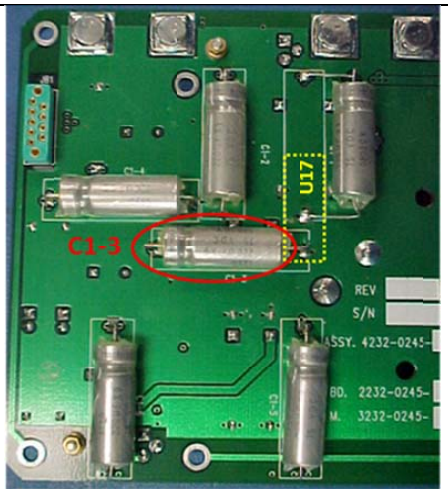
■ Production checks:

Rockwell-Collins has added X-ray examinations of circuit boards to the HSECU manufacturing process to detect any cold solder joints after the component soldering step.

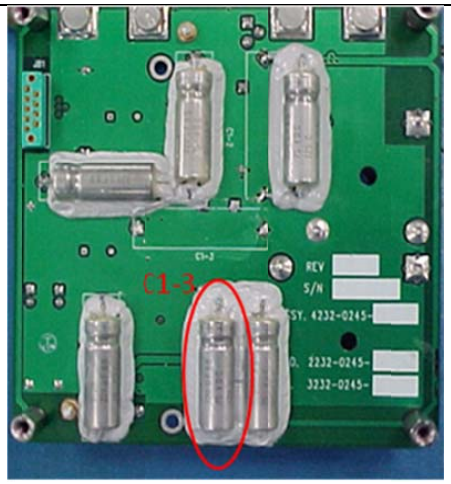
■ Change to circuit board design

During investigations into the cause of the failure, the HSECU circuit boards were examined and two components on adjacent circuit boards were found to be in physical contact with each other.

This defect was only present on HSECU model 051244-04. Even though it did not contribute to the incident, Rockwell-Collins developed a new version of the HSECU (051244-05) in which one of the two components was moved:



HSECU P/N 051244-04 (ancien modèle)



HSECU P/N 051244-05 (nouveau modèle)

Source Dassault Aviation

At the request of Dassault Aviation, Rockwell-Collins also:

- ❒ added insulation to the plated through-hole on the circuit board to help increase the temperature when the L4 induction coil is soldered;
- ❒ added HSECU internal supply voltage monitoring so that if any voltage outside tolerances are delivered, the ACMU disables the control channel and switches to a redundant channel.

5.2 Measures taken by Dassault-Aviation

Following the event, when the cause of the problem was still unknown, Dassault Aviation immediately asked EASA to temporarily ground all flights for the Falcon 7X fleet by issuing an Airworthiness Directive.

Dassault Aviation then took the following actions to gradually return the fleet to service:

Design and certification

As the cause of pitch trim runaway was not known, the first modifications consisted in:

Mod 1236[43]: introducing an additional monitoring function (performed by the flight control system, independent of the HSECU) that no longer uses THS motor rotation speed data;

[43] 16 June 2011.

Mod 1235[44]: installing a push-button in the cockpit to enable pilots to force the flight control system to switch over to the BACK-UP system (see Pitch trim system operation) and manually control the pitch trim.

[44] 16 June 2011.

Mod 1239[45]: eliminating potential mechanical interferences between HSECU components.

[45] 07 June 2011.

Once modifications 1235 and 1236 were implemented and the HSECU on every aeroplane had been checked, the fleet was able to return to service with a restricted flight envelope (maximum operating limit speed) due to the time required for the new monitoring function to trip.

A modification (mod 1245[46]) was then implemented to enable all flights to use the full flight envelope. It includes software changes to improve monitoring, particularly by introducing THS speed monitoring and to improve HSTS reversal logic to achieve quicker detection of pitch trim runaway.

[46] 29 August 2011.

EASA supervised and approved each of these steps via Airworthiness Directives.

Dassault Aviation also reviewed the safety assessments of flight control systems, taking into account the HSECU FMEA update.

Operation

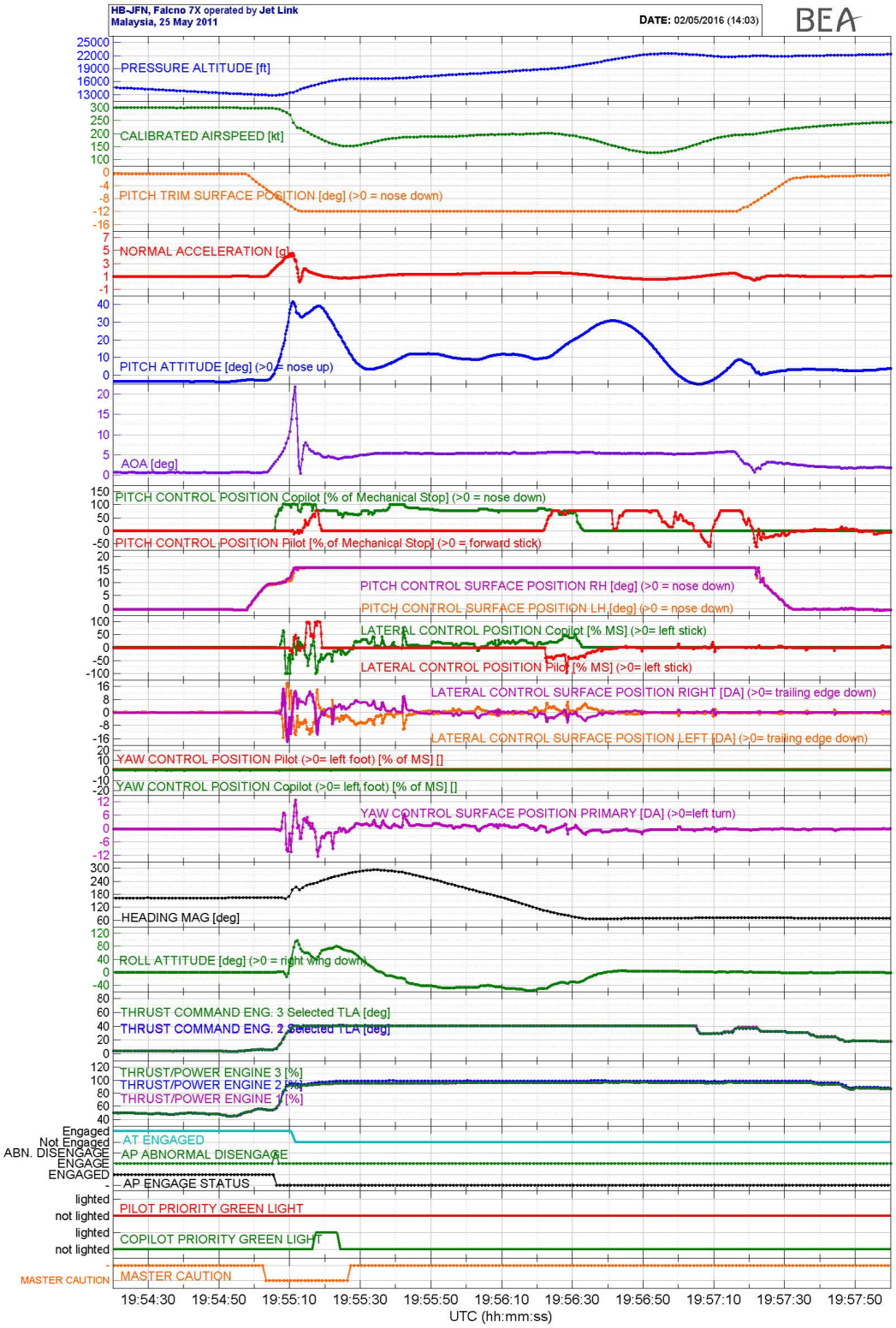
Flight permits with limitations were issued so that the Falcon 7X fleet could gradually return to service based on the abovementioned modifications. Airlines and operators were informed via forums, newsletters and a training module for pilots.

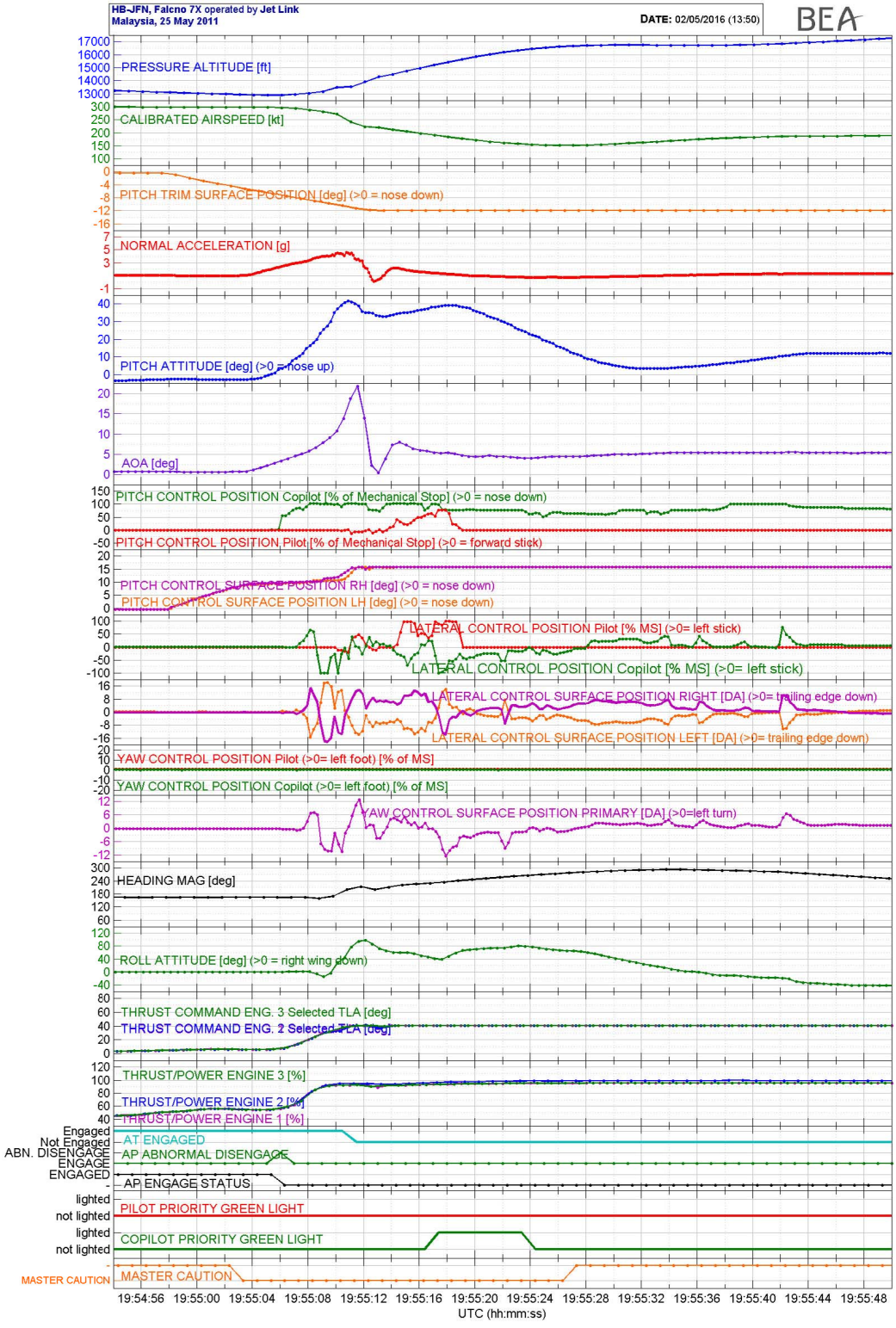
Flight and maintenance manuals were updated and training centres received the necessary information related to documents and modifications to be applied for flight simulators.

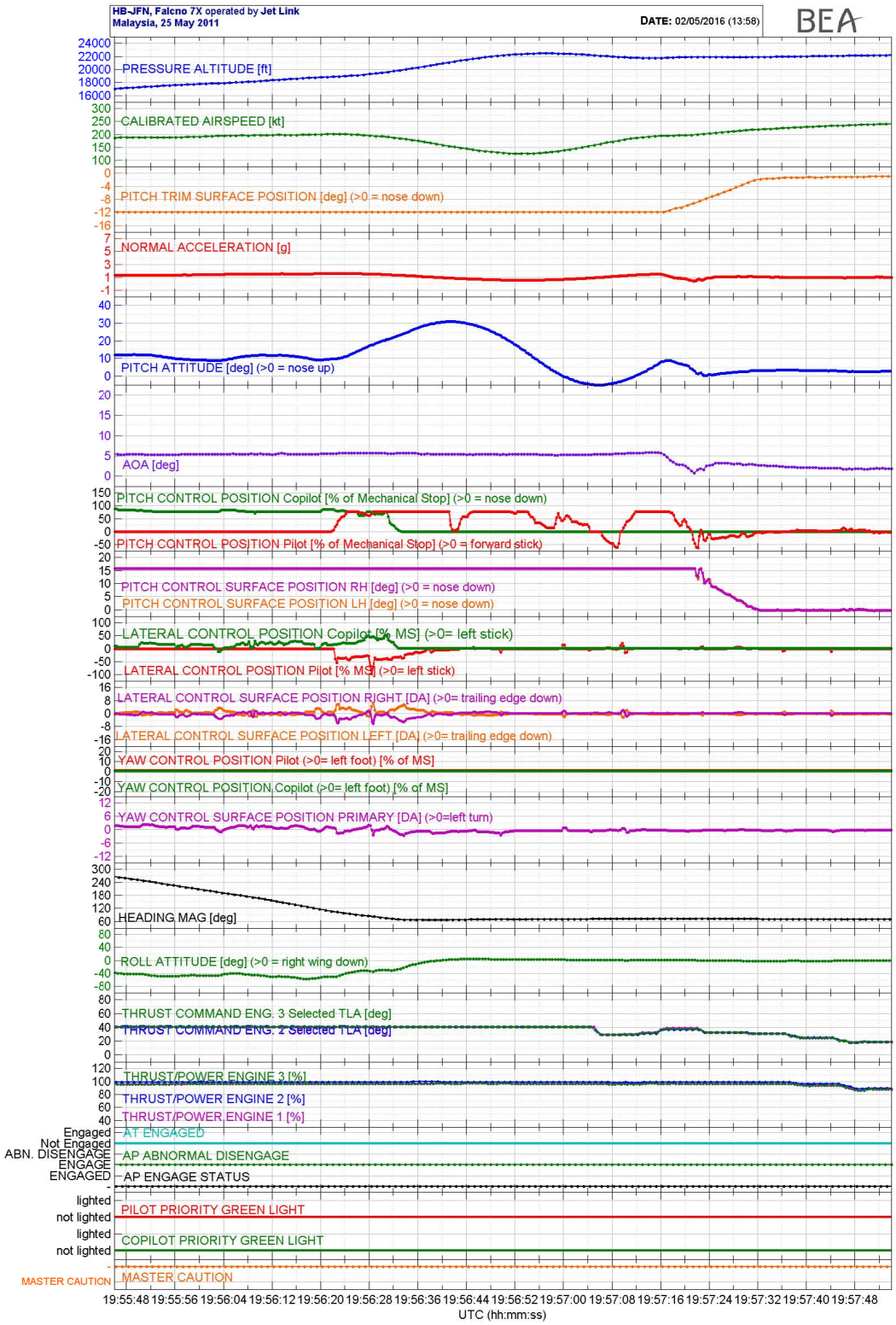
LIST OF APPENDICES

Appendix 1

FDR parameters




HB-JFN, Falcno 7X operated by Jet Link
Malaysia, 25 May 2011
DATE: 02/05/2016 (13:50)
BEA
PRESSURE ALTITUDE [ft]
CALIBRATED AIRSPEED [kt]
PITCH TRIM SURFACE POSITION [deg] (>0 = nose down)
NORMAL ACCELERATION [g]
PITCH ATTITUDE [deg] (>0 = nose up)
AOA [deg]
PITCH CONTROL POSITION Copilot [% of Mechanical Stop] (>0 = nose down)
PITCH CONTROL POSITION Pilot [% of Mechanical Stop] (>0 = forward stick)
PITCH CONTROL SURFACE POSITION RH [deg] (>0 = nose down)
PITCH CONTROL SURFACE POSITION LH [deg] (>0 = nose down)
LATERAL CONTROL POSITION Pilot [% MS] (>0= left stick)
LATERAL CONTROL POSITION Copilot [% MS] (>0= left stick)
LATERAL CONTROL SURFACE POSITION RIGHT [DA] (>0= trailing edge down)
LATERAL CONTROL SURFACE POSITION LEFT [DA] (>0= trailing edge down)
YAW CONTROL POSITION Pilot (>0= left foot) [% of MS]
YAW CONTROL POSITION Copilot (>0= left foot) [% of MS]
YAW CONTROL SURFACE POSITION PRIMARY [DA] (>0=left turn)
HEADING MAG [deg]
ROLL ATTITUDE [deg] (>0 = right wing down)
THRUST COMMAND ENG. 3 Selected TLA [deg]
THRUST COMMAND ENG. 2 Selected TLA [deg]
THRUST/POWER ENGINE 3 [%]
THRUST/POWER ENGINE 2 [%]
THRUST/POWER ENGINE 1 [%]
Engaged
Not Engaged
ABN. DISENGAGE
ENGAGE
ENGAGED
AT ENGAGED
AP ABNORMAL DISENGAGE
AP ENGAGE STATUS
lighted
not lighted
PILOT PRIORITY GREEN LIGHT
lighted
not lighted
COPILOT PRIORITY GREEN LIGHT
MASTER CAUTION
MASTER CAUTION
19:54:56 19:55:00 19:55:04 19:55:08 19:55:12 19:55:16 19:55:20 19:55:24 19:55:28 19:55:32 19:55:36 19:55:40 19:55:44 19:55:48
UTC (hh:mm:ss)


HB-JFN, Falcno 7X operated by Jet Link
Malaysia, 25 May 2011
DATE: 02/05/2016 (13:58)
BEA
PRESSURE ALTITUDE [ft]
CALIBRATED AIRSPEED [kt]
PITCH TRIM SURFACE POSITION [deg] (>0 = nose down)
NORMAL ACCELERATION [g]
PITCH ATTITUDE [deg] (>0 = nose up)
AOA [deg]
PITCH CONTROL POSITION Copilot [% of Mechanical Stop] (>0 = nose down)
PITCH CONTROL POSITION Pilot [% of Mechanical Stop] (>0 = forward stick)
PITCH CONTROL SURFACE POSITION RH [deg] (>0 = nose down)
PITCH CONTROL SURFACE POSITION LH [deg] (>0 = nose down)
LATERAL CONTROL POSITION Copilot [% MS] (>0= left stick)
LATERAL CONTROL POSITION Pilot [% MS] (>0= left stick)
LATERAL CONTROL SURFACE POSITION RIGHT [DA] (>0= trailing edge down)
LATERAL CONTROL SURFACE POSITION LEFT [DA] (>0= trailing edge down)
YAW CONTROL POSITION Pilot (>0= left foot) [% of MS]
YAW CONTROL POSITION Copilot (>0= left foot) [% of MS]
YAW CONTROL SURFACE POSITION PRIMARY [DA] (>0=left turn)
HEADING MAG [deg]
ROLL ATTITUDE [deg] (>0 = right wing down)
THRUST COMMAND ENG. 3 Selected TLA [deg]
THRUST COMMAND ENG. 2 Selected TLA [deg]
THRUST/POWER ENGINE 3 [%]
THRUST/POWER ENGINE 2 [%]
THRUST/POWER ENGINE 1 [%]
Engaged
Not Engaged
AT ENGAGED
ABN. DISENGAGE
ENGAGE
ENGAGED
AP ABNORMAL DISENGAGE
AP ENGAGE STATUS
lighted
not lighted
PILOT PRIORITY GREEN LIGHT
lighted
not lighted
COPILOT PRIORITY GREEN LIGHT
MASTER CAUTION
MASTER CAUTION
19:55:48 19:55:56 19:56:04 19:56:12 19:56:20 19:56:28 19:56:36 19:56:44 19:56:52 19:57:00 19:57:08 19:57:16 19:57:24 19:57:32 19:57:40 19:57:48
UTC (hh:mm:ss)

PITCH TRIM RUNAWAY

Unwanted pitch effect

- Counteract using side stick and the manual pitch trim. ➔**(1)**
- Crew must apply continuous pressure on side stick as airplane is not autotrimmed.

TASKS AND CALL OUT

TASK ALLOCATION			CALL – OUT	
PF	PNF	Emergency situation identified	PF PNF	TRIM RUNAWAY
PF		Counteract unwanted pitch effect using side stick and manual trim control **(1)**		

TECHNICAL EXPLANATIONS

Triggering event

This failure concerns manual trim only while it is being used.

Objectives of the Operating Technique

Counteract unwanted pitch effect due to pitch trim runaway.

Expanded explanation

➔ **(1) Counteract pitch effect**

The crew must apply continuous pressure on sidestick if airplane is not auto-trimmed.
If in Normal or Alternate laws, the PNF can attempt reconnecting the AP upon PF request.

BEA

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

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE