Parution : Février 2016

Rapport

Incident grave survenu le **24 mai 2011**
en descente vers l'aéroport de Subang (Malaisie)
à l'avion Dassault Falcon 7X
immatriculé **HB-JFN**
exploité par **Jet Link AG**

BEA

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

Ministère de l'Ecologie, du Développement durable et de l'Energie

Les enquêtes de sécurité

Le BEA est l'autorité française d'enquêtes de sécurité de l'aviation civile. Ses enquêtes ont pour unique objectif l'amélioration de la sécurité aérienne et ne visent nullement la détermination des fautes ou responsabilités.

Les enquêtes du BEA sont indépendantes, distinctes et sans préjudice de toute action judiciaire ou administrative visant à déterminer des fautes ou des responsabilités.

Table des matières

LES ENQUÊTES DE SÉCURITÉ 2

GLOSSAIRE 5

SYNOPSIS 7

1 - RENSEIGNEMENTS DE BASE 8

1.1 Déroulement du vol 8

1.2 Tués et blessés 9

1.3 Dommages à l'aéronef 9

1.4 Autres dommages 10

1.5 Renseignements sur le personnel 10

1.5.1 Commandant de bord 10

1.5.2 Copilote 10

1.6 Renseignements sur l'aéronef 11

1.6.1 Cellule 11

1.6.2 Moteurs 11

1.6.3 Masse et centrage 12

1.6.4 Entretien 12

1.6.5 Instruments de bord 12

1.6.6 Système de compensation de profondeur 15

1.6.7 Pilote automatique (PA) 17

1.7 Renseignements météorologiques 18

1.8 Aides à la navigation 18

1.9 Télécommunications 18

1.10 Renseignements sur l'aérodrome 18

1.11 Enregistreurs de bord 18

1.12 Renseignements sur l'épave et sur l'impact 18

1.13 Renseignements médicaux et pathologiques 18

1.14 Incendie 18

1.15 Questions relatives à la survie des occupants 18

1.16 Essais et recherches 19

1.16.1 Examens du HSECU 19

1.16.2 Origine du déroulement non commandé du compensateur de profondeur 20

1.16.3 Origine du défaut de brasure 21

1.17 Renseignements sur les organismes et la gestion 21
1.17.1 Renseignements sur l'AESA et la certification de type 21
1.17.2 Renseignements sur Dassault Aviation 25
1.17.3 Renseignements sur Rockwell-Collins 29
1.18 Renseignements supplémentaires 33
1.18.1 Méthodes d'analyse de sécurité 33
1.18.2 Accident survenu le 9 avril 2007 à un Airbus A321 exploité par Alitalia 35
1.18.3 Accident survenu le 7 janvier 2013 à un Boeing 787-8 exploité par Japan Airlines 35
1.18.4 Témoignages des pilotes 36
1.18.5 Récupération de situations inusuelles 37
1.18.6 Evénements avec actions simultanées de pilotage 39

2 - ANALYSE 40

2.1 Scénario 40
2.2 Production des équipements 40
2.3 Analyses de sécurité 40
2.3.1 Défaillance d'un seul composant 40
2.3.2 Limites dans l'élaboration des FMEA 41
2.3.3 Limites des SSA et surveillances mises en jeu 43
2.4 Récupération aux situations inusuelles 44
2.5 Actions simultanées de pilotage 44

3 - CONCLUSION 45

3.1 Faits établis par l'enquête 45
3.2 Causes de l'incident grave 46

4 - RECOMMANDATIONS DE SECURITE 48

4.1 Méthodes complémentaires aux FMEA 48
4.2 Indépendance entre chaînes de commande et de surveillance 48
4.3 Entraînement à la prise de priorité sur avions équipés de manches non conjugués mécaniquement 49

5 - MESURES PRISES DEPUIS L'ÉVÉNEMENT 49

5.1 Mesures prises par Rockwell-Collins 49
5.2 Mesures prises par Dassault-Aviation 51

Glossaire

ACMU	*Actuator Control Monitoring Unit*
ADIRU	*Air Data Inertial Reference Unit*
AESA	Agence Européenne de la Sécurité Aérienne
ADI	*Attitude Director Indicator*
AMJ	*Advisory Material Joint*
ANSV	*Agenzia Nazionale per la Sicurezza del Volo*
APU	*Auxiliary Power Unit*
ATPL(A)	Licence de pilote de ligne *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	Gestion des ressources en équipe *Crew Resource Management*
CS	*Certification specifications*
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* Niveau de vol
FMEA/AMDEC	*Failure Modes and Effect Analysis* Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité
Ft	*Feet* Pieds
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*
ICATEE	*International Committee for Aviation Training in Extended Envelopes*
IPT	*Integrated Procedures Trainer*
JAR	*Joint Aviation Requirements*
Kg	kilogramme
Kt	*Knot* Nœuds
lbs	*Pound*
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* Liste Minimale d'Equipements
MFCC	*Main Flight Control Computer*
MMEL	Liste minimale d'équipements de référence *Master Minimum Equipment List*
NTSB	*National Transportation Safety Board*
OACI	Organisation de l'Aviation Civile Internationale
OCAS	Outil de conception assistée de spécification et d'analyse de système
PA	Pilote Automatique
PDU	*Primary Display Unit*
PF	*Pilot Flying*
PNC	Personnel Navigant Commercial
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* Système d'Alerte de trafic et d'évitement des collisions
THS	*Tail Horizontal Stabilizer*
TOGA	*Take Off / Go Around*
VMC	Conditions météorologiques de vol à vue *Visual Meteorological Conditions*

Synopsis

Déroulement intempestif du stabilisateur horizontal en loi normale, pendant la descente

Aéronef	Avion Dassault Falcon 7X immatriculé HB-JFN
Date et heure	24 mai 2011 vers 19 h 55[1]
Exploitant	Jet Link AG
Lieu	Espace aérien malais, en descente vers l'aéroport de Subang (Malaisie)
Nature du vol	Transport public, vol non commercial de mise en place
Personnes à bord	Commandant de bord (PNF), copilote (PF), un PNC
Conséquences et dommages	Aucun

[1] Sauf précision contraire, les heures figurant dans ce rapport sont exprimées en temps universel coordonné (UTC).

ORGANISATION DE L'ENQUETE

L'incident grave s'est produit dans l'espace aérien de la Malaisie. Le BEA a informé les autorités de l'aviation civile malaisiennes. Celles-ci lui ont alors délégué l'enquête.

En application des dispositions de l'Annexe 13 de l'OACI, des représentants accrédités et des conseillers de la Suisse (Etat d'immatriculation et d'exploitation de l'avion), des Etats-Unis (Etat de construction de l'équipement HSECU) et de la Malaisie (Etat d'occurrence) ont été associés à l'enquête.

Celle-ci a duré plus de quatre ans durant lesquels la détermination précise des circonstances et la récupération d'informations auprès de l'équipementier Rockwell-Collins se sont avérées difficiles. En particulier, des délais de réponses, pouvant atteindre plusieurs mois ont pu être observés. Ils ont été justifiés par le fait que l'enquête du BEA porte sur des facteurs organisationnels pouvant être à l'origine de l'incident grave et que les éléments de réponses nécessitaient du temps pour être récupérés.

1 - RENSEIGNEMENTS DE BASE

1.1 Déroulement du vol

Note : les éléments suivants sont issus de données extraites de l'enregistreur de paramètres (FDR) et des témoignages de l'équipage.

Le 24 mai 2011 à 08 h 10, l'équipage du Falcon 7X immatriculé HB-JFN décolle de Nuremberg (Allemagne) à destination de Kuala Lumpur (aéroport de Subang) pour un vol de mise en place. Le copilote est aux commandes (PF).

Pendant la descente, le pilote automatique (PA) et l'automanette sont engagés et la vitesse conventionnelle est de 300 kt. Vers 19 h 55, le PF décide de réduire le taux de descente à l'approche de l'altitude autorisée (11 000 ft). Il sélectionne une vitesse verticale de 1 300 ft/min et active le mode vertical VS[2]. Quelques secondes plus tard, alors que l'avion passe 13 000 ft, le plan horizontal réglable, THS[3], passe en quinze secondes d'une position neutre à sa butée à cabrer (12 degrés).

Le PA reste engagé pendant les huit premières secondes du déroulement du THS. Les lois de commandes de vol contrent le mouvement à cabrer du THS par une action à piquer des gouvernes de profondeur qui atteignent deux tiers environ de leur débattement maximal deux secondes avant la déconnexion du PA[4]. Le THS continue son mouvement à cabrer. L'assiette longitudinale de l'avion et le facteur de charge augmentent.

Le PF applique des actions en butée à piquer au mini-manche et place les manettes de poussée en position Take Off. L'automanette se déconnecte. Les actions à piquer du PF n'arrêtent pas le mouvement à cabrer du THS qui atteint sa butée sept secondes après la déconnexion du PA. Le message « *FCS : TRIM LIMIT* » s'affiche sur l'écran primaire (PDU). Entre la déconnection du PA et la position en butée du THS, la vitesse conventionnelle de l'avion est passée de 297 à 220 kt.

L'augmentation de l'assiette longitudinale lors du déroulement du THS est accompagnée d'une légère inclinaison à droite et d'une augmentation de l'altitude. Le PF applique sur son mini-manche une action vers la gauche qui conduit à une inclinaison de 15 degrés à gauche. L'assiette longitudinale atteint 25 degrés à cabrer. Estimant que son action en tangage est inefficace, le PF applique alors une action en butée à droite. Il explique avoir voulu atteindre une inclinaison suffisante pour faire diminuer l'assiette longitudinale, augmenter la vitesse et reprendre le contrôle en tangage. Pendant cette manœuvre, l'inclinaison atteint 98 degrés à droite.

Dans le même temps, le commandant de bord (PNF) applique pendant neuf secondes des actions à piquer et des actions en roulis opposées à celles du PF. Ces actions simultanées de pilotage ont pour effet de diminuer l'inclinaison commandée par le PF et d'augmenter à nouveau l'assiette longitudinale, le facteur de charge et l'incidence. Ces actions simultanées déclenchent l'alarme « *DUAL INPUT* ». Le PF indique qu'il a alors demandé au PNF d'arrêter ses actions au mini-manche. Il a aussi pris la priorité sur les commandes en appuyant sur le bouton approprié de son mini-manche pendant six secondes. Le PF maintient l'inclinaison entre 40 et 80 degrés à droite pendant une vingtaine de secondes. Après avoir atteint 42 degrés à cabrer, l'assiette longitudinale diminue progressivement vers 10 degrés. L'angle d'incidence et le facteur de charge diminuent rapidement, respectivement de 22 vers 5 degrés et de 4,5g à des valeurs comprises entre 1,25 et 1,5g. Dans le même temps, la vitesse conventionnelle est passée de 300 kt à 150 kt.

[2] Mode de maintien de vitesse verticale.

[3] Tail Horizontal Stabilizer, acronyme utilisé par Dassault.

[4] A la déconnection du PA, l'assiette longitudinale est de zéro degré et le facteur de charge de 2g, tous deux en augmentation.

Le PF applique ensuite des actions en roulis sur la gauche jusqu'à stabiliser l'inclinaison vers 50 degrés. Alors que le THS est toujours en butée à cabrer, l'assiette longitudinale et la vitesse conventionnelle restent stables pendant une quarantaine de secondes à des valeurs respectives de 10 degrés à cabrer et de 200 kt. Le PNF indique avoir tenté d'utiliser le compensateur de profondeur manuel et de réarmer les commandes de vol en appuyant sur le bouton *« FCS ENGAGE »* du panneau supérieur.

Ne constatant aucune amélioration de la situation, le PNF applique aussi sur son mini-manche des actions en roulis, opposées à celles du PF ainsi que des actions en butée à piquer. Les actions simultanées en roulis des deux pilotes amènent progressivement l'inclinaison au neutre, ce qui a pour conséquence d'augmenter à nouveau l'assiette longitudinale jusqu'à environ 30 degrés et de réduire la vitesse conventionnelle jusqu'à 125 kt. L'équipage indique avoir entendu l'alarme sonore *« INCREASE SPEED »*. Cette nouvelle phase de double pilotage dure environ douze secondes. Les commandes sont ensuite transférées au commandant de bord. L'assiette commence à diminuer et l'altitude atteint un maximum de 22 500 ft. Lorsque l'assiette atteint 5 degrés à piquer, le commandant de bord applique des actions à cabrer. L'assiette augmente de nouveau et le commandant de bord reprend ses actions en butée à piquer.

Pour une raison que l'équipage n'explique pas, le THS commence à évoluer vers une position d'équilibre, passant de douze à un degré à cabrer en quinze secondes. Le contrôle de l'avion en tangage par les actions au mini-manche est redevenu possible. L'équipage décide de poursuivre le vol en pilotage manuel. L'approche et l'atterrissage se déroulent sans autre événement particulier.

Entre le début du mouvement à cabrer du THS et son retour en position d'équilibre, il s'est écoulé 2 minutes et 36 secondes au cours desquelles :

- le facteur de charge a atteint 4,6g ;
- l'altitude est passée de 13 000 à 22 500 ft ;
- la vitesse conventionnelle a évolué entre 300 et 125 kts ;
- l'assiette longitudinale a atteint 41 degrés.

A la suite de cet incident grave, la flotte de Falcon 7X a été arrêtée de vol temporairement[5]. La remise en service s'est faite à partir du 16 juin 2011.

[5] Par une consigne de navigabilité urgente de l'AESA émise le 26 mai 2011 (AD No.: 2011-0102-E).

1.2 Tués et blessés

	Blessures		
	Mortelles	**Graves**	**Légères/Aucune**
Membres d'équipage	-	-	3
Passagers	-	-	-
Autres personnes	-	-	-

1.3 Dommages à l'aéronef

Les inspections d'entretien effectuées à l'issue de l'incident n'ont révélé aucun dommage.

1.4 Autres dommages

Il n'y a aucun dommage.

1.5 Renseignements sur le personnel

1.5.1 Commandant de bord

1.5.1.1 Commandant de bord

Homme, 39 ans

1.5.1.1 Expérience et qualifications

- licence de pilote de ligne avion ATPL(A) délivrée le 30 octobre 2010 conformément aux exigences du JAR-FCL1 ;
- examen pratique de qualification de type Falcon 7X le 03 février 2011 ;
- qualification de type Falcon 7X et Falcon 900 valides ;
- stage commandant de bord en juin 2006 ;
- dernier contrôle hors ligne le 03 février 2011 ;
- dernier contrôle en ligne le 15 mai 2011 ;
- dernière formation CRM en février 2010 ;
- aptitude médicale valide de classe 1 du 09 décembre 2010.

Expérience :

- 3 917 heures de vol dont 134 sur type ;
- 125 heures dans les trois derniers mois, toutes sur type ;
- 57 heures dans les trente derniers jours, toutes sur type ;
- Aucune heure de vol dans les 24 dernières heures précédant l'événement.

1.5.1.2 Carrière aéronautique

- instructeur avion de 1994 à 2000 ;
- recruté en tant que copilote sur Falcon 900 par Jet-Link AG en juillet 2001.

1.5.2 Copilote

Homme, 40 ans

1.5.2.1 Expérience et qualifications

- licence de pilote de ligne avion ATPL(A) délivrée le 15 mai 2008 conformément aux exigences du JAR-FCL1 ;
- examen pratique de qualification de type Falcon 7X le 10 mars 2011 ;
- qualification de type Falcon 7X et Falcon 900 valides ;
- dernier contrôle hors ligne le 10 mars 2011 ;
- depuis l'examen pratique de qualification de type, le copilote était en adaptation en ligne sous supervision ;
- dernière formation CRM en février 2011 ;
- aptitude médicale valide de classe 1 du 17 mars 2011.

Expérience :

- 2 685 heures de vol dont 83 sur type ;
- 83 heures dans les trois derniers mois, toutes sur type ;
- 57 heures dans les trente derniers jours, toutes sur type ;
- Aucune heure de vol dans les 24 dernières heures précédant l'événement.

1.5.2.2 Carrière aéronautique

- pilote de chasse sur Mirage 2000 de décembre 1994 à septembre 1999 puis sur Mirage IV de septembre 1999 à septembre 2002 ;
- officier de sécurité des vols dans l'armée de l'air de 2002 à 2005 ;
- à partir de juin 2008, copilote sur Falcon 900 chez Netjets, transporteur aérien exploitant des avions d'affaires ;
- recruté en février 2010 par le propriétaire du HB-JFN en tant que copilote sur Falcon 900 ;
- transition chez Jet-Link AG, exploitant du HB-JFN.

1.6 Renseignements sur l'aéronef

Le HB-JFN appartient à la société Wallenmount Ltd basée à Hongkong et est exploité par Jet-Link AG, transporteur aérien basé en Suisse et exploitant d'avions d'affaire.

1.6.1 Cellule

Constructeur	Dassault Aviation
Type	Falcon 7X
Numéro de série	116
Immatriculation	HB-JFN
Mise en service	Mars 2011
Certificat de navigabilité	Valide délivré par l'aviation civile suisse
Certificat d'examen de navigabilité	Valide
Utilisation au 24 mai 2011	164 heures de vol et 67 cycles

1.6.2 Moteurs

Constructeur : Pratt & Whitney Canada
Type : PW307A

	Moteur n° 1	**Moteur n° 2**	**Moteur n° 3**
Numéro de série	PCE-CH 0367	PCE-CH 0366	PCE-CH 0368
Date d'installation	07 mars 2011	07 mars 2011	07 mars 2011
Temps total de fonctionnement	164 heures et 67 cycles	164 heures et 67 cycles	164 heures et 67 cycles

1.6.3 Masse et centrage

La masse de l'avion au décollage était de 69 243 lbs pour une masse maximale autorisée au décollage de 70 000 lbs ou 31 751 kg. Le centrage estimé de l'avion au décollage était de 27,5 % de la corde aérodynamique moyenne, à l'intérieur des limites opérationnelles (19,5 à 31,33 %).

Au moment du déroulement non commandé du THS, la masse de l'avion a été estimée par l'exploitant à 41 000 lbs et le centrage à 31,9 %, à l'intérieur des limites opérationnelles (19,5 à 38,5 %).

1.6.4 Entretien

Du 19 au 23 mai 2011, le HB-JFN se trouvait à Nuremberg pour des opérations d'entretien. Celles-ci ont été effectuées par Aero Dienst, organisme d'entretien agréé Part 145 (DE.145.0059) et comprenaient principalement des travaux liés à la cabine et aux moteurs. L'autorisation pour remise en service a été délivrée par Aero Dienst le 23 mai 2011.

1.6.5 Instruments de bord

1.6.5.1 Ecrans d'affichage

Le Falcon 7X est équipé de la suite avionique EASY (Enhanced Avionics SYstem) qui comprend quatre écrans permettant d'afficher les informations de pilotage, de gestion du vol ainsi que l'état des systèmes et les check lists électroniques. Ces écrans sont configurables par l'équipage en fonction des besoins opérationnels.

Dans une configuration standard, les PDU (Primary Display Unit) contiennent :

- ❒ un ADI (Attitude Director Indicator) avec les informations essentielles nécessaires au pilotage (attitudes, vitesse, altitude, etc) ;
- ❒ un HSI (Horizontal Situation Indicator) qui rassemble les principales informations de navigation ;
- ❒ la fenêtre ENG-CAS qui affiche les paramètres moteurs et les messages CAS (Crew Alerting System) ;
- ❒ une fenêtre paramétrable permettant l'affichage de la position des compensateurs (fenêtre ENG-TRIM), les moyens radiophoniques et de radionavigation, ou encore des informations de trafic issues du TCAS . Au moment du déroulement du THS, cette fenêtre affichait les moyens radiophoniques et de radionavigation sur le PDU de gauche et la fenêtre ENG-TRIM sur le PDU de droite. Quelques secondes après la reprise des commandes par le commandant de bord, l'affichage de cette fenêtre sur son PDU a changé au profit de la fenêtre ENG-TRIM.

Les MDU, plus modulables, peuvent être utilisés par l'équipage pour afficher, selon les phases de vol :

- ❒ des informations supplémentaires de navigation et de gestion du vol (cartes, listes des points tournant, performances de l'avion, etc) ;
- ❒ des schémas synoptiques indiquant l'état des systèmes et des conjoncteurs-disjoncteurs.

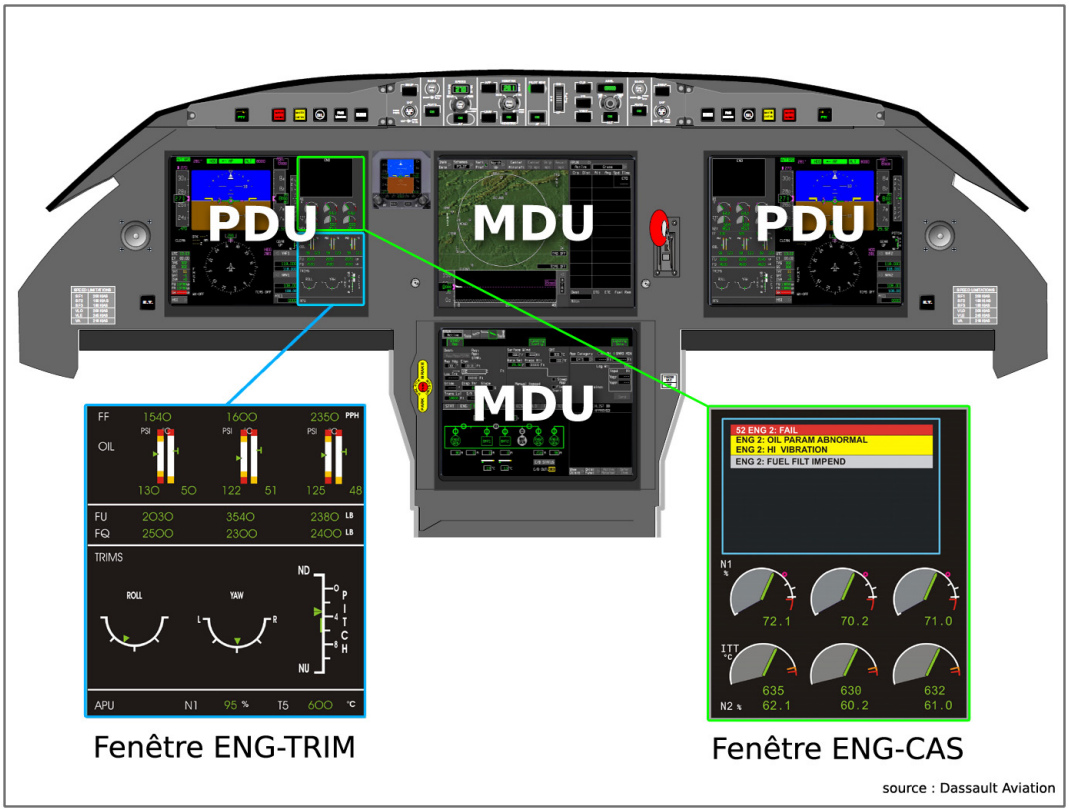


Figure 1 - instruments de bord

1.6.5.2 Crew Alerting System (CAS)

Le système CAS surveille en permanence l'état des systèmes et alerte l'équipage en générant un message dans la fenêtre ENG-CAS et/ou une alerte sonore en fonction de la criticité de la panne.

Lors de l'événement, le message ambre « *FCS : TRIM LIMIT* » a été généré. Un message de couleur ambre indique une panne ou un événement anormal nécessitant une attention immédiate de l'équipage suivie d'une action corrective.

Le système CAS génère un message « *FCS : TRIM LIMIT* » lorsque l'ordre en tangage ou en roulis est supérieur à 90 % de l'ordre maximal. L'action corrective associée nécessite de la part de l'équipage de :

- ❒ maintenir une vitesse et une configuration pour lesquelles les forces exercées sur les commandes de vol sont acceptables ;
- ❒ de vérifier l'état des gouvernes, la répartition du carburant, le centrage et l'accumulation éventuelle de glace pour corriger le déroulement du compensateur ;
- ❒ puis de reprendre une vitesse et une configuration avion correspondant à la phase de vol.

Lorsque le message « *FCS : TRIM LIMIT* » est émis, un signal d'alerte Master Caution s'allume et l'alerte sonore « *Gong* » est générée.

1.6.5.3 Indications de double pilotage

Le Falcon 7X est équipé de deux mini-manches indépendants qui permettent le contrôle de l'avion en tangage et en roulis. En cas d'action simultanée de chaque pilote, les ordres sont sommés algébriquement. Une alarme sonore « *DUAL INPUT* » est alors générée et le vibreur de manche est activé.

A tout moment, l'un des deux pilotes peut désactiver le mini-manche de l'autre en appuyant et en maintenant enfoncé le bouton de prise de priorité (PTY).

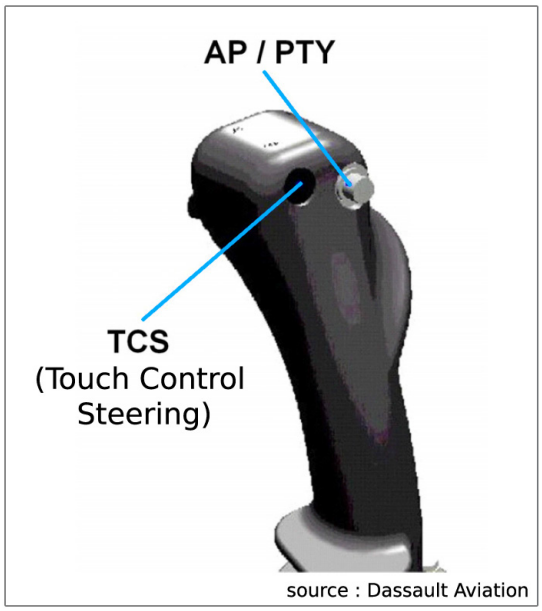


Figure 2 - mini-manche

Dans ce cas :

- un indicateur lumineux vert PTY[6] s'allume devant le pilote dont le mini-manche est actif ;
- une flèche ambre s'allume devant le pilote dont le mini-manche est désactivé et indique le côté qui a la priorité ;
- une alarme sonore « *PRIORITY RIGHT* » est générée si le pilote en place droite a pris la priorité, ou « *PRIORITY LEFT* » si la priorité est opposée.

[6]PRIORITY.

Ainsi, lorsque le co-pilote prend la priorité sur le commandant de bord, les indications suivantes sont présentées, à gauche devant le commandant de bord et à droite devant le co-pilote :

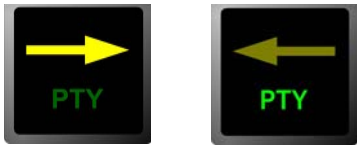


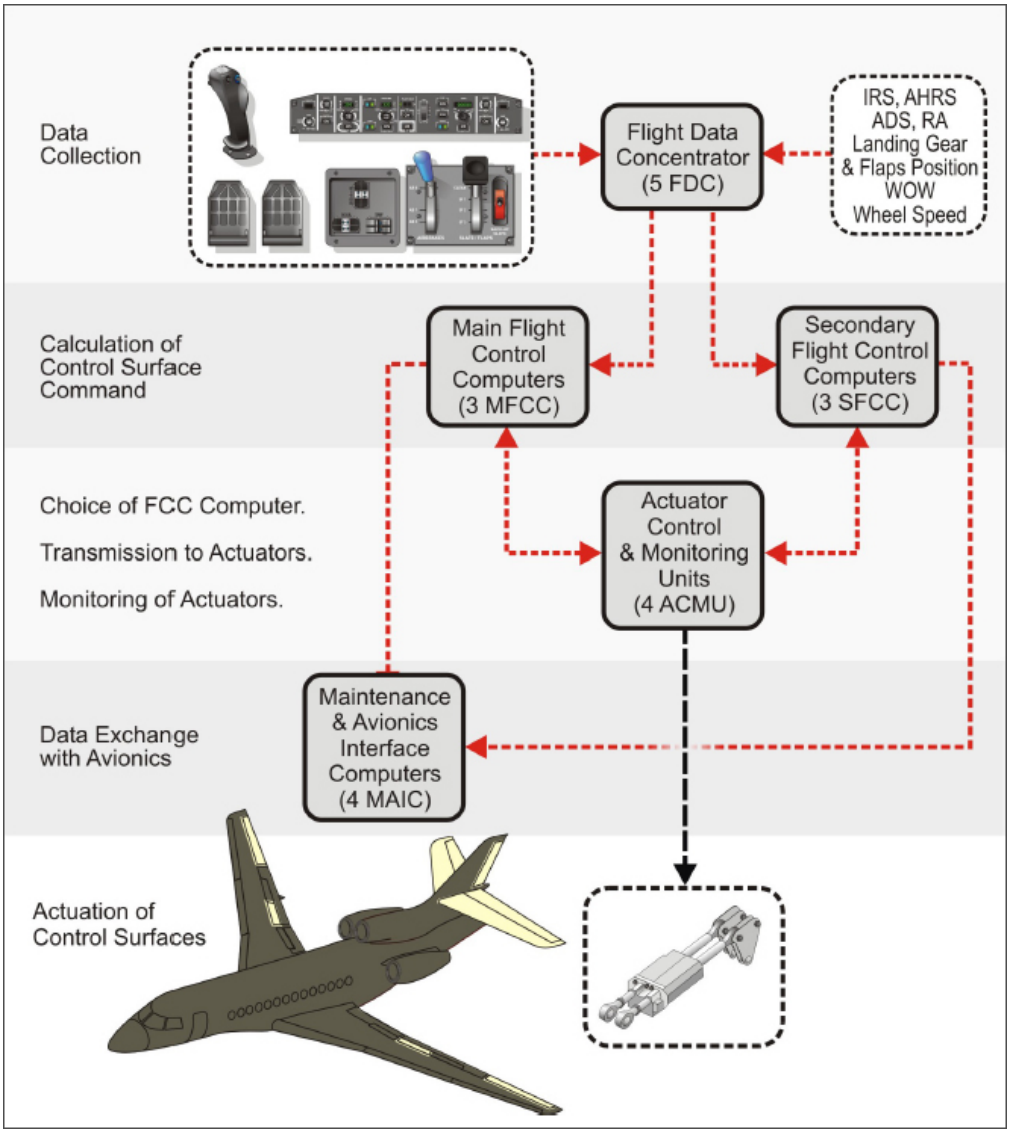
Figure 3 - indications visuelles de prise de priorité

1.6.6 Système de compensation de profondeur

1.6.6.1 Architecture générale du système de commande de vol électrique

Le système de commande de vol électrique du Falcon 7X est assuré par les éléments suivants :

- cinq FDC (*Flight Data Concentrators*) qui collectent des données issues des capteurs et des dispositifs de contrôle de l'avion ;
- trois MFCC (*Main Flight Control Computer*) et trois SFCC (*Secondary Flight Control Computer*) qui reçoivent les informations issues des FDC et élaborent les ordres de braquage des gouvernes en fonction des lois de commande de vol disponibles ;
- quatre ACMU (*Actuator Control Monitoring Unit*) qui reçoivent chacun les ordres élaborés par tous les MFCC et les SFCC, écartent éventuellement les ordres incohérents et envoient ensuite l'ordre de braquage aux gouvernes qui leur sont rattachées. Les ACMU asservissent ensuite les actionneurs aux ordres transmis ;
- quatre MAIC (Maintenance and Avionics Interface Computer) qui reçoivent les données[7] des MFCC et SFCC et d'autres calculateurs. A partir de ces informations, les MAIC élaborent d'une part les informations présentées dans les différents synoptiques des écrans d'affichage et d'autre part, les messages CAS.



(source : Dassault Aviation)

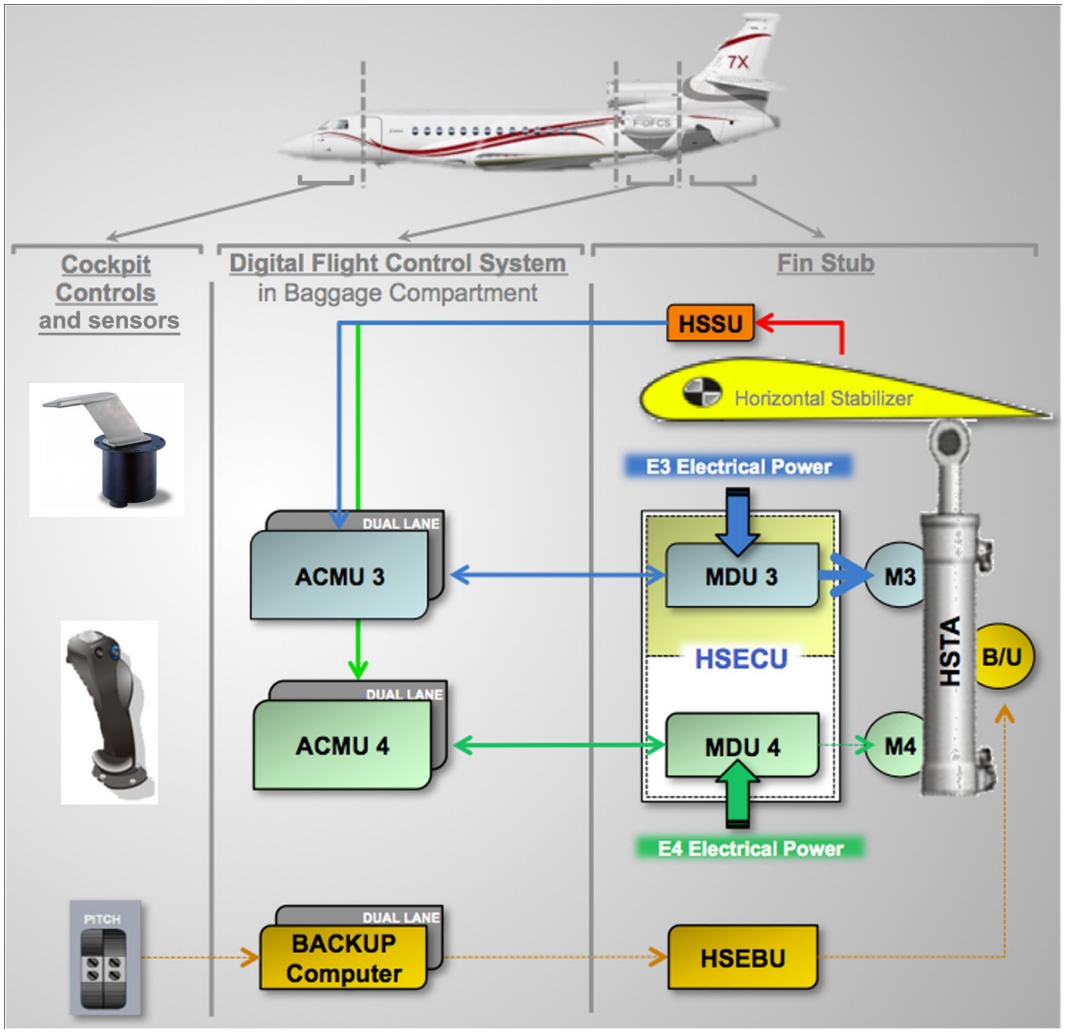
Figure 4 - architecture générale du système de commande de vol électrique

[7] En particulier les modes des lois de commandes de vols (Normal, Alternate, Direct Laws) ainsi que les états de pannes des différents capteurs/calculateurs/ actionneurs.

1.6.6.2 Contrôle du THS

Le contrôle du THS est assuré par les éléments suivants :

- un actionneur électrique, HSTA (*Horizontal Stabilizer Trim Actuator*), pouvant être actionné par trois moteurs électriques, M3, M4 et B/U (*Back Up*) ;
- un contrôleur électronique, HSECU (*Horizontal Stabilizer Electronic Control Unit*), composé de deux chaînes de commande, MDU (Motor Drive Unit) 3 et MDU4, qui contrôlent respectivement les moteurs M3 et M4;
- l'ACMU 3 et l'ACMU 4, qui reçoivent des MFCC et des SFCC les ordres de position du THS et qui élaborent la consigne de vitesse de rotation de M3 ou M4. Cette consigne est ensuite transmise au MDU 3 ou 4 ; les ACMU surveillent également le fonctionnement du MDU qui leur est associé ;
- deux capteurs doubles de position du compensateur, HSSU, qui envoient cette information aux ACMU ;
- un contrôleur électronique de secours, HSEBU (*Horizontal Stabilizer Electronic Backup Unit*), qui commande le moteur de secours de l'actionneur, B/U ;
- un BACKUP Computer, qui reçoit les ordres provenant de la commande manuelle de trim située dans le cockpit et qui les transmet au HSEBU.



(source : Dassault Aviation)

Figure 5 - contrôle du THS

Trois chaînes indépendantes assurent donc le contrôle du compensateur de profondeur :

- ❒ la chaîne 3, qui est la chaîne active en fonctionnement normal. Dans ce cas, le MDU3 contrôle le moteur 3 selon les ordres reçus de l'ACMU3. Les moteurs 4 et B/U ne sont pas alimentés et la fonction de compensation automatique (auto-trim) est active ;
- ❒ la chaîne 4 qui est activée lorsqu'un problème est détecté sur le moteur 3. Le HSECU bascule alors sur le MDU 4 qui commande le moteur 4 selon les ordres reçus de l'ACMU 4. La fonction auto-trim reste active ;
- ❒ la chaîne de secours, utilisée lorsqu'un problème est détecté sur les moteurs 3 et 4. Dans ce cas, la fonction auto-trim est perdue. Le compensateur est alors contrôlé manuellement par l'équipage par la commande située dans le cockpit.

En vol, tant que la fonction auto-trim est active, l'équipage ne peut pas contrôler le compensateur manuellement et n'a accès au contrôle manuel que lorsque la fonction auto-trim est perdue.

Les ordres envoyés par les chaînes de commande 3 et 4 aux moteurs actionnant le THS sont transmis sous la forme de vitesses de rotation de ces moteurs.

Les surveillances mises en jeu pour changer de chaîne de commande sont effectuées par les ACMU notamment à partir :

- ❒ de la position du THS envoyée par le HSSU et
- ❒ des informations suivantes reçues du HSECU :
  - ■ vitesse et sens de rotation du moteur du THS ;
  - ■ température de ce moteur ;
  - ■ intensité du courant consommé.

Un certain nombre de surveillances sont conçues pour détecter un déroulement non commandé du THS en fonction de l'origine du dysfonctionnement (HSSU, ACMU ou HSECU). La surveillance mise en place pour détecter un déroulement non commandé résultant d'un dysfonctionnement du HSECU consiste à vérifier la cohérence entre :

- ❒ la consigne de vitesse calculée par l'ACMU et
- ❒ la vitesse et le sens de rotation du moteur transmis par le HSECU.

De plus, les surveillances sur le courant consommé et sur la température du moteur sont conçues pour se déclencher en cas de blocage du THS (saturation, blocage mécanique, butée mécanique).

Ainsi, la fonction de surveillance de la chaîne de commande du THS réalisée par l'ACMU dépend des paramètres renvoyés par le HSECU qui assure le contrôle du THS.

1.6.7 Pilote automatique (PA)

La déconnexion du PA peut être manuelle ou automatique. Une déconnexion automatique intervient lorsque l'une des conditions suivantes est remplie :

- ❒ le bouton TOGA des manettes des gaz est actionné ;
- ❒ les efforts sur l'un des mini-manches dépassent un certain seuil ;
- ❒ une panne du pilote automatique est détectée ;
- ❒ les protections haute ou basse vitesse du système de commande de vol sont activées ;
- ❒ le roulis ou la pente dépassent respectivement 80 ou ± 60 degrés.

Ainsi, il apparaît à la lecture des paramètres du FDR (*cf. annexe 1*) que lors de l'incident, la seule condition qui a pu provoquer la déconnexion automatique du PA est l'action à piquer du co-pilote sur son mini-manche.

1.7 Renseignements météorologiques

L'équipage a indiqué qu'au moment de l'événement, l'avion évoluait en conditions de vol VMC sans turbulence.

1.8 Aides à la navigation

Sans objet.

1.9 Télécommunications

Sans objet.

1.10 Renseignements sur l'aérodrome

Sans objet.

1.11 Enregistreurs de bord

L'avion était équipé de deux enregistreurs de vol[8], chacun permettant d'enregistrer les paramètres des 25 dernières heures de vol ainsi que les données phoniques des deux dernières heures de vol.

Sur l'aire de stationnement, l'alimentation électrique de l'avion n'a pas été arrêtée et les données phoniques relatives à l'évènement n'ont donc pas été disponibles.

Des courbes de paramètres sont jointes en annexe 1.

[8] Les deux enregistreurs de vol, identiques, sont fabriqués par Honeywell et portent le P/N 980-6021-072.

1.12 Renseignements sur l'épave et sur l'impact

Sans objet.

1.13 Renseignements médicaux et pathologiques

Sans objet.

1.14 Incendie

Sans objet.

1.15 Questions relatives à la survie des occupants

Sans objet.

1.16 Essais et recherches

1.16.1 Examens du HSECU

Le HSECU est un équipement produit par Rockwell Collins répondant aux spécifications techniques de Dassault Aviation. Il est intégré dans le système de contrôle du compensateur de profondeur par Dassault Aviation.

Des tests fonctionnels et un examen visuel n'ont révélé aucun dysfonctionnement du HSECU.

Note : les inspections visuelles des cartes électroniques du HSECU ont toutefois permis de constater que, du fait de leur implantation, certains composants installés sur des cartes adjacentes étaient en contact mécanique l'un avec l'autre. Il a été découvert par la suite que ces interférences mécaniques n'étaient pas à l'origine de l'évènement. Ces cartes ont cependant fait l'objet d'une modification par Rockwell Collins détaillée dans la partie 5 de ce rapport.

Des tests réalisés sur des HSECU identiques à celui équipant le HB-JFN ont mis en évidence que l'alimentation des cartes électroniques du HSECU avec une tension interne aux alentours de +0,7 V au lieu de -15 V en fonctionnement nominal, permettait de reproduire un déroulement du THS similaire à celui de l'événement.

Un examen de l'alimentation -15 V a permis de restreindre à trois le nombre de modes de défaillance susceptibles de générer de telles variations de tensions électriques. Un complément d'examen a été effectué pour détecter la présence éventuelle d'un de ces modes de défaillance sur le HSECU équipant l'avion HB-JFN. Il a révélé que :

- la valeur de l'impédance[9] du composant référencé L4 était instable, variant entre la valeur nominale de 0.5 Ω et des valeurs anormales atteignant 300 kΩ lorsqu'un faible appui était exercé sur le composant ;
- l'une des brasures de cette inductance présentait des fissures à sa base induisant une perte du lien mécanique et un mouvement possible de la broche du composant dans le circuit imprimé. Ce type de brasure est appelé « *brasure froide* ».

[9] L'impédance d'un composant électrique mesure l'opposition que présente ce composant au passage d'un courant électrique.

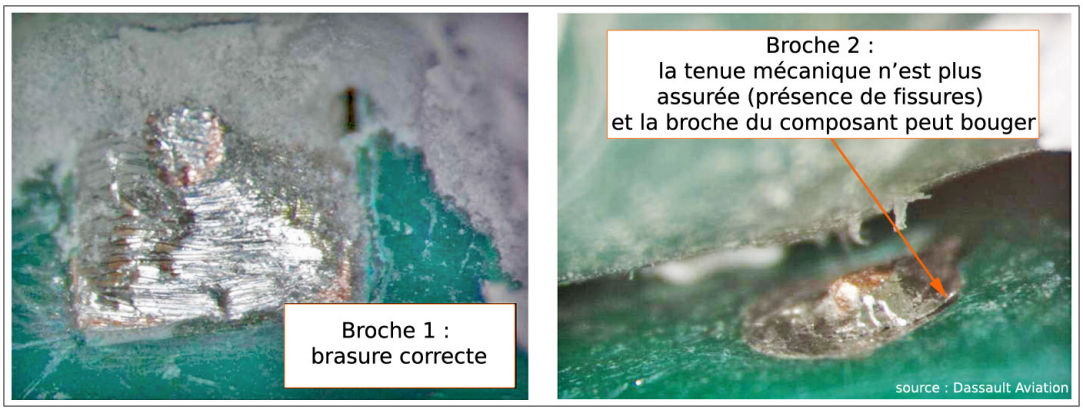


Figure 6 - défaut de brasure de l'inductance L4

Après remontage de la carte dans le boîtier et mise sous tension, il n'a pas été possible de reproduire le dysfonctionnement de l'alimentation -15V malgré plusieurs tentatives.

L'examen du défaut de brasure aux rayons X a permis de mettre en évidence :

- ❒ l'absence d'alliage dans 90% du trou métallisé[10] ;
- ❒ la présence de microfissures entre la broche du composant et le circuit imprimé.

[10] Trou percé dans une carte électronique pour braser la broche d'un composant.

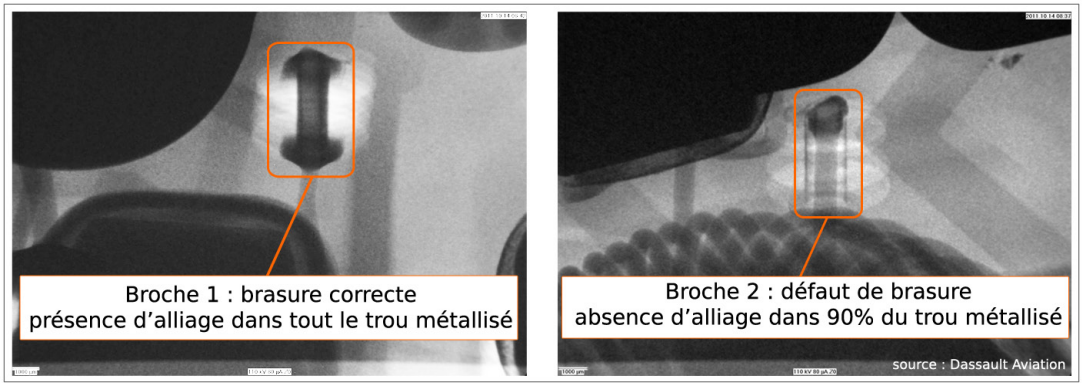


Figure 7 - examen au RX du défaut de brasure de l'inductance L4

1.16.2 Origine du déroulement non commandé du compensateur de profondeur

Le défaut de brasure a créé des fluctuations de l'impédance du composant L4 et a conduit l'alimentation interne du HSECU à délivrer une tension inadaptée en valeur absolue et en signe.

En raison de ce défaut de brasure, la chaîne de commande du HSECU a alors élaboré et transmis en permanence un ordre à cabrer au moteur du THS, alors qu'elle envoyait dans le même temps à l'ACMU une vitesse de rotation indiquant un mouvement à piquer du THS, comme l'illustre le schéma ci-après.

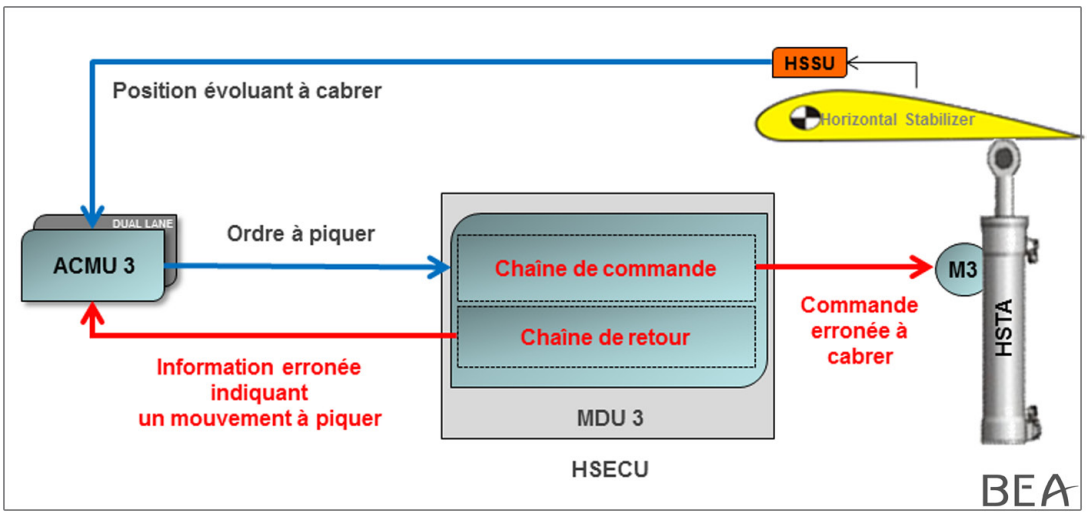


Figure 8 - impact du dysfonctionnement de l'alimentation interne du HSECU

Pour contrer le mouvement à cabrer de l'avion, l'ACMU envoyait au HSECU un ordre à piquer et recevait du HSECU une vitesse indiquant un mouvement à piquer du THS, cohérente avec l'ordre envoyé.

Par conséquent, la surveillance basée sur la cohérence entre la consigne de vitesse envoyée par l'ACMU et la vitesse renvoyée par le HSECU ne pouvait pas se déclencher.

Par ailleurs, la surveillance basée sur le courant consommé ne s'est également pas déclenchée. Les examens réalisés sur le HSECU ont démontré que cette surveillance ne se déclenche pas lorsque l'alimentation interne (tension de -15 V) n'est pas correcte (dans le cas présent pour des tensions aux alentours de +0,7 V). Il n'a pas été envisagé, au moment de la conception, qu'une alimentation -15V puisse délivrer de telles valeurs de tension.

Par la suite, lorsque l'actionneur du THS a atteint sa butée, la réception continue d'ordres à cabrer a fait augmenter la température du moteur M3. Lorsque son seuil d'activation a été dépassé, la surveillance en température, s'est déclenchée. L'ACMU a alors fait basculer le contrôle du THS sur la chaîne 4 qui a commandé un mouvement à piquer du THS jusqu'au retour à l'équilibre en tangage.

1.16.3 Origine du défaut de brasure

La présence de microfissures sur la brasure de l'une des broches de l'inductance L4 provient d'une chaleur insuffisante lors du processus de brasage. Ceci est dû au fait que le trou métallisé n'était pas suffisamment isolé thermiquement du plan de masse de la carte électronique. Une partie de la chaleur apportée pour le brasage a de fait été absorbée empêchant la réalisation d'une brasure correcte.

1.17 Renseignements sur les organismes et la gestion

1.17.1 Renseignements sur l'AESA et la certification de type

1.17.1.1 Définitions

CS/JAR 25 : Spécifications de certification pour les aéronefs de masse maximale au décollage supérieure à 5 700 kg.

Part 21 : Exigences et procédures relatives à la certification des aéronefs et des produits, pièces et équipements associés, et à celle des organismes de conception et de production.

Organisme de conception : Organisme en charge de la conception des produits, des pièces et des équipements, des modifications ou des réparations à apporter à ces derniers. Il doit démontrer ses capacités conformément aux dispositions de la Part 21. Il doit en particulier maîtriser et surveiller l'ensemble de la conception. Lorsque des pièces ou équipements sont prévus d'être conçus par des partenaires ou des sous-traitants, la manière dont leur acceptabilité est déterminée doit être établie par l'organisme de conception.

Organisme de production : Organisme responsable de la production des produits, des pièces et des équipements. Il doit démontrer ses capacités conformément aux dispositions de la Part 21.

1.17.1.2 Renseignements sur l'AESA

L'Agence Européenne de la Sécurité Aérienne (AESA) est l'autorité compétente chargée par la Commission Européenne d'harmoniser les normes de sécurité aérienne en Europe et en particulier d'assurer pour le compte des États membres les fonctions et les tâches de l'État de conception en matière de certification des aéronefs.

A cette fin, l'AESA délivre notamment les certificats de type ainsi que les agréments d'organismes de conception.

Les organismes détenteurs d'un agrément de conception et postulant à un certificat de type doivent démontrer la conformité aux conditions techniques applicables et soumettre à l'AESA les moyens par lesquels cette conformité est démontrée.

Les organismes détenteurs d'un agrément de production doivent fournir des attestations de conformité pour tout aéronef, pièce, produit ou équipement. Ces attestations permettent de garantir que :

- ❒ chaque produit, pièce ou équipement est conforme aux données de définition approuvées, et qu'il peut fonctionner en toute sécurité ;
- ❒ chaque aéronef a fait l'objet d'essais au sol et en vol.

L'AESA est impliquée tôt dans le processus de certification de type, notamment lors de la validation du plan identifiant les moyens de conformité retenus ainsi que les documents de certification présentés comme justification. Dans ce cadre, l'agence n'a pas obligation de vérifier l'ensemble de la documentation, ni de procéder à toute inspection ni d'effectuer (ou d'assister à) tout essai pour vérifier la validité de la conformité. La documentation revue est définie entre l'AESA et l'organisme de conception en fonction du projet à certifier.

Pour la certification du Falcon 7X, trois catégories de documents ont ainsi été définies :

- ❒ **Catégorie 2** : document fourni à l'AESA pour acceptation après validation par l'organisme de conception ;
- ❒ **Catégorie 1** : document accepté par l'AESA sans vérification et fourni à l'AESA pour information après validation par l'organisme de conception ;
- ❒ **Catégorie 0** : document accepté par l'AESA sans vérification et non fourni à l'AESA après validation par l'organisme de conception. Celui-ci doit fournir ce type de document, sur demande de l'AESA.

1.17.1.3 Exigences réglementaires liées aux commandes de vol

Les conditions réglementaires applicables aux systèmes de commandes de vol sont spécifiées, entre autres, dans les paragraphes JAR25.671 et JAR 25.1309. Le règlement FAR dispose des mêmes conditions.

- ■ JAR 25.671[(11)] : généralités sur les commandes de vol

Le concepteur de l'avion doit en particulier montrer par analyse, essai ou les deux, qu'un vol peut être poursuivi en toute sécurité, dans l'enveloppe de vol normale de l'avion et sans nécessiter de qualité ou de force exceptionnelles de la part de l'équipage, après notamment les pannes suivantes :

- ❒ toute panne unique, à l'exception de celle conduisant à un blocage d'une gouverne ou d'une commande dû à une interférence physique ;
- ❒ toute combinaison de panne n'étant pas démontrée comme étant extrêmement improbable[(12)] ;
- ❒ toute panne ou événement qui conduit à un blocage d'une gouverne ou d'une commande pilote qui reste fixe dans une position en raison d'une interférence physique ;
- ❒ tout déroulement non commandé d'une gouverne vers une position indésirable si ce déroulement résulte d'une panne unique ou d'une combinaison de pannes qui n'est pas extrêmement improbable.

[(11)] JAR 25.671 et conditions spéciales applicables pour le Falcon 7X.

[(12)] Probabilité par heure de vol de 1 x 10-9 ou moins.

- JAR 25.1309[13] : équipements, systèmes et installations

Ce paragraphe s'applique à de nombreux systèmes et équipements, dont le système de compensation. Il fournit des conditions supplémentaires au paragraphe JAR 25.671 dont les suivantes :

- (b) : les systèmes avion et leurs composants, considérés de manière séparée ou commune, doivent être conçus de telle sorte que :
  - toute condition de panne catastrophique[14] soit extrêmement improbable et ne résulte pas d'une panne unique ;
  - toute condition de panne dangereuse soit « *extremely remote* » / très peu probable[15] ;
  - toute condition de panne majeure soit « *remote* » / peu probable[16].
- (d) : le respect les conditions du sous-paragraphe (b) doit être démontré par des analyses, et, si nécessaire, par des essais appropriés au sol, en vol ou en simulateur. Ces analyses doivent considérer :
  - 1. les modes de panne possibles, y compris les dysfonctionnements et dommages de sources extérieures ;
  - 2. la probabilité de pannes multiples et de pannes non détectées ;
  - 3. les effets sur l'aéronef et ses occupants ;
  - 4. les alarmes, les actions correctives requises de la part de l'équipage et la capacité à détecter des problèmes.

Pour démontrer le respect des exigences précédentes, des moyens acceptables (AMJ[17]) sont également décrits dans le JAR 25. Pour le paragraphe JAR 25.1309, il ressort en particulier les points suivants :

- Ces moyens reposent sur le principe que les systèmes doivent être conçus de telle sorte qu'il existe une relation inverse entre :
  - la sévérité des conséquences d'une condition de panne/défaillance (cinq niveaux : sans effet, mineur, majeur, dangereux et catastrophique) et
  - les probabilités d'occurrence de cette condition (probable, faible, très faible, extrêmement improbable). Ces probabilités sont définies de manière qualitative et quantitative. Par exemple, toute condition de panne catastrophique devrait être extrêmement improbable.
- Le concept de « *fail safe design* » définit certains objectifs relatifs aux pannes. Par exemple, pour chaque système ou sous-système, aucune panne unique d'un élément, composant ou connexion au cours d'un vol ne devrait conduire à une condition de panne catastrophique.
- Tous les moyens de conformité au JAR 25.1309 (b) et (d) n'étant pas définis, il est précisé qu'un accord sur les moyens utilisés doit être établi tôt dans le processus d'analyse entre le concepteur et l'autorité de certification.
- Différentes techniques sont décrites pour l'évaluation des causes, la sévérité et la probabilité des conditions de panne, dont l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC ou FMEA). Les FMEA sont décrites comme étant des analyses structurées, inductives qui peuvent être utilisées pour évaluer les effets sur les systèmes et l'aéronef de chaque panne possible d'élément ou de composant. Le paragraphe précise que lorsqu'elles sont correctement réalisées, ces analyses permettent d'identifier les pannes latentes et les causes possibles de chaque mode de panne.

[13] JAR 25.1309 et conditions spéciales applicables pour le Falcon 7X.

[14] Condition de panne qui ne permet pas la poursuite du vol et l'atterrissage en toute sécurité.

[15] Probabilité par heure de vol de 1 x 10-7 ou moins mais supérieure à 1 X 10-9

[16] Probabilité par heure de vol de 1 x 10-5 ou moins mais supérieure à 1 X 10-7.

[17] Advisory Material Joint.

1.17.1.4 Processus d'analyses de sécurité

Le processus d'analyse de sécurité peut être représenté selon un cycle en V, la partie gauche du V correspondant à la phase de développement, de spécification et de validation, la partie droite aux phases d'intégration et de vérification.

Dans le cadre de la conformité au JAR25.1309, les analyses de sécurité effectuées dans le cadre de la conception lors de la phase de développement des systèmes comportent, entre autres, les documents suivants :

- FHA (Functional Hazard Assessment) : ces analyses interviennent très tôt dans la conception et sont mises à jour régulièrement avec les évolutions de conception de l'avion et de ses systèmes.
  - elles examinent les fonctions de l'avion et des systèmes et identifient les conditions de pannes fonctionnelles associées à chacune de ces fonctions ;
  - elles déterminent les effets de chacune des conditions de panne identifiées et établissent leur gravité.
- PSSA (Preliminary System Safety Assessment) : ce type d'analyse évalue les propositions de conception des systèmes et décline les objectifs de sécurité définis par la FHA au niveau des systèmes et équipements concernés. A cet effet, elles contiennent typiquement des arbres de défaillance des conditions de panne identifiées par la FHA ainsi qu'une estimation des probabilités d'occurrence correspondantes.
- SSA (System Safety Assessment) : les SSA prennent en compte les résultats des FMEA (*cf. ci-dessous*) et d'autres analyses de sécurité et contiennent la liste définitive des conditions de panne du système et des probabilités associées. Le but des SSA est ainsi de vérifier que les exigences de sécurité sont respectées.
- FMEA (Failure Modes and Effect Analysis) : A partir d'une démarche inductive aussi exhaustive que possible, les FMEA identifient pour chaque composant d'un équipement :
  - les fonctions de ce composant ;
  - les différents modes de défaillance de chacun des composants ;
  - les causes de ces pannes (type de défaillance de chaque composant ou de fonction de l'équipement) ;
  - les effets de chaque panne sur l'équipement ou le système ;
  - les probabilités d'occurrence de chaque panne.

L'élaboration des FMEA, largement utilisées dans l'industrie pour déterminer les modes de panne des équipements, repose en partie sur les connaissances et l'expérience des modes et des mécanismes de défaillance que peut avoir le personnel de l'équipementier.

L'AESA s'assure que les organismes de conception fournissent l'ensemble des documents indispensables pour la certification de type. Elle vérifie et approuve ou accepte les FHA et les SSA. Les FMEA ne sont pas vérifiées de manière systématique par l'AESA qui de fait, n'a pas nécessairement de contact avec les équipementiers dans le cadre de la certification de type d'un aéronef.

1.17.1.5 Standards techniques

Les documents suivants servent de référence aux équipementiers pour la conception des analyses de sécurité :

- document technique militaire américain MIL-STD-1629A du 24 novembre 1980 ;
- ARP4761 de décembre 1996 ;
- DO178B de décembre 1992.

MIL-STD-1629A

Ce document est un standard militaire qui décrit des procédures visant à développer des analyses de panne d'équipements et à évaluer l'impact potentiel de leur défaillance fonctionnelle ou matérielle. Il peut être utilisé pour la conception, le développement, l'évaluation et la validation d'un programme.

ARP 4761

Publié par SAE[18], le standard technique ARP4761 fournit des guides d'élaboration d'analyses de sécurité en vue de se conformer aux exigences réglementaires des paragraphes JAR/FAR 25.1309. Il décrit de manière détaillée le processus d'analyse de sécurité des systèmes complexes (FHA, SSA Préliminaires, SSA) ainsi que les méthodes utilisables (dont les FMEA) pour se conformer à ce processus. En particulier, il prévoit au cours du processus SSA d'inclure une analyse de mode commun permettant d'assurer l'indépendance entre fonctions utilisant les mêmes sources d'information (signal, alimentation) et d'identifier les éventuels défauts de mode commun. Il est cité comme référence dans les moyens de conformité au paragraphe 25.1309 de la version actuelle du CS25. Ce document indique, en particulier en paragraphe G 3.2.2, que la détermination de tous les modes de pannes est extrêmement difficile et quelque fois impossible, sauf pour les composants les plus simples pour lesquels des données de l'industrie sont disponibles.

[18] Society of Automative Engineers. Société fondée en 1905 par des industriels dans le but de développer et de partager des standards techniques qui comprennent les ARP, Aerospace Recommended Practices.

DO178B

Ce document, élaboré conjointement par l'EUROCAE (*European Organization for Civil Aviation Equipment*) et le RTCA (*Radio Technical Commision for Aeronautics*), est un guide pour le développement de logiciels destinés à être installés sur des matériels certifiés. Ce document rassemble les bonnes pratiques en vigueur dans l'industrie depuis de nombreuses années. Il ne recommande pas de méthode ou de processus particuliers, mais fixe des objectifs que ces processus doivent respecter.

1.17.2 Renseignements sur Dassault Aviation

1.17.2.1 Certification de type du Falcon 7X

Le certificat de type du Falcon 7X a été délivré par l'AESA le 27 avril 2007[19]. A la date de l'incident, la flotte des Falcon 7X comptait environ 75 000 heures de vol.

Le Falcon 7X répond aux spécifications de certification en vigueur au moment de la demande de certification de type, en l'occurrence le JAR25 change 15[20], ainsi qu'aux conditions spéciales émises par l'AESA.

[19] Le Falcon 7X a aussi été certifié par la FAA.

[20] JAR25 change 16 pour le paragraphe JAR 25.1309 (b) et conditions spéciales pour le JAR25.671 (cf.1.17.1.3).

Conformément à ces exigences réglementaires et à certaines normes, Dassault Aviation, organisme de conception agréé Part 21 par l'AESA, a élaboré des spécifications techniques pour chacun des équipements de l'avion. La conception des contrôleurs électroniques HSECU a été sous-traitée à Rockwell-Collins qui ne dispose pas d'un agrément AESA d'organisme de conception. Cette activité de conception s'est donc effectuée sous la surveillance de Dassault. Des points réguliers et des revues techniques entre Dassault et Rockwell-Collins ont ainsi été effectués lors de la phase de conception des HSECU. Ceux-ci sont approuvés pour être installés sur les Falcon 7X et répondent aux spécifications demandées par Dassault Aviation.

1.17.2.2 Analyses de sécurité des systèmes de commandes de vol du Falcon 7X

Le système de commandes de vol du Falcon 7X a fait l'objet d'une SSA basée sur un outil de modélisation et d'analyse dysfonctionnelle (OCAS[21]). Cette méthode permet une approche intégrée pour les analyses de sécurité. Le choix de cette méthode a été fait en concertation avec l'AESA.

[21] Outil de conception assistée de spécification, qualifié conformément aux paragraphes relatifs aux outils de vérification du standard technique DO178B.

Cet outil a été qualifié selon le processus de qualification défini dans le document technique DO178B et permet de réaliser une PSSA approfondie et une SSA du système de commandes de vol du Falcon 7X. Cette dernière est un document de catégorie 2 (*cf. 1.17.1.2*) soumis à l'acceptation de l'AESA après validation par Dassault Aviation.

Elle est constituée de cinq documents :

- **Analyse de sécurité du système de commandes primaires de vol** :
  - Il s'agit de la synthèse de l'ensemble des conditions de panne, de leur criticité et de leur probabilité d'occurrence.
- **Livre 1 - Evaluation de sécurité du système de commandes primaires de vol** :
  - Ce document explicite les résultats des analyses de sécurité quantitatives et qualitatives pour chaque mode de défaillance.
- **Livre 2 - « *minimal cuts set*[22] »** :
  - Ce document liste les défaillances ou combinaison de défaillances des différents systèmes ou équipements, avec leur probabilité d'occurrence, pouvant conduire au mode de défaillance considéré.
  - Ce document permet de démontrer comment ont été établies les probabilités d'occurrence des modes de défaillance considérés pour le système de commandes de vol primaires.
- **Livre 3 - MMEL :**
  - Ce document fait le lien entre les modes de défaillance considérés et la MMEL.
- **Livre 4 - Liste globale d'événement** :
  - Ce document liste l'ensemble des défaillances prises en compte dans les analyses de sécurité de chaque mode de défaillance du système de commandes de vol primaires.
  - Les probabilités d'occurrence de ces défaillances sont également indiquées dans ce document.

[22] « *ensemble de coupes minimales* » correspondant à une panne donnée.

1.17.2.3 Analyses de sécurité liées à un déroulement non-commandé d'une gouverne primaire en loi normale

Il ressort en particulier des documents d'analyse de sécurité du système de commandes de vol primaires les éléments suivants :

SSA :

- ❒ Ce document identifie une condition de panne relative à un déroulement non-commandé et non arrêté par les sécurités d'une gouverne primaire en loi normale (nommée « *one primary control surface runaway* »). L'objectif à atteindre concernant cette condition de panne, dont la conséquence est considérée comme catastrophique, est d'avoir une probabilité d'occurrence extrêmement improbable.
- ❒ Pour le système de compensation en profondeur, cette condition de panne, correspondant à ce qui s'est produit lors du vol de l'incident, se caractérise par une position du THS en butée avec pour résultat une possible perte de contrôle de l'avion.
- ❒ La probabilité d'occurrence estimée dans le cadre de la SSA à partir de l'outil OCAS est inférieur à cet objectif ($2.2*10^{-10}$), ce qui répond aux spécifications réglementaires.
- ❒ Par ailleurs, la SSA indique aussi qu'en cas de déroulement non-commandé en loi normale d'une gouverne primaire :
  - ■ aucune indication n'est prévue dans le poste de pilotage,
  - ■ aucune procédure n'est disponible pour les équipages.

Livre 1 :

- ❒ Ce document définit le mode de défaillance d'un déroulement non-commandé d'une gouverne primaire. Celui-ci est la conséquence d'un déroulement des destructeurs de portance, de la gouverne de direction, des ailerons ou de la gouverne de profondeur. Il n'y a pas de mention du THS.
- ❒ L'origine de chaque cas de déroulement non-commandé est listée dans le document. Le déroulement non-commandé du THS n'est pas décrit.

Livre 2 :

- ❒ Aucune défaillance au niveau du HSECU n'apparaît dans l'ensemble des défaillances ou combinaison de défaillances du système de commande de vol.

Livre 3 :

- ❒ Sans objet pour le mode de défaillance étudié.

Livre 4 :

- ❒ Parmi l'ensemble des défaillances prises en compte pour effectuer l'analyse de sécurité relative au système de commandes de vol primaires, le livre 4 ne mentionne aucune défaillance du HSECU.

Ainsi, à la date de l'incident, l'analyse de sécurité faite par Dassault Equipement sur le système de commandes de vol primaires ne prévoyait pas un déroulement non-commandé en loi normale du THS. Cette absence est expliquée selon le constructeur par le fait que, lors de l'analyse de sécurité faite pour élaborer le Livre 2, il était difficile de quantifier la probabilité d'un déroulement non commandé du THS dans la mesure où les sécurités mises en place pour le HSECU, assurées par les ACMU3 et ACMU4, sont de type logiciel. Etant donné le nombre de sécurités mises en place, Dassault Aviation a considéré qu'un déroulement non commandé du THS serait détecté suffisamment tôt pour basculer sur une chaîne redondante et arrêter immédiatement le déroulement. Ainsi, la probabilité d'un déroulement non commandé du THS a été considérée comme « *extrêmement improbable* ».

Par ailleurs, les résultats de la PSSA ont conduit à qualifier d'équipements critiques[23] les modules des ACMU en charge du THS ainsi que le HSECU. A ce titre les mesures prises pour éviter une erreur de conception d'un équipement sont les plus rigoureuses (DO178 et DO254 « *Level A* ») en particulier pour ce qui concerne les activités de validation et de vérification.

[23]Equipements pour lesquels une défaillance ou un dysfonctionnement ou une erreur de conception peut avoir des conséquences catastrophiques. Ces équipements doivent bénéficier du plus haut niveau d'assurance de conception (Development Assurance Level A) conformément aux bonnes pratiques de l'époque, qui ont été par la suite formalisées dans l'ARP 4754 (guide de développement d'un aéronef civil et de ses systèmes publié par SAE).

1.17.2.4 Prises en compte des FMEA par Dassault Aviation

Les analyses de sécurité développées par Dassault prennent en compte les FMEA établies par les équipementiers. Classées comme documents de catégorie 1, les FMEA ont été envoyées pour information à l'AESA qui ne les a donc pas validées (*cf. 1.17.1.4*). Avant leur transmission à l'AESA selon les règles prévues dans le plan de certification, les FMEA ont fait l'objet de revues par des équipes de Dassault à partir des informations fournies par les équipementiers. Le but de ces revues n'est pas de refaire une analyse détaillée des conditions de panne, déjà réalisée par l'équipementier.

Note : Concernant le HSECU, les sécurités embarquées sur les cartes des ACMU prennent en compte les modes de pannes identifiés dans la FMEA du HSECU.

1.17.2.5 Documentation opérationnelle

La documentation développée par Dassault Aviation à l'attention des équipages comprend :

- le manuel de vol de l'avion ;
- un manuel d'utilisation de l'avion, le CODDE[24], composé de trois parties :
  - CODDE 1 : Description de l'avion et de ses systèmes
  - CODDE 2 : Manuel opérationnel
  - CODDE 3 :
    QRH1 : procédures normales
    QRH2 : procédures anormales et d'urgence
    ECL : Checklist électronique

[24]Crew Operational Documentation for Dassault Easy.

1.17.2.6 Programme de qualification de type Falcon 7X

Le programme de qualification de type s'attache principalement à familiariser les équipages à utiliser et exploiter l'avion en respectant les principes CRM.

Un exercice de récupération aux situations de forte assiette longitudinale à cabrer est prévu lors de deux séances de simulateurs Full Flight (FFS) sur les huit prévues lors de la qualification initiale de type.

Sur les actions de pilotage simultané, les principes de conception (alertes visuelles, tactiles et sonores, bouton des mini-manches) et de gestion de situation de pilotage simultané (coordination entre les pilotes) sont tout d'abord exposés de manière théorique. Lors d'une séance de simulateur FFS, un exercice de démonstration du fonctionnement des mini-manches en situation de pilotage simultané est effectué. La prise de commandes par un des deux pilotes est enseignée au cours d'un exercice d'incapacité « *virtuelle* » d'un des deux pilotes.

1.17.2.7 Déroulement non commandé de compensateur de profondeur

La documentation opérationnelle de Dassault Aviation (CODDE volume 2) fournit une technique opérationnelle de gestion d'un déroulement non commandé du compensateur de profondeur, disponible en annexe 1. Elle ne concerne que le cas où le compensateur de profondeur manuel est utilisé, ce qui implique que la fonction auto-trim a été préalablement perdue.

La technique décrite par Dassault Aviation précise qu'une fois la situation détectée, le PF ou le PNF doit annoncer « *TRIM RUNAWAY* ». Le PF doit alors contrer le déroulement du compensateur à l'aide du mini-manche et du compensateur de profondeur manuel.

Dassault Aviation a, depuis l'événement, mis à jour cette technique dans la documentation opérationnelle[25] (*cf. partie 5 du rapport*).

[25] CODDE Volume 2.

1.17.3 Renseignements sur Rockwell-Collins

1.17.3.1 Description générale

Rockwell-Collins est un équipementier qui ne dispose pas d'agrément de conception. Les HSECU ont été conçus par l'intermédiaire de l'agrément de conception de Dassault Aviation conformément à la Partie 21[26].

[26] Partie 21.A.239 et 21.A.243.

1.17.3.2 Développement et validation des analyses des modes de défaillance (FMEA)

Une division technique de Rockwell-Collins est chargée de la définition des spécifications et de la validation des FMEA.

Les ressources allouées au processus de développement, de vérification des FMEA et de planification des FMEA sont déterminées par cette division technique. Les principales compétences et responsabilités nécessaires selon Rockwell Collins pour un ingénieur senior impliqué dans ce processus sont les suivantes :

- connaissances dans le développement de systèmes ;
- connaissances des standards techniques tels que l'ARP4761 ;
- spécialiste dans un domaine spécifique RMS ou généraliste dans plusieurs domaines ;
- connaissances importantes du département des équipements et des systèmes ;
- capacité à :
  - organiser, analyser, concevoir, tester et documenter des produits complexes et capacité à les intégrer dans un système ;
  - estimer et suivre les coûts et les prévisions d'un projet tout en gérant les risques associés ;
  - fournir des analyses logiques et détaillées de problèmes ou de situations.

Les FMEA sont développées selon une démarche qualité de Rockwell Collins en suivant une procédure basée sur la référence technique MIL-STD-1629A et des guides internes. La procédure prévoit en particulier des révisions et des validations au fur et à mesure du développement du document. Ces revues peuvent impliquer des ingénieurs de Rockwell Collins, des représentants des clients et éventuellement des autorités de certification.

1.17.3.3 Analyse des modes de pannes du HSECU

L'ensemble des circuits du HSECU a été analysé selon le processus qualité interne de Rockwell-Collins. Dans le paragraphe *« Méthodes et procédures FMEA »* de la FMEA, il est précisé que *« tous les efforts ont été faits pour déterminer toutes les conditions potentielles de panne qui peuvent affecter la performance ou l'exploitation du HSTA »*.

La première version de FMEA du HSECU date de juillet 2004. La version en vigueur au moment de l'incident était la version C de février 2008. Elle a été développée, revue et validée par trois personnes de Rockwell Collins :

- **préparation et développement** : un ingénieur systèmes ayant six ans d'expérience dans l'élaboration d'analyses de sécurité et dans le domaine de la fiabilité, la maintenance et la sécurité des systèmes ;
- **vérification** : un ingénieur en électronique ayant 25 ans d'expérience dans la conception de systèmes électriques pour des équipements critiques ;
- **révision et validation :** un manager ayant dix ans d'expérience en fiabilité, maintenance et sécurité des systèmes dans l'industrie aérospatiale.

A partir de la FMEA et de cartes électroniques fournies par Rockwell-Collins, les équipes de Dassault Equipements ont vérifié de manière globale d'une part, que les modes de panne correspondaient à ceux habituellement retenus et d'autre part, que les effets locaux ou systèmes de ces conditions de panne apparaissaient vraisemblables. Après vérification de la cohérence documentaire, la FMEA du HSECU a été transmise pour information à l'AESA.

1.17.3.4 Conditions de panne et conséquences associées liées à l'incident grave

Les conséquences de pannes sont décrites de manière générale. De nombreuses conséquences sont mentionnées comme ayant un possible effet latent[27] ou pouvant altérer le fonctionnement du HSECU. Pour l'inductance L4, il est ainsi noté :

Type de panne	Cause de la panne	Effet local (au niveau du composant)	Effet global	Méthode de détection de la panne (A : équipage ; B : au sol)
Court-circuit	Composant endommagé, matériel dégradé, érodé	bruit	Perte de « *power boost* », bruit	« *vendor test/evaluate ; box ATP* »
Circuit ouvert	Composant endommagé, matériel dégradé, érodé	Perte de puissance liée à la tension -15VDC	Perte de l'interprétation de vitesse et de direction, « *no motor drive for actuator* »	A : perte de la chaine active (normal channel)B : « *vendor test/evaluate ; box ATP* »
Valeur fluctuante	vieillissement	Défaillance latente potentielle	Tolérances affectées ou latent	« *vendor test/evaluate ; box ATP* »

[27] Les conséquences latentes liées à une défaillance d'un composant du HSECU se retrouvent dans 162 pages de la version C de la FMEA sur 181.

Le type de panne « *valeur fluctuante* » signifie, pour le composant L4, que la valeur de son inductance[28] (en Henry) varie.

[28] L'inductance est la capacité d'un composant électrique à créer une tension à ses bornes proportionnelle à la variation de courant qui le traverse.

Dans le cas de l'incident, le circuit était partiellement ouvert du fait du défaut de brasure. Le type de panne à considérer peut correspondre aux types « *circuit ouvert* » et « *valeur fluctuante* ». Le tableau indique dans le premier cas que la conséquence est une perte de la chaîne active (chaîne 3) et que dans le deuxième cas il s'agit d'une panne latente potentielle qui a un effet global latent ou pouvant affecter les tolérances du HSECU.

Rockwell Collins donne les définitions suivantes pour les termes employés dans la FMEA :

- une « *panne latente potentielle* » d'un composant est une panne ne faisant pas l'objet d'une surveillance particulière et qui, par conséquent, peut survenir sans être détectée ;
- l'effet global « *tolérances affectées ou latent* » signifie qu'en cas de valeurs fluctuantes, il n'y a pas d'effet indésirable si les valeurs restent à l'intérieur de la plage acceptable prévue lors de la conception ; en revanche, si les valeurs fluctuantes dépassent les tolérances prévues en conception, alors le fonctionnement du composant est altéré et cela devient une panne latente.

D'une manière générale, il ressort de la FMEA que les pannes répertoriées ont essentiellement pour conséquence une perte de la chaîne active et donc un basculement de la chaîne de commande vers une chaîne redondante, ou bien sont considérées comme latentes.

1.17.3.5 Mise à jour de la FMEA après l'incident grave

Rockwell-Collins a modifié la FMEA[29] à la suite de l'incident grave en utilisant la même méthode et les mêmes références documentaires. Dans cette nouvelle version, aucune panne n'est considérée comme latente et les descriptions des effets des pannes de chaque composant ou fonction du HSECU sont plus détaillées. L'ensemble des pannes répertoriées peut générer 31 conséquences différentes sur le fonctionnement du HSECU.

Pour l'inductance L4, il est en particulier noté (les différences avec la version C de la FMEA apparaissent en rouge) :

Type de défaillance	**Cause de la défaillance**	**Effet local (au niveau du composant)**	**Effet global**	**Méthode de détection de la panne (A : équipage ; B : au sol)**
Court-circuit	Composant endommagé, matériel dégradé, érodé	-15VDC figé à 0 V	Perte du « power boost », bruit	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*
Circuit ouvert	Composant endommagé, matériel dégradé, érodé	Perte de l'alimentation -15VDC par U3	Perte de l'interprétation de vitesse et de direction, *« no motor drive for actuator »*	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*
Valeur fluctuante	vieillissement	Le pire cas considéré est une impédance additionnelle aux bornes de L4 provoquant une augmentation de la tension -15V jusqu'à des valeurs supérieures à 0V (démontré par test)	Moteur commandé de manière intempestive en survitesse ET envoi d'une vitesse erronée à l'ACMU (non figée à 0) ET signal *"Overcurrent"* figé à une valeur basse (pas de panne)	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*

[29] Version D de novembre 2011.

1.18 Renseignements supplémentaires

1.18.1 Méthodes d'analyse de sécurité

1.18.1.1 Accident survenu en Australie le 7 octobre 2008 à un Airbus A330 exploité par Qantas[30]

En croisière au FL370, l'un des trois calculateurs ADIRU[31] de l'avion envoie par intermittence aux autres systèmes embarqués des valeurs incorrectes de certains paramètres de vol, notamment d'angles d'incidence. Environ deux minutes plus tard, des protections en incidence se déclenchent et conduisent les calculateurs des commandes de vol à commander des ordres à piquer. Parmi les 303 passagers, 101 ont été blessés ainsi que 9 des 12 membres d'équipage.

L'enquête de sécurité a permis d'identifier de nombreux enseignements de sécurité concernant les analyses de sécurité des systèmes. Certains présentent des points communs avec l'incident du HB-JFN.

Les éléments contenus dans les paragraphes qui suivent sont issus des résultats de cette enquête ainsi que de plusieurs autres références documentaires.

1.18.1.2 L'analyse de sécurité au niveau système : PSSA/SSA

Les méthodes classiques d'analyse de sécurité d'un système reposent principalement sur le développement d'arbres de panne au travers des PSSA et des SSA, alimentées par les résultats des FMEA. Ces méthodes, initialement conçues pour des systèmes matériels, s'avèrent peu adaptées à des systèmes plus complexes intégrant des parties logicielles.

Pour pallier ce défaut, des méthodes dites formelles consistent à créer un modèle mathématique ou logique du système puis de l'utiliser pour réaliser automatiquement certaines tâches, dont la génération des arbres de panne.

Ce type de méthode a été employé pour l'analyse de sécurité du système de commande de vol du Falcon 7X. Il permet aux équipes en charge de la conception du système et des analyses de sécurité d'utiliser la même représentation du système et de réduire le risque d'interprétation erronée ou d'incompréhension.

Cependant, les résultats dépendent de la précision avec laquelle le modèle représente le système et l'environnement dans lequel il opère. De plus, le type de panne envisagé prend rarement en compte les phénomènes transitoires ou la temporalité d'une panne. Le nombre de résultats pouvant être fournis peut également se révéler impossible à exploiter.

Quelle que soit la méthode utilisée, l'intérêt des arbres de panne est en général d'estimer la probabilité d'un événement redouté. Or, la plupart des erreurs dans les analyses de sécurité viennent du fait que l'identification de l'ensemble des scénarios conduisant à un événement redouté n'est pas exhaustive, en particulier pour les systèmes complexes et récemment entrés en service.

[30] Le rapport final est disponible sur le site de l'ATSB au lien suivant : http://www.atsb.gov.au/publications/investigation_reports/2008/aair/ao-2008-070.aspx

[31] Air Data Inertial Reference Unit

1.18.1.3 L'analyse de sécurité au niveau d'un équipement: FMEA

La FMEA, méthode d'analyse apparue à la fin des années 1940, reste largement utilisée dans l'industrie. Elle comporte cependant les limitations suivantes :

- ❒ elle ne prend en compte que les modes de panne connus ou anticipés de composants élémentaires ;
- ❒ elle ne traite la panne ou un mode de panne que d'un composant à la fois et ne prend pas en compte des pannes plus complexes impliquant plusieurs composants ;
- ❒ elle ne garantit pas l'identification exhaustive des conséquences fonctionnelles des modes de panne;
- ❒ la qualité et l'exhaustivité d'une FMEA dépendent de la capacité de l'analyste à comprendre et anticiper le fonctionnement de l'équipement alors qu'il est en cours de développement ;
- ❒ cette méthode est conçue pour évaluer les pannes de composants électriques ou mécaniques ; elle est peu adaptée pour les systèmes complexes comprenant des parties logicielles, notamment du fait que la notion de « *panne* » est difficile à appliquer à un logiciel ou une partie de logiciel.

1.18.1.4 Méthodes alternatives

D'autres méthodes considèrent la survenue d'une panne comme étant notamment le résultat d'une incapacité du système à contrôler une perturbation de son fonctionnement. Cette perturbation peut résulter d'une défaillance d'un composant, d'une mauvaise interaction entre plusieurs parties du système ou d'une perturbation du milieu extérieur.

L'application de ces méthodes est encore limitée à l'heure actuelle.

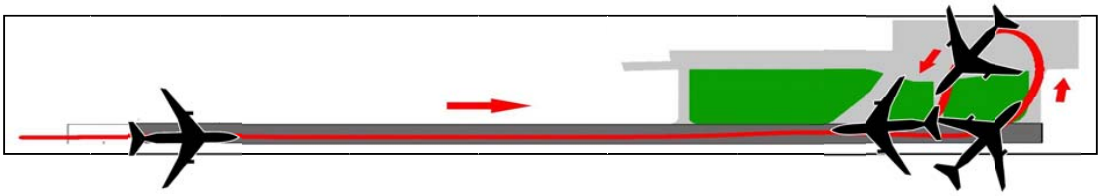
1.18.1.5 Aspects Facteurs Humains de l'analyse de sécurité

Beaucoup d'efforts ont été consacrés aux recherches sur les facteurs humains des équipages, des contrôleurs aériens ainsi que des personnels de maintenance. En revanche, le rapport de l'ATSB précise que très peu d'informations sont disponibles sur les facteurs pouvant affecter la performance humaine des personnels en charge de la conception ou des analyses de sécurité et sur les facteurs pouvant contribuer aux erreurs de conception.

Parmi les facteurs, qui peuvent avoir une influence sur la détection d'une erreur de conception ou sur la capacité à évaluer l'exhaustivité d'un arbre de panne, figurent notamment l'expérience de la personne, les informations à sa disposition, la complexité de la tâche et le fait que l'erreur par omission soit par nature plus difficile à détecter. La pression temporelle liée à l'activité de l'organisme et aux objectifs calendaires associés au programme industriel peut aussi influer sur le résultat final.

1.18.2 Accident survenu le 9 avril 2007 à un Airbus A321 exploité par Alitalia

L'équipage est autorisé à l'atterrissage à Naples (Italie) en piste 24. Le vent est calme. En raison de la masse de l'avion et de la longueur de piste disponible, le commandant de bord décide d'utiliser au maximum les inverseurs de poussée et de ne pas appliquer le freinage automatique. Au toucher des roues, un signal d'alerte sonore se déclenche et un message de dysfonctionnement du système de freinage automatique apparaît alors qu'il n'a pas été engagé. L'équipage ne ressent aucune décélération significative et annonce une situation d'urgence au contrôleur. Approchant l'extrémité de piste, le commandant de bord vire vers la gauche en utilisant la commande de direction du train avant. Compte-tenu de la trajectoire de l'avion, le pilote d'un hélicoptère en vol stationnaire sur une voie de circulation décolle et l'équipage d'un avion arrête le roulage pour éviter tout risque de collision avec l'A321. Le commandant de bord débute un virage vers la droite et l'avion s'arrête sur la piste utilisée pour l'atterrissage, dans la direction opposée.



Parmi les faits établis par l'autorité italienne responsable des enquêtes de sécurité, l'ANSV, il ressort en particulier la présence un défaut de brasure au niveau d'une broche d'un composant de type thermistance du BSCU. Ce défaut de brasure a généré des variations anormales de tension et de fait un dysfonctionnement par intermittence du BSCU.

Cet accident est un autre exemple des conséquences possibles d'un défaut de brasure. Le rapport d'enquête ne fait pas mention d'éléments relatifs aux analyses de sécurité.

1.18.3 Accident survenu le 7 janvier 2013 à un Boeing 787-8 exploité par Japan Airlines

Alors que l'avion est sur l'aire de stationnement de l'aéroport international de Boston (USA), le personnel de nettoyage découvre de la fumée en cabine arrière. Dans le même temps, un agent de maintenance dans le poste de pilotage s'aperçoit que l'APU s'est arrêtée de fonctionner automatiquement. Lors de l'ouverture du compartiment électronique arrière, de la fumée épaisse et des flammes se dégagent du couvercle de la batterie de l'APU (modèle identique aux batteries principales du Boeing 787).

Le NTSB a démontré qu'un court-circuit interne a provoqué une augmentation incontrôlable de température et de pression au niveau d'une cellule de la batterie de l'APU. Cette augmentation s'est propagée aux cellules adjacentes de la batterie et a conduit à l'apparition de fumée et de feu. Le NTSB a conclu que cet accident résultait de :

- ❒ l'absence de prise en compte par Boeing de moyens permettant d'atténuer les conséquences les plus sévères d'un court-circuit interne au sein d'une cellule de batterie d'APU et de
- ❒ l'absence d'identification par la FAA de ce défaut de conception au cours du processus de certification.

Parmi les enseignements de sécurité identifiés dans le rapport d'enquête du NTSB[32], il ressort en particulier pour les analyses de sécurité que :

- la condition de panne avérée au niveau de la batterie de l'APU lors de l'accident n'avait pas été identifiée par Boeing ni par ses sous-traitants au cours du processus d'analyse de sécurité des batteries du Boeing 787 ;
- l'hypothèse forte selon laquelle l'emballement thermique d'une cellule ne se propage pas aux cellules adjacentes n'a pas été explicitée et justifiée au cours des analyses de sécurité ;
- une approche conservatrice considérant que l'hypothèse précédente pouvait être erronée n'a pas été adoptée, contrairement à ce que prévoient les règlements de certification ;
- les deux points précédents n'ont pas été relevés par la FAA lors de la revue des analyses de sécurité.

[32] Le rapport final est disponible sur le site du NTSB au lien suivant : http://www.ntsb.gov/investigations/AccidentReports/Reports/AIR1401.pdf

1.18.4 Témoignages des pilotes

1.18.4.1 Commandant de bord

Le commandant de bord indique qu'au moment de l'événement, l'équipage est occupé par la gestion de la descente et des modes verticaux pour respecter les clairances du contrôle aérien. Le cockpit est calme, c'est la fin d'un vol de presque 12 heures, et il n'y a pas de phénomène météorologique particulier.

Lorsque l'assiette commence à augmenter, le commandant de bord se demande si ce mouvement est piloté par le PF. En le voyant actionner son mini-manche, il réalise qu'il essaie au contraire de contrer le phénomène. Il indique qu'il a instinctivement porté sa main au niveau de la console centrale, à l'endroit où se trouve le bouton « *TRIM EMERG* » sur Falcon 900, bouton permettant de reprendre le contrôle manuel du compensateur de profondeur. Il a également pris les commandes pour voir s'il arrivait à reprendre le contrôle de son côté, sans que cela n'améliore la situation.

Il précise que la prise d'inclinaison a servi à diminuer l'assiette de l'avion en attendant de trouver une solution. Il ajoute qu'il n'a jamais eu d'entraînement pour gérer les prises d'assiette longitudinale excessives.

L'absence de passager à bord a, selon lui, facilité le travail de l'équipage.

1.18.4.2 Copilote

Le copilote indique que lors de la descente, vers l'altitude de 12 500 ft, l'avion a subi un moment cabreur qualifié de « *violent* » et s'est incliné vers la droite sans aucun signe précurseur ni message CAS. Il précise que lorsque la vitesse de l'avion a atteint environ 130 kt, l'alarme sonore « *INCREASE SPEED* » s'est déclenchée. Il a essayé de contrer le moment cabreur en appliquant un effort à piquer en butée sur le mini-manche. Il explique qu'il a incliné l'avion en butée vers la droite pour réduire l'incidence et qu'il a poussé les manettes de poussée pour augmenter la vitesse. Pendant cette phase, il précise que le commandant de bord a :

- essayé d'utiliser le trim manuel ;
- tenté de réarmer les commandes de vol en appuyant sur le bouton « *PFS Engage* » du panneau supérieur ;

- appliqué des actions sur le mini-manche puisque l'alarme sonore « *DUAL INPUT* » s'est déclenchée. En réaction à cette alarme, le copilote a crié pour que le commandant arrête son action au mini-manche.

Selon le copilote, trois messages sont apparus à la fenêtre ENG-CAS :

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

Ne constatant aucune amélioration de la situation, le copilote indique qu'il a proposé au commandant de bord de prendre les commandes pour qu'il stabilise à son tour la trajectoire de l'avion. L'avion a subi un nouveau moment cabreur, plus faible que le premier, et l'altitude a atteint 24 000 ft. La diminution de vitesse associée a, de nouveau, conduit au déclenchement de l'alarme sonore « *INCREASE SPEED* ». Sur demande du commandant de bord, le copilote a essayé de réarmer les commandes de vol.

Le copilote explique que lorsque le contrôle de l'avion a été récupéré, le commandant de bord a décidé de piloter manuellement. Lors de l'approche, l'équipage a déclaré une situation d'urgence aux services de contrôle de l'aéroport de Subang.

Le copilote, de langue maternelle française, précise qu'en raison du stress généré par le moment cabreur, il a éprouvé des difficultés à expliquer en anglais ce qui se passait au commandant de bord, de langue maternelle anglaise.

Le copilote indique qu'il a incliné l'avion lors du déroulement du compensateur de profondeur par « *réflexe* » et que son expérience en tant que pilote militaire lui a été très utile pour réagir à cette situation. En effet, il explique que lorsque le déroulement du THS s'est produit, l'augmentation rapide de l'assiette longitudinale lui a rappelé une manœuvre de largage de bombes en « *palier - ressource* » qu'il a appliquée de nombreuses fois lors d'entraînements sur avion de chasse. Cette manœuvre consiste à approcher vers une cible en palier, puis à effectuer une ressource (environ 5 g et 30 degrés d'assiette longitudinale) pour lâcher la bombe à une distance d'environ 5 km de la cible. Le pilote doit ensuite virer en inclinant l'avion à plus de 90 degrés pour diminuer l'assiette et quitter la zone à très basse altitude. Lors de cette manœuvre, la pleine poussée doit être appliquée.

Le copilote précise qu'il n'a reçu au cours de sa carrière de pilote de ligne aucune formation ou entraînement spécifique à la récupération des situations inusuelles. Il indique que les situations inusuelles peuvent être évoquées en formation CRM.

1.18.5 Récupération de situations inusuelles

1.18.5.1 Manuel de récupération de situations inusuelles

De nombreux constructeurs, exploitants, organismes de formation et autorités se sont associés pour élaborer un guide de formation aux techniques de récupération de situations inusuelles[33].

D'une manière générale, la récupération d'une telle situation nécessite d'acquérir rapidement une bonne conscience de la situation pour pouvoir réagir de manière appropriée.

[33] « *Airplane Upset Recovery* », Training Aid, Revision 2 de novembre 2008.

Ainsi, en cas d'assiette longitudinale élevée et d'inclinaison faible, le manuel prévoit :

- dans un premier temps de désengager le PA et l'automanette, ainsi que d'identifier et de confirmer la situation ;
- d'appliquer ensuite un ordre à piquer de manière à obtenir une diminution de l'assiette longitudinale, ce qui peut nécessiter d'utiliser le débattement complet de la commande de profondeur ;
- puis, si les efforts à appliquer sur la commande de profondeur pour maintenir l'ordre à piquer sont importants, d'utiliser avec précaution le compensateur de profondeur de manière à diminuer ces efforts, sans pour autant piloter l'assiette au compensateur.

Si ces actions ne sont pas suffisantes, plusieurs techniques complémentaires peuvent être appliquées :

- une mise en roulis de l'avion à une inclinaison suffisante permet de diminuer l'assiette longitudinale. Maintenir l'action à piquer au cours de cette manœuvre permet d'obtenir la meilleure efficacité des ailerons. L'angle de roulis ne doit en général pas excéder 60 degrés. Si la vitesse diminue trop, le débattement complet de la commande en roulis peut être utilisé ;
- si la hauteur le permet, une réduction de la poussée peut permettre de diminuer l'augmentation de l'angle d'incidence pour les avions dont les moteurs sont sous les ailes ;
- si l'efficacité des ailerons et des spoilers n'est pas suffisante pour augmenter l'inclinaison, la gouverne de direction peut être utilisée. Une action modérée est nécessaire pour éviter une perte de contrôle en latéral.

Pour terminer la manœuvre de récupération, lorsque l'assiette longitudinale tend vers zéro degré, les ailes peuvent être remises à plat. L'assiette longitudinale doit être maintenue légèrement négative dans un premier temps pour éviter de rentrer à nouveau dans une situation inusuelle. Puis, après avoir vérifié la vitesse, la poussée et l'assiette longitudinale peuvent être ajustées si nécessaire.

1.18.5.2 Formation à la prévention et à la récupération des situations inusuelles

L'OACI a publié en 2014 un manuel de prévention et de récupération des situations inusuelles destiné aux autorités de l'aviation civile, aux organismes de formation approuvés ainsi qu'aux exploitants et à leurs équipages. L'objectif est de fournir des conseils de programmes de formation pour réduire les risques associés aux situations inusuelles en préparant les équipages à reconnaître, détecter et éviter la survenue de telles situations et en les entraînant à les récupérer de manière efficace. Les conseils donnés découlent d'une analyse d'accidents de perte de contrôle en vol. L'avant-propos du manuel précise qu'entre 2006 et 2011, les accidents d'avions résultant de pertes de contrôle représentaient la principale cause de décès en aviation commerciale.

Les conseils donnés dans le manuel reposent sur une approche de la formation qui intègre :

- une formation théorique ;
- une formation pratique sur avion ;
- une formation en simulateur multi-pilotes, dans toutes les phases de vol et dans des conditions représentatives.

Par ailleurs, le manuel définit une situation inusuelle par une situation non intentionnelle au cours de laquelle les paramètres d'un avion en vol dépassent ceux normalement attendus en exploitation ou en formation :

- assiette longitudinale supérieure à 25 degrés à cabrer, ou
- assiette longitudinale supérieure à 10 degrés à piquer, ou
- inclinaison supérieure à 45 degrés, ou
- les paramètres ci-dessus étant respectés, vitesse inappropriée pour les conditions du vol.

Depuis mars 2014, la FAA[34] a modifié les critères de formation des pilotes des exploitants aériens. La réglementation impose ainsi une modification avant mars 2019 des programmes de formation et d'entraînement pour améliorer le pilotage manuel en situation critique, dont la récupération de situations inusuelles.

[34] FAR 121.423

A la date de publication du rapport, il n'existe pas de réglementation similaire pour les exploitants des pays membres de l'Union européenne. Cependant, l'AESA a lancé en août 2013 deux tâches réglementaires (RMT[35].0581 et RMT.0582) intitulée « *formation à la prévention et à la récupération des pertes de contrôle* ». Ces tâches ont pour objectifs de développer des règlements garantissant une formation initiale et continue des pilotes adaptée à la prévention et à la récupération de pertes de contrôle. Pour cela, elles intègrent les dernières publications de l'OACI sur ce sujet et s'appuient en particulier sur les travaux réalisés par des groupes de travail internationaux[36] ainsi que sur des recommandations de sécurité d'organismes d'enquêtes.

[35] RuleMaking Task.

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

1.18.6 Evénements avec actions simultanées de pilotage

Les actions simultanées de pilotage ne sont pas spécifiques à l'équipage du HB-JFN. Plusieurs rapports d'enquêtes de sécurité mentionnent que, malgré la présence d'alertes visuelles, sonores et, comme sur le Falcon 7X, tactiles (dispositif vibreur situé dans le manche), ce type d'actions[37] peuvent avoir lieu. Elles sont principalement liées à des situations de stress et de surprise.

[37] Accident survenu en Libye en mai 2010 à un A330 exploité par Afriqiyah, incident survenu en Israël en avril 2012 à un A320 d'Air France.

Elles sont aussi parfois notifiées par les équipages. Une recherche dans la base de données d'évènements de la DGAC entre 2006 et 2013 fait ressortir 145 événements de pilotage simultané (dont aucun concernant les avions de type Falcon 7X). La plupart ont eu lieu volontairement au cours de l'arrondi à l'atterrissage pour corriger les actions au manche du PF. D'autres se sont produits lors de remises de gaz, de manœuvres d'évitement TCAS ou de turbulences.

Le principe de l'OSD[38], qui demande aux constructeurs d'aéronefs de fournir un certain nombre de données, a été introduit dans la réglementation en 2014 dans le but de mieux prendre en compte les particularités de conception de chaque aéronef dans la formation des équipages et l'exploitation.

[38] Operational Suitability Data.

2 - ANALYSE

2.1 Scénario

Un défaut de brasure au niveau d'une broche d'une inductance du HSECU a conduit ce calculateur à envoyer des ordres erronés à cabrer au moteur actionnant le THS, et à fournir aux systèmes en charge de la surveillance de son fonctionnement des valeurs erronées indiquant une évolution à piquer de cette gouverne. Aucun système n'a détecté ces erreurs qui ont eu pour conséquence le déroulement en butée à cabrer du THS lors de la descente vers l'aéroport de Subang.

L'effet immédiat du déroulement du THS a été une forte augmentation de l'assiette longitudinale. L'équipage n'avait aucun moyen à sa disposition en loi normale pour modifier la position du THS.

Les actions réflexes du PF, cohérentes avec les manœuvres de récupération des situations à forte assiette longitudinale, ont permis de stabiliser l'avion malgré cette position. Le maintien d'une forte inclinaison a permis de stabiliser l'assiette longitudinale.

Le commandant de bord a aussi effectué des actions simultanées de pilotage opposées à celles du PF en roulis pendant deux périodes d'environ dix secondes chacune. Ces actions simultanées ont eu pour effet de diminuer l'inclinaison et, de ce fait, d'augmenter à nouveau l'assiette longitudinale. L'équipage a perçu ces situations de pilotage simultané et les a gérées par prise de priorité puis par transfert des commandes.

Environ deux minutes après le déroulement du THS, une surveillance en température du calculateur du système de commandes de vol (ACMU) a permis le basculement vers une chaîne de commandes redondante et par conséquent le retour à un fonctionnement normal du THS.

2.2 Production des équipements

Des microfissures au niveau de la brasure de l'inductance ont conduit au déroulement du THS. Ce défaut de brasure résulte d'un défaut de production qui n'a pas été détecté au cours du processus de production du HSECU. L'origine de ce défaut provient d'un isolement thermique insuffisant entre le trou métallisé et le plan de masse de la carte.

L'accident survenu en 2007 à un Airbus A321 exploité par Alitalia (*cf 1.18.2*) est un autre exemple des conséquences possibles d'un défaut unique de brasure sur une broche d'un seul composant.

2.3 Analyses de sécurité

2.3.1 Défaillance d'un seul composant

Le défaut de brasure d'une broche de l'inductance L4 du HSECU a modifié l'impédance de ce composant et conduit au déroulement non-commandé du THS (*cf. 1.16.2*). Or, le déroulement non-commandé d'une gouverne primaire, considéré comme une panne, qui ne permet pas de poursuivre le vol en sécurité, ne doit donc pas résulter d'une défaillance d'un seul élément ou composant (*cf. 1.17.1.3*) ou d'une combinaison de pannes qui ne serait pas extrêmement improbable.

Les conséquences possibles de la panne d'un composant d'un équipement sont normalement décrites et détaillées dans la FMEA de l'équipement concerné. Celle du HSECU envisageait le cas de panne correspondant à un défaut de brasure au niveau de l'inductance L4 comme potentiellement latent. Ses effets n'étaient donc pas considérés comme visibles au niveau du HSECU. D'une manière générale, une grande majorité de pannes était décrite comme latente par Rockwell-Collins dans la FMEA du HSECU.

L'estimation imprécise des effets sur le HSECU de pannes de ses composants, et en particulier de la panne constatée sur l'inductance L4, a ainsi limité l'évaluation de ses effets dans l'analyse de sécurité.

2.3.2 Limites dans l'élaboration des FMEA

Les conséquences d'une panne de l'inductance L4 présentant un défaut de brasure ont été nettement sous-estimées dans la FMEA du HSECU. En effet, les conséquences d'une valeur fluctuante de l'inductance de ce composant étaient considérées comme « *potentiellement* » latentes alors qu'elles avaient des effets significatifs sur le fonctionnement du HSECU, du système de commandes de vol et donc sur le contrôle en vol de l'avion.

Les FMEA sont des outils utilisés depuis de nombreuses années dans la conception d'équipements aéronautiques. L'élaboration des FMEA s'appuie sur des standards techniques (*cf. 1.17.1.5*) et des procédures propres à chaque équipementier. Toutefois, l'accident survenu en Australie le 7 octobre 2008 à un Airbus A330 exploité par Qantas (*cf. 1.18.1*) ainsi que cet incident grave montrent certaines limites dans le processus d'élaboration, de vérification et de validation des FMEA.

2.3.2.1 Le processus d'élaboration des FMEA

Dans le cas du HSECU, il a fallu trois mois d'analyse pour déterminer l'effet de la panne du composant L4 sur le comportement de la chaîne de commande du THS. A la suite de cet événement, Rockwell-Collins a mis à jour de manière complète la FMEA du HSECU en utilisant les mêmes méthodes et références documentaires. Il s'avère que cette FMEA mise à jour présente des résultats différents de la version en vigueur au moment de l'incident grave (*cf. 1.17.3.4 et 1.17.3.5*). Cela illustre la difficulté d'estimation a priori des conséquences d'une panne d'un composant. Malgré l'utilisation de procédures identiques, il subsiste une certaine variabilité, et par conséquent une incertitude, sur les résultats de ce type de document qui constitue pourtant l'une des bases du processus d'analyse de sécurité des systèmes. De même, l'ATSB a identifié à la suite de l'accident survenu en Australie le 7 octobre 2008 à un Airbus A330 exploité par Qantas que les FMEA ne permettaient pas systématiquement de déterminer de manière exhaustive l'ensemble des scénarios pouvant conduire à une panne donnée au niveau avion. Ces deux exemples montrent certaines limitations des FMEA et témoignent d'une certaine fragilité du système.

Ces limitations peuvent s'expliquer par :

- des facteurs humains tels que la dépendance à l'expérience, la formation ou la charge de travail des analystes ;
- des facteurs organisationnels tels que les ressources humaines allouées à l'élaboration d'une FMEA ou la pression temporelle dans le processus de développement industriel et de certification ;
- des facteurs intrinsèques aux FMEA dans la mesure où notamment ce type d'analyse ne prend en compte que les modes de panne connus ou anticipés et ne traite pas les pannes impliquant plusieurs composants. Par ailleurs les FMEA, développées à la fin des années 1940 pour l'analyse d'équipements électriques et mécaniques simples, peuvent se révéler inadaptées pour l'analyse d'équipements complexes, notamment ceux incluant des calculateurs numériques.

2.3.2.2 La vérification et la validation des FMEA

Dans le cadre de la certification de type, les organismes de conception doivent préciser les méthodes pour déterminer l'acceptabilité des équipements conçus par des sous-traitants et des taches effectuées par ceux-ci. Ainsi, Dassault Aviation n'a pas refait de manière exhaustive la FMEA du HSECU pour la confronter avec celle de Rockwell Collins mais a effectué un contrôle général de ces résultats à partir des informations à sa disposition. Par ailleurs, l'AESA ne vérifie pas le contenu des FMEA dans la mesure où elles ne font pas partie des documents devant être acceptés, car elle s'appuie pour cela sur l'agrément de conception de l'avionneur. D'une manière générale, ni l'avionneur ni l'AESA ne disposent des moyens et des compétences techniques nécessaires pour assurer eux-mêmes une vérification et une validation détaillées des FMEA de l'ensemble des équipements présents dans un aéronef. Par conséquent, seuls les équipementiers sont à même de vérifier en détail et de valider les résultats des FMEA.

Ainsi, les résultats des FMEA peuvent dépendre uniquement des procédures internes mises en place par les équipementiers, même pour des équipements critiques et pour lesquels une erreur de conception ou un dysfonctionnement non prévu pourrait conduire à une condition de panne catastrophique au niveau avion. Ainsi pour le HSECU du Falcon 7X, équipement identifié comme critique, le processus d'élaboration, de vérification et de validation de la FMEA a reposé uniquement sur l'expérience de trois personnes de Rockwell-Collins.

Dans ce contexte, des erreurs dans une FMEA peuvent conduire à l'élaboration d'analyses de sécurité qui, bien qu'erronées, permettent de démontrer le respect des exigences de certification. Ces erreurs de conception « *latentes* » peuvent avoir des conséquences directes sur l'exploitation des aéronefs puisqu'elles ont un impact direct et pratique sur la sécurité des systèmes, les procédures (opérationnelles et de maintenance) ainsi que sur la formation des équipages et des agents de maintenance. Cet incident et l'accident survenu en Australie (*cf. 1.18.1.1*) sont deux exemples qui illustrent la manifestation de ces erreurs latentes.

2.3.3 Limites des SSA et surveillances mises en jeu

L'analyse de sécurité (SSA) faite par Dassault Aviation sur le système de commandes de vol primaires a pris en compte les résultats de la FMEA du HSECU après avoir vérifié certains modes de pannes. Au-delà des conséquences de la panne de l'inductance estimées comme « *potentiellement* » latentes, le nombre de résultats similaires dans cette FMEA a conduit à ne faire apparaître le HSECU dans aucune des conditions de panne décrites dans la SSA pour le système de commandes de vol du Falcon 7X.

Ainsi, le déroulement non commandé du THS en loi normale apparaît dans le document de synthèse de l'analyse de sécurité mais pas dans les documents présentant les résultats plus détaillés par mode de panne (*Livre 1 et Livre 2, cf 1.17.2.2*). Ceci n'a pas été remis en question par Dassault Aviation, qui a validé la SSA du système de commande de vol, ni par l'AESA qui a accepté cette SSA sur la base de sa validation par Dassault Aviation.

Les résultats de la SSA du système de commandes de vol primaires ont eu des conséquences sur le développement des surveillances associées au système de commande du THS. Ainsi, au moment de l'incident, le système de commande du THS était conçu de telle sorte que la fonction de surveillance, assurée par l'ACMU, dépendait entièrement du boîtier de contrôle de la gouverne, à savoir le HSECU, pour détecter un déroulement non commandé du THS provoqué par un dysfonctionnement du HSECU. Cette architecture ne garantissait ni la détection d'un dysfonctionnement du boîtier de contrôle ni la reconfiguration vers une autre chaîne de contrôle par un moyen indépendant. Ceci a permis à une panne simple de provoquer le déroulement du THS, considéré comme catastrophique. Ce type d'architecture répond toutefois aux exigences réglementaires qui ne demandent pas explicitement une indépendance entre les chaînes de surveillance et de contrôle. L'ensemble de la chaîne de commande du THS est pourtant un système considéré comme critique car impliqué dans plusieurs modes de panne catastrophiques tels que le déroulement non commandé d'une gouverne primaire.

Ainsi, le plus haut niveau d'assurance conception (DAL A) a été attribué aux modules des ACMU en charge du THS ainsi qu'au HSECU. Les niveaux de vérification et de validation tout au long du processus de conception et d'analyse de sécurité étaient donc normalement les plus élevés, mais n'ont pas permis d'identifier les modes de défaillances critiques du HSECU, ni d'anticiper l'apparition d'un déroulement non commandé du THS en loi normale.

L'incident grave révèle donc, pour un système complexe tel que le système de commande de vol primaire, la vulnérabilité du processus d'analyse de sécurité aux erreurs ou difficultés pouvant survenir aux différentes étapes du processus :

- élaboration et validation de la FMEA d'un équipement par un équipementier ;
- capacité de maîtrise et de surveillance d'un organisme de conception lors de la conception d'équipements, et notamment d'équipements considérés comme critiques par des partenaires ou sous-traitants ;
- validation d'une SSA par un organisme de conception ;
- acceptation par l'autorité en charge de la certification.

Les accidents survenus en Australie (*cf. 1.18.1.1*) et aux Etats-Unis (*cf. 1.18.3*) confirment que les processus d'analyse de sécurité peuvent ne pas anticiper la survenue de conditions de pannes non identifiées lors de la conception, aux conséquences potentiellement catastrophiques, en particulier lorsqu'il s'agit de systèmes complexes ou de technologies nouvelles.

2.4 Récupération aux situations inusuelles

L'exposition des équipages à des situations inusuelles est rare, tant en formation qu'en exploitation. La récupération du contrôle de l'avion nécessite d'identifier rapidement et de maîtriser les techniques de récupération appropriées. Dans le cas de l'événement, l'expérience antérieure dans l'Armée de l'air française du copilote a été le facteur déterminant pour récupérer temporairement le contrôle de l'avion alors que l'assiette longitudinale avait fortement augmenté à la suite du déroulement non-commandé du THS en loi normale. Cette réaction s'apparente à un réflexe lié à l'augmentation de l'assiette longitudinale qui a pu être favorisé par la répétition de manœuvres similaires sur avion d'armes. Par ailleurs, la technique opérationnelle décrite dans la documentation de Dassault Aviation en vigueur au moment de l'événement n'était pas adaptée lorsque la fonction auto-trim était disponible et active.

Le constat dressé sur les accidents de perte de contrôle et les situations inusuelles dans le manuel de l'OACI (*cf. 1.18.4.2*) tend à montrer que les actions du copilote qui a augmenté l'assiette longitudinale représentent une réponse souhaitée mais pas générique de la part d'un pilote de ligne. D'une manière générale, ce constat associé au contenu insuffisant de la formation actuelle des pilotes ne permet pas de garantir la construction et le maintien de compétences nécessaires à la récupération de situations inusuelles. La formation des équipages à la récupération de situations inusuelles fait d'ailleurs l'objet d'initiatives d'organismes tels que l'OACI, l'AESA ou la FAA.

2.5 Actions simultanées de pilotage

Le déroulement du THS a généré deux situations de pilotage simultané en moins de trois minutes, chacune ayant duré environ dix secondes. Ces situations peuvent s'expliquer par :

- la forte charge émotionnelle associée à l'effet de surprise ;
- la soudaineté et l'amplitude de la perturbation liée au déroulement du THS ;
- l'incompréhension de la situation, surtout lors de la phase du déroulement du THS ;
- l'absence d'exposition de l'équipage à ce type de phénomène, tant en formation qu'en exploitation ;
- la faible expérience des deux pilotes sur avions équipés de mini-manches.

L'absence d'enregistrement phonique de l'événement n'a pas permis d'analyser précisément la gestion par l'équipage de ces deux situations de pilotage simultané. Toutefois, l'analyse des paramètres et des témoignages de l'équipage apporte les éléments suivants :

- la gestion par l'équipage des deux phases de pilotage simultané a permis la reprise de contrôle par un des pilotes dans une période de sept à onze secondes ;
- la gestion par l'équipage des deux phases de pilotage simultané s'est faite grâce aux dispositifs visuels et tactiles d'indication de pilotage simultané puis de prise de priorité des commandes au mini-manche. Ces dispositifs ont ainsi suffi à l'équipage pour identifier les phases de pilotage simultané et les gérer.

Les actions simultanées de pilotage sur avions équipés de mini-manches ne sont pas des événements isolés. Même si l'ergonomie associée aux actions simultanées de pilotage sur avions équipés de mini-manches (vibrations du mini-manche, alarmes sonore et visuelle) doit permettre de gérer ce type de situation, comme le montre cet incident, la formation reçue par les équipages sur ce sujet reste succincte. Il apparaît notamment que le scénario utilisé en formation de qualification de type (incapacité d'un des deux pilotes) est peu représentatif des situations de pilotage simultané couramment rencontrées (*cf. 1.17.2.6 et 1.18.5*).

3 - CONCLUSION

3.1 Faits établis par l'enquête

- l'incident grave s'est produit dans le cadre d'un vol de convoyage ;
- l'équipage détenait les licences et qualifications nécessaires pour effectuer le vol ;
- l'avion avait un certificat de navigabilité en état de validité ; il était entretenu conformément à la réglementation ;
- la masse et le centrage de l'avion se trouvaient à l'intérieur des limites opérationnelles ;
- l'avion avait décollé de Nuremberg sans problème technique connu ;
- une broche d'un composant du calculateur HSECU présentait un défaut de brasure ;
- le défaut de brasure n'a pas été détecté lors de la production du HSECU ;
- lors de la descente vers l'aérodrome de destination, à une altitude d'environ 13 000 ft, le THS est passé en quinze secondes de sa position au neutre à sa butée à cabrer ;
- le PF a repris les commandes et appliqué des ordres en butée à piquer ;
- les ordres à piquer appliqués par le PF étant inefficaces, celui-ci a exécuté une manœuvre de récupération en inclinant l'avion sur la droite jusqu'à 98 degrés d'inclinaison initialement ;
- le PF avait réalisé ce type de manœuvre à de nombreuses reprises au cours de sa carrière militaire ;
- cette manœuvre, transformant la ressource en virage, a permis de retrouver temporairement le contrôle en tangage de l'avion malgré une position du THS en butée à cabrer puis de stabiliser l'attitude de l'avion et sa vitesse ;
- une surveillance de la température du moteur actionnant le THS a déclenché le changement de chaîne de commande du THS ; le contrôle de l'avion en tangage par les actions au mini-manche est alors redevenu possible ;

- entre le début du mouvement à cabrer du THS et son retour en position d'équilibre, il s'est écoulé 2 minutes et 36 secondes. Pendant cette période, le facteur de charge a atteint 4,6 g ; l'altitude est passée de 13 000 à 22 500 ft ; la vitesse conventionnelle a évolué entre 300 et 125 kt ; l'assiette longitudinale a atteint 41 degrés ;
- au cours de l'événement, des actions simultanées de pilotage ont été exercées par l'équipage durant deux périodes de neuf et douze secondes respectivement ;
- ces phases d'actions simultanées de pilotage ont été gérées à l'aide des dispositifs d'indication visuelle, sonore et tactile, et des dispositifs de prise de priorité des commandes au mini-manche ;
- aucun événement significatif n'a eu lieu avant le déroulement non commandé du THS ;
- l'estimation des conséquences du type de défaillance correspondant à un défaut de brasure de l'inductance L4 était erronée dans la FMEA du HSECU ;
- les processus de vérification et de validation de la FMEA réalisés par l'équipementier et le constructeur n'ont pas permis de détecter cette erreur ;
- le plus haut niveau d'assurance conception (DAL A) a été attribué aux modules des ACMU en charge du THS ainsi qu'au HSECU ;
- les FMEA ne faisaient pas partie des documents à accepter par l'AESA lors de la certification de type du Falcon 7X ;
- l'architecture du système de contrôle du THS était telle que la fonction de surveillance de la chaîne de commande et du bon fonctionnement du HSECU réalisée par l'ACMU dépendait de paramètres élaborés par le HSECU en charge du contrôle du THS.

3.2 Causes de l'incident grave

Un défaut de brasure au niveau d'une broche d'un composant du HSECU a conduit ce calculateur à envoyer des ordres erronés à cabrer au moteur actionnant le THS, et à fournir aux systèmes en charge de la surveillance de son fonctionnement des valeurs erronées indiquant une évolution à piquer de cette gouverne. Ce défaut unique a ainsi conduit à des défaillances simultanées sur les chaînes de contrôle et de surveillance du THS qui n'ont été détectées par aucun système et qui ont suffi pour provoquer le déroulement non commandé du THS en loi normale.

Les facteurs suivants ont contribué à l'incident grave :

- un défaut de production et l'absence de détection de ce défaut avant la mise en service du HSECU ;
- l'évaluation imprécise des conséquences des types de panne considérés dans la FMEA du HSECU, la validation de cette FMEA et d'une manière générale la variabilité des résultats fournis par une FMEA, qui peuvent dépendre de facteurs humains et organisationnels propres à l'équipementier ;
- l'absence de moyens de détection d'éventuelles erreurs dans les FMEA d'équipements considérés comme critiques au cours du processus d'analyse de sécurité et de certification de l'avion, les FMEA ne faisant pas l'objet d'une vérification détaillée par l'avionneur ou par l'AESA ;

- les limites du processus de vérification par l'avionneur de la SSA et les limites du processus de son acceptation par l'AESA, dans la mesure où la synthèse de cette SSA mentionnait le déroulement non commandé de THS en loi normale alors qu'aucune combinaison de pannes pouvant conduire à un tel déroulement ne figurait dans les résultats détaillés, et bien que le HSECU ait été identifié comme un équipement critique pour lequel un dysfonctionnement ou une erreur de conception peuvent conduire à une situation catastrophique ;
- l'architecture du système de commande du THS dont les chaînes de surveillance et de contrôle dépendaient l'une de l'autre, empêchant, dans le cas de l'événement, la détection du dysfonctionnement du HSECU et la reconfiguration vers une chaîne de commande redondante.

Ainsi, cet événement met en défaut des dispositions sensées répondre à l'exigence réglementaire de certification selon laquelle une défaillance unique d'un élément d'un système ou d'un équipement au cours d'un vol ne devrait pas conduire à un déroulement non commandé d'une commande de vol primaire vers une position indésirable.

Le déroulement non commandé du THS en loi normale, événement qui ne fait pas l'objet de procédure particulière ou de formation pour les équipages, a été soudain et de forte amplitude. Malgré l'effet de surprise, l'équipage a pu récupérer et conserver le contrôle de l'avion avec le THS en butée à cabrer par :

- l'application immédiate et adaptée d'une technique de récupération des situations avec des prises d'assiettes excessives qui s'explique par la formation et l'entraînement reçus par le PF au cours de sa carrière militaire ;
- la coordination entre les deux membres d'équipage qui a permis d'assurer et de conserver la répartition des tâches jusqu'au retour à des conditions de vol normales malgré l'application à deux reprises d'actions simultanées de pilotage sur leur mini-manche.

Le déclenchement d'une surveillance en température deux à trois minutes après le début du déroulement du THS a permis de récupérer la pilotabilité de l'avion jusqu'à la fin du vol en basculant vers une chaîne de commande fonctionnelle et, par conséquent, en retrouvant l'équilibre en tangage.

4 - RECOMMANDATIONS DE SECURITE

Rappel : conformément aux dispositions de l'article 17.3 du règlement n° 996/2010 du Parlement européen et du Conseil du 20 octobre 2010 sur les enquêtes et la prévention des accidents et des incidents dans l'aviation civile, une recommandation de sécurité ne constitue en aucun cas une présomption de faute ou de responsabilité dans un accident, un incident grave ou un incident. Les destinataires des recommandations de sécurité rendent compte à l'autorité responsable des enquêtes de sécurité qui les a émises, des mesures prises ou à l'étude pour assurer leur mise en œuvre, dans les conditions prévues par l'article 18 du règlement précité.

4.1 Méthodes complémentaires aux FMEA

L'enquête, au travers de l'incident grave survenu au Dassault Falcon 7X exploité par JetLink et immatriculé HB-JFN tend à montrer que les moyens permettant de détecter les erreurs qui pourraient figurer dans des analyses de mode de défaillances et de leurs effets (FMEA) sont insuffisants, notamment lorsqu'il s'agit d'équipements considérés comme critiques. Ce constat s'appuie sur d'autres accidents. Elle présente également les limites des FMEA qui, s'ils sont bien adaptés aux systèmes simples et aux défaillances matérielles pour lesquels ils ont été créés il y a plusieurs décennies, paraissent moins efficaces pour des équipements électroniques ou logiciels.

C'est pourquoi le BEA recommande que :

- **L'AESA, en coordination avec la FAA, la SAE et EUROCAE[39], évalue et propose des méthodes alternatives ou complémentaires aux FMEA pour les équipements électroniques et logiciels. [Recommandation 2016-002]**

- **la FAA, en coordination avec l'AESA et la SAE et EUROCAE, évalue et propose des méthodes alternatives ou complémentaires aux FMEA pour les équipements électroniques et logiciels. [Recommandation 2016-003]**

[39] Acronyme de EURopean Organisation for Civil Aviation Equipment, organisme européen établissant des règles de standardisation des systèmes utilisés par l'aviation civile.

4.2 Indépendance entre chaînes de commande et de surveillance

L'indépendance entre des chaînes de commande et de surveillance ainsi que la vérification de cette indépendance constituent des éléments clés de la sécurité d'un système. Elles ne sont pas explicitement exigées par les spécifications de certification. Certaines erreurs qui peuvent exister dans les analyses de sécurité sont difficiles, voire impossibles à détecter à partir des standards techniques disponibles, que ce soit lors de leur vérification et validation par l'organisme de conception ou lors de leur acceptation par les autorités en charge de la certification. Dans le cas de cet incident grave, un simple défaut de brasure a suffi pour provoquer des défaillances non détectées sur ces deux chaînes et le déroulement non-commandé d'une commande de vol primaire vers une position indésirable. C'est pourquoi le BEA recommande que :

- **L'AESA, en coordination avec la FAA, la SAE et EUROCAE, développe des moyens ou méthodes permettant de consolider lors des analyses de sécurité les vérifications de l'indépendance entre les chaînes de commande et de surveillance d'un système. [Recommandation 2016-004]**

- **la FAA, en coordination avec l'AESA, la SAE et EUROCAE, développe des moyens ou méthodes permettant de consolider lors des analyses de sécurité les vérifications de l'indépendance entre les chaînes de commande et de surveillance d'un système. [Recommandation 2016-005]**

4.3 Entraînement à la prise de priorité sur avions équipés de manches non conjugués mécaniquement

L'enquête a montré que l'entraînement à la reprise des commandes sur manches non conjugués mécaniquement tel qu'il est effectué actuellement lors de la formation initiale et en entraînement périodique ne permet pas de garantir le maintien de compétence des équipages dans ce domaine. Il apparaît alors nécessaire, dans le cadre des OSD de prendre en compte les procédures spécifiques relatives à la reprise de commandes sur les aéronefs équipés de manches non conjugués.

Ce constat a également été fait lors de l'enquête relative à l'accident survenu le 29 mars 2013 à Lyon Saint-Exupéry (69) à l'Airbus A321 immatriculé SX-BHS exploité par Hermes Airlines et affrété par Air Méditerranée[40]et pour lequel le BEA a recommandé que :

- ***« l'AESA, en coordination avec les constructeurs, s'assure que les futurs programmes définis dans le cadre des OSD comportent une formation initiale et des entraînements périodiques à la prise de priorité sur avions équipés de manches non conjugués. [Recommandation 2015-024] »***

[40]http://www.bea.aero/docspa/2013/sx-s130329/pdf/sx-s130329.pdf

5 - MESURES PRISES DEPUIS L'ÉVÉNEMENT

Cet incident a conduit l'équipementier et le constructeur de l'avion à prendre un certain nombre de mesures de sécurité.

5.1 Mesures prises par Rockwell-Collins

■ Analyse de sécurité

La FMEA[41] a été mise à jour à la suite de l'incident selon la même approche et les mêmes références documentaires. Elle fait apparaître des descriptions plus détaillées des effets des pannes de chaque composant ou fonction du HSECU. Pour l'inductance dont la brasure était défectueuse, les différences entre cette nouvelle FMEA et celle en vigueur à la date de l'incident grave sont notées en rouge dans le tableau suivant :

[41]Version D de novembre 2011.

Type de défaillance	Cause de la défaillance	Effet local (au niveau du composant)	Effet global	Méthode de détection de la panne (A : équipage B : au sol)
Court-circuit	Composant endommagé, matériel dégradé, érodé	-15VDC figé à 0 V	Commande intempestive du moteur en survitesse ET Vitesse érronée renvoyée à l'ACMU (figée à 0).	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*
Circuit ouvert	Composant endommagé, matériel dégradé, érodé	Perte de l'alimentatjon -15 VDC	Commande intempestive du moteur en survitesse ET Vitesse érronée renvoyée à l'ACMU (non figée à 0) ET sortie OverCurrent figée en valeur basse (no fault).	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*
Valeur fluctuante	vieillissement	Le pire cas considéré est une impédance additionelle aux bornes de L4 provoquant une augmentation de -15 V au dela de 0V (démontré par tests)	Commande intempestive du moteur en survitesse ET Vitesse érronée renvoyée à l'ACMU (non figée à 0) ET sortie OverCurrent figée en valeur basse (no fault).	A : Mouvement non commandé de l'actionneur, détectable par des capteurs de positions externes B : *« vendor test/ evaluate ; box ATP »*

Rockwell-Collins a modifié la FMEA du HSECU. Dans cette nouvelle version, aucune panne n'est considérée comme latente et trente-et-une conditions de panne différentes sont répertoriées (dans la version en vigueur à la date de l'incident, seul un basculement de la chaîne de commande était considéré).

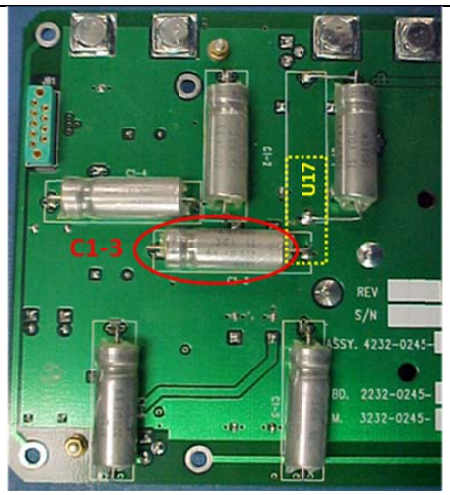
■ Contrôles de la production

Un examen aux rayons X des cartes électroniques a été rajouté par Rockwell-Collins dans le processus de production des HSECU après l'étape de soudure des composants afin de détecter les éventuelles brasures froides.

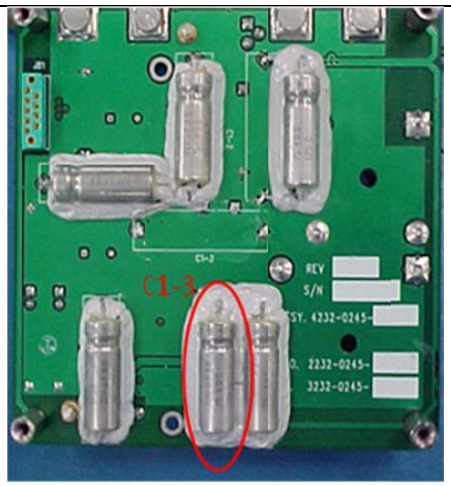
■ Modification du design des cartes électroniques

Durant la phase de recherche de l'origine de la panne, les examens des cartes électroniques du HSECU ont révélé que deux composants situés sur des cartes électroniques adjacentes entraient en contact physique l'un avec l'autre.

Ce défaut était présent uniquement sur les HSECU de modèle 051244-04. Même si cela n'a pas contribué à l'événement, une nouvelle version du HSECU (051244-05) a donc été élaborée par Rockwell-Collins dans laquelle un des deux composants a été déplacé :



HSECU P/N 051244-04 (ancien modèle)



HSECU P/N 051244-05 (nouveau modèle)

Source Dassault Aviation

Par ailleurs, à la demande de Dassault Aviation, Rockwell-Collins a également ajouté :

- une pastille isolante pour isoler thermiquement le trou métallisé du plan de masse de la carte électronique pour favoriser l'élévation de température au moment du brasage de l'inductance L4 ;
- dans le HSECU une surveillance de la tension délivrée par les alimentations internes, de manière à ce que toute tension délivrée en dehors des tolérances conduise à désactiver la chaine de commande et par conséquent déclencher le basculement vers une chaîne redondante par l'ACMU.

5.2 Mesures prises par Dassault-Aviation

Alors que l'origine du problème était encore inconnue, l'action immédiate prise par Dassault Aviation après l'événement a été de demander à l'AESA la suspension temporaire des vols de l'ensemble de la flotte de Falcon 7X qui a fait l'objet de l'émission d'une consigne de navigabilité.

Les actions suivantes ont ensuite été entreprises par Dassault Aviation pour remettre progressivement la flotte en service :

Conception et certification

L'origine du problème ayant causé le déroulement du compensateur de profondeur n'étant pas connue, les premières modifications ont consisté à :

- **Mod 1236**[42] : introduire une fonction supplémentaire de surveillance, qui ne fait plus appel à l'information de vitesse de rotation du moteur du THS qui est assurée par le système de commande de vol, indépendante du HSECU ;

[42] 16 juin 2011.

- **Mod 1235**[43] : installer un bouton poussoir dans le poste de pilotage pour permettre aux pilotes le passage forcé du système de commandes de vol sur le système de secours (BACK-UP, cf. Fonctionnement du système de compensateur de profondeur) et de pouvoir contrôler manuellement le compensateur de profondeur ;
- **Mod 1239**[44] : supprimer des interférences mécaniques potentielles entre les composants du HSECU.

[43] 16 juin 2011.

[44] 07 juillet 2011.

La mise en place des modifications 1235 et 1236 ainsi qu'une vérification du HSECU de chaque avion ont permis de reprendre l'exploitation de la flotte avec une restriction du domaine de vol à haute vitesse du fait du temps nécessaire au déclenchement de la nouvelle surveillance.

Une modification (mod 1245[45]) a ensuite été introduite pour permettre le retour de l'ensemble des vols dans toute l'enveloppe de vol. Elle comprend des modifications logicielles pour améliorer la surveillance, notamment en introduisant une surveillance de la vitesse du THS, et améliorer la logique de réversion en permettant en particulier une détection plus rapide d'un éventuel déroulement de compensateur de profondeur.

[45] 29 août 2011.

Chacune de ces étapes a été suivie et approuvée par l'AESA et diffusée sur l'ensemble de la flotte des Falcon 7X par l'intermédiaire de consignes de navigabilité.

Dassault Aviation a également revu les analyses de sécurité des systèmes de commandes de vol en prenant en compte la mise à jour de la FMEA des HSECU.

Exploitation

Des permis de vol avec limitations ont été émis pour permettre une mise en service progressive de la flotte des Falcon 7X en fonction des modifications décrites ci-dessus. Les exploitants ont été informés par l'intermédiaire de forums, de lettres d'informations et d'un module de formation pour les pilotes.

Les manuels de vol et de maintenance ont été mis à jour et les centres de formation ont reçu les informations nécessaires au niveau de la documentation et des modifications à appliquer aux simulateurs.

Liste des annexes

annexe 1

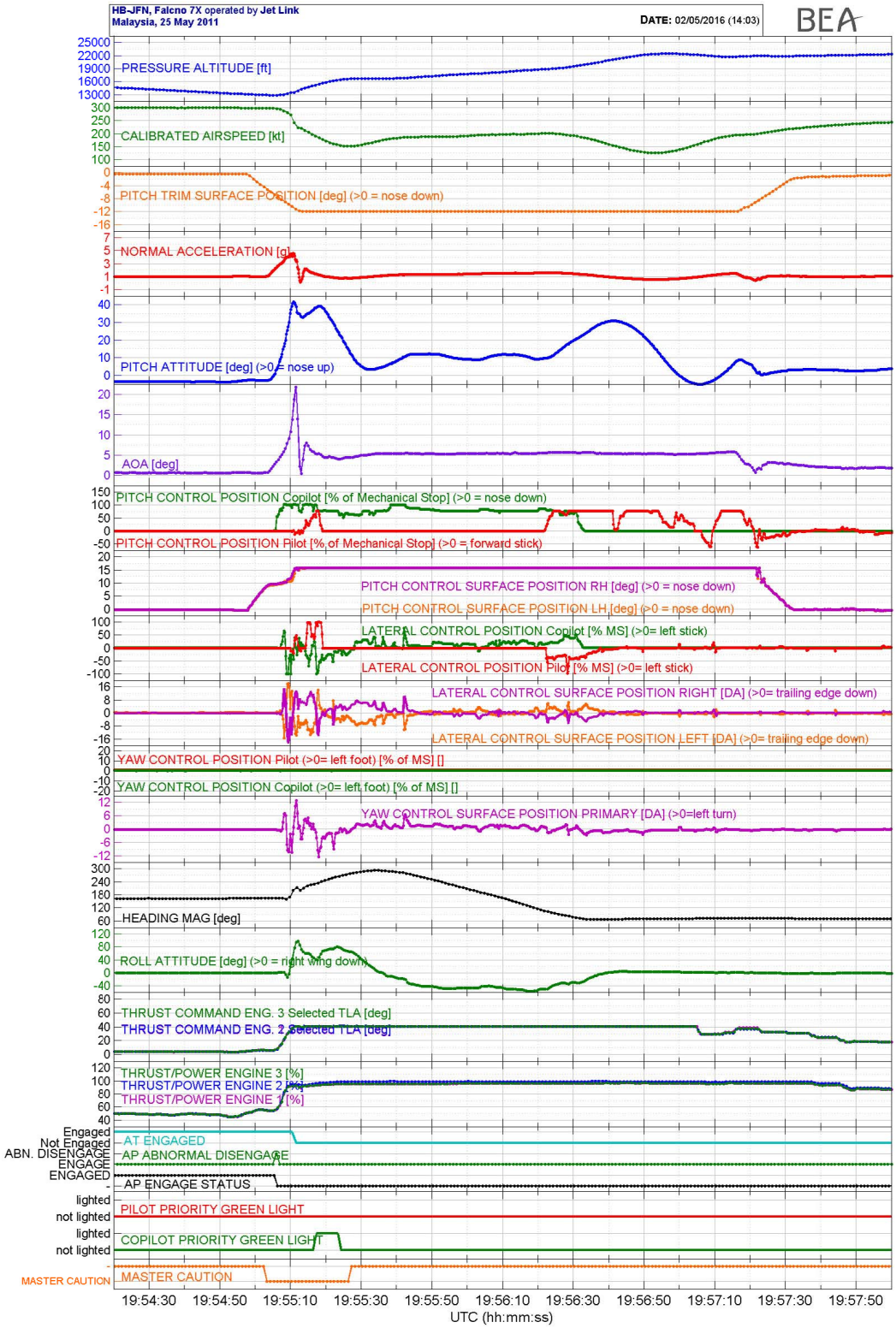
Paramètres FDR

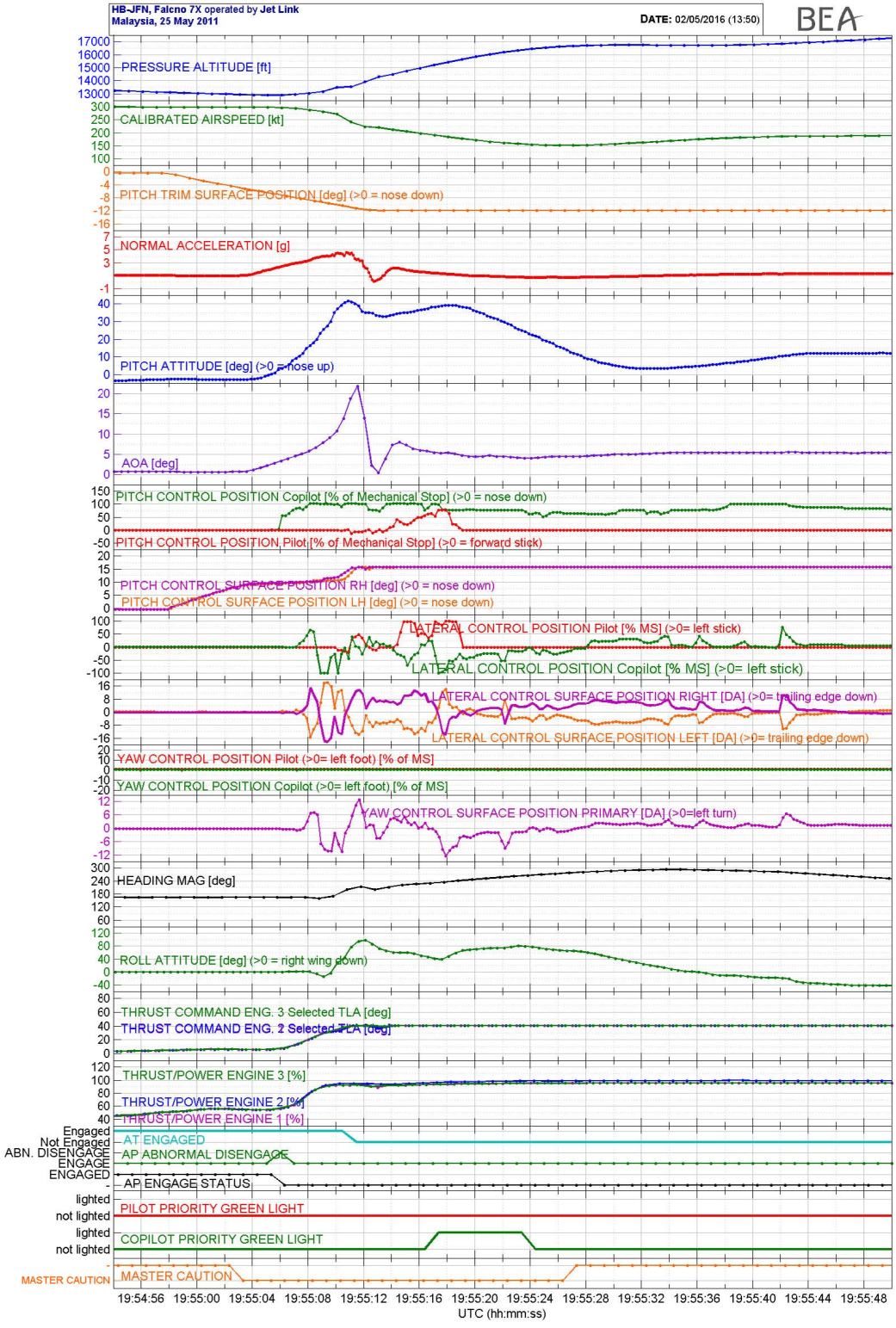
annexe 2

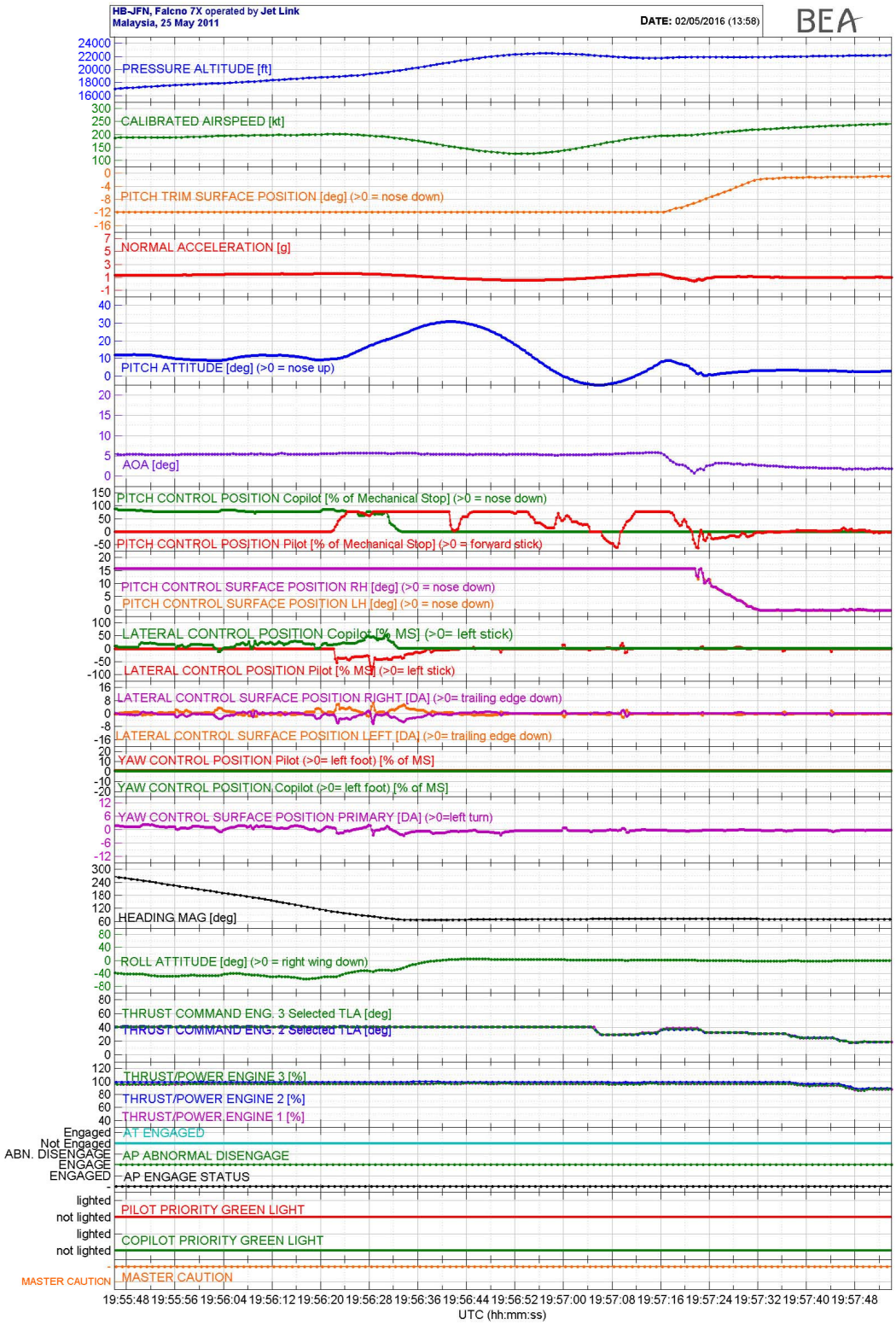
Procèdure PITCH TRIM RUNAWAY

Annexe 1

Paramètres FDR




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)

Annexe 2

Procédure PITCH TRIM RUNAWAY

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.

Source : Dassault Aviation

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