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

Reverse-Engineering the Causal Links Reveals Safety Analysis Issues

Sébastien DAVID / David ROMAT
Senior Safety Investigators

Context of the flight

Consequences

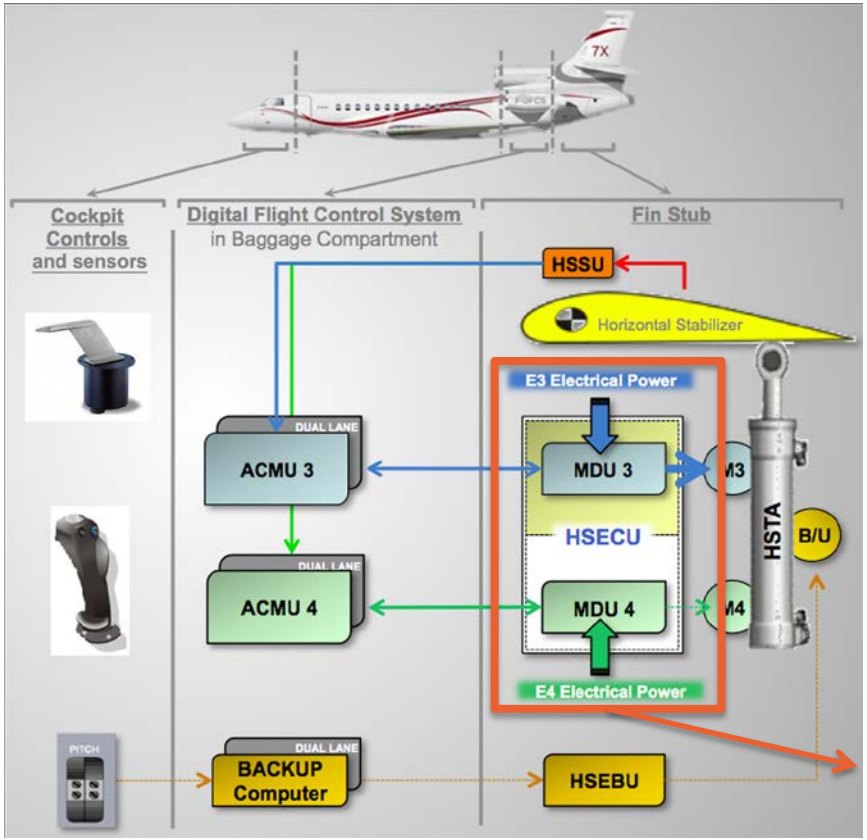
Dassault Falcon 7X fleet temporarily grounded

- Emergency Airworthiness Directive (AD)
- Return to service 3 weeks after the serious incident
  - Airworthiness and commercial pressure

High probability of accident despite PF reflex reaction

- Possible loss of control

Trimmable Horizontal Stabilizer (THS) Control

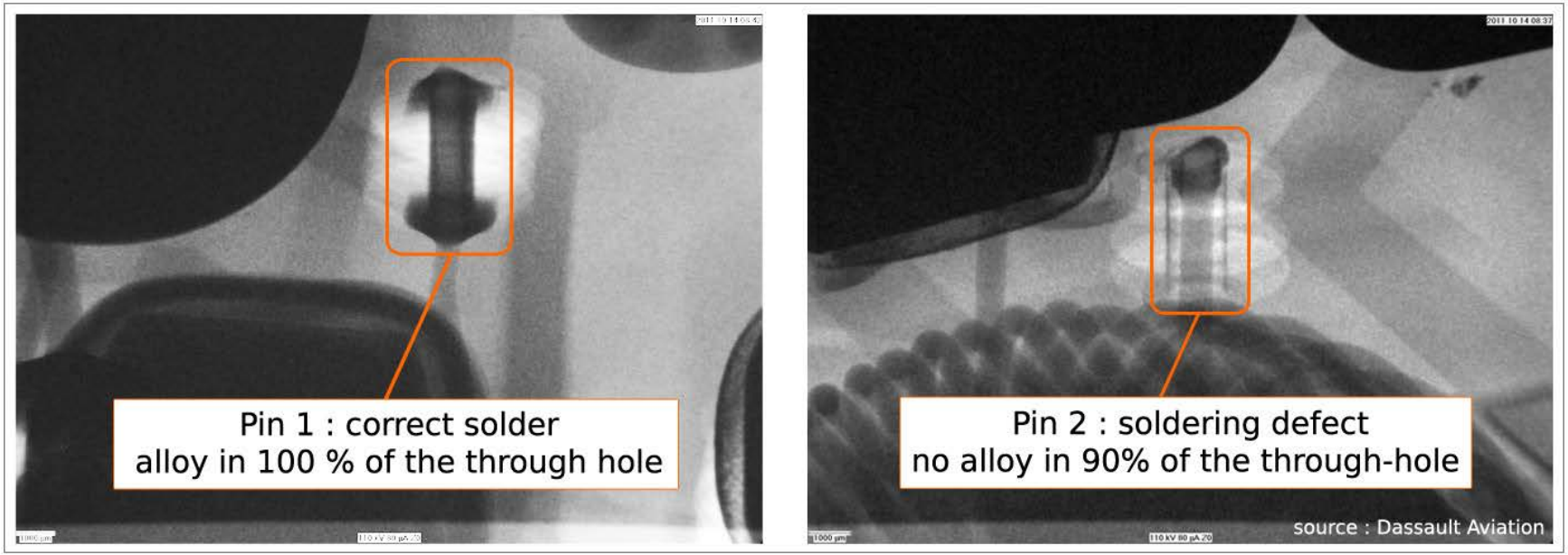


HSECU examination

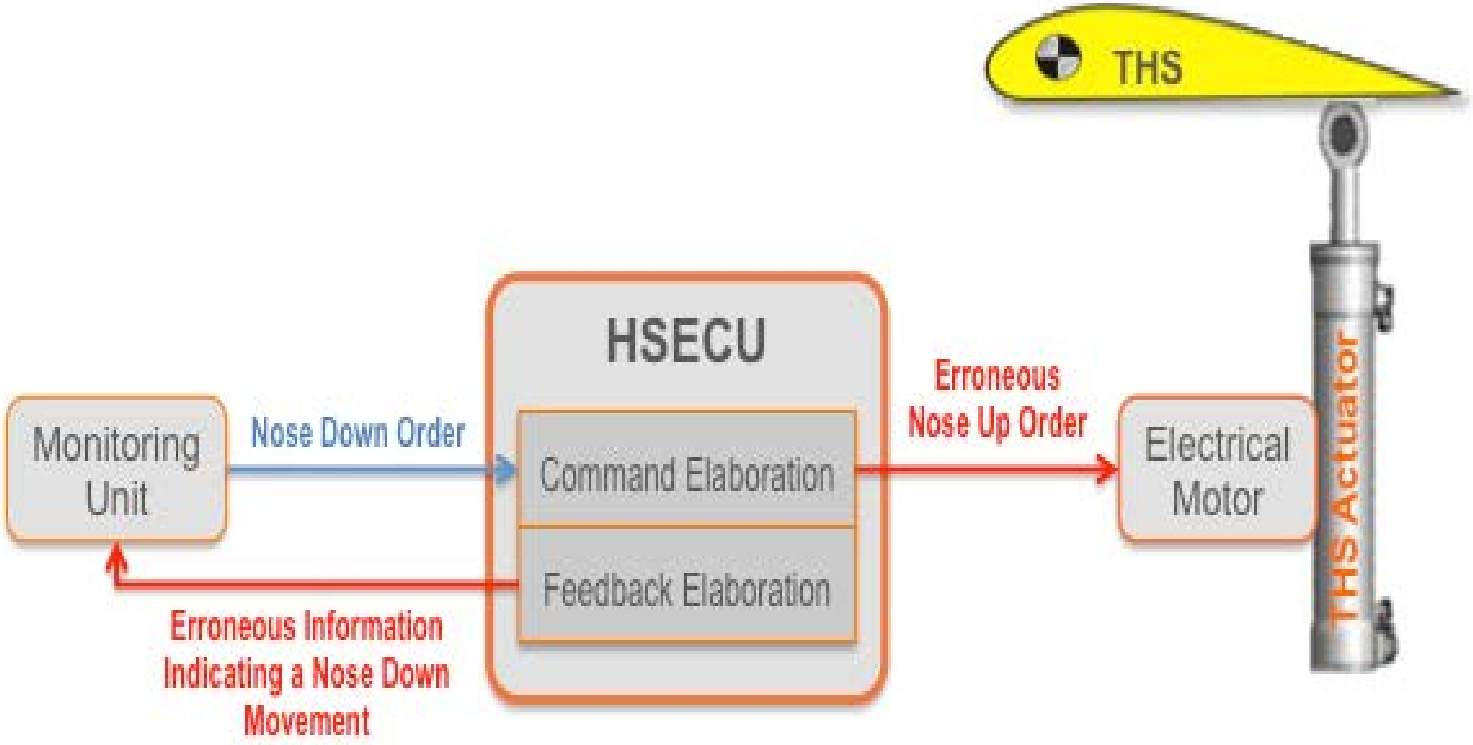
Triggering Event

Solder defect on the L4 induction coil

Triggering event



Triggering event



Scope of the investigation

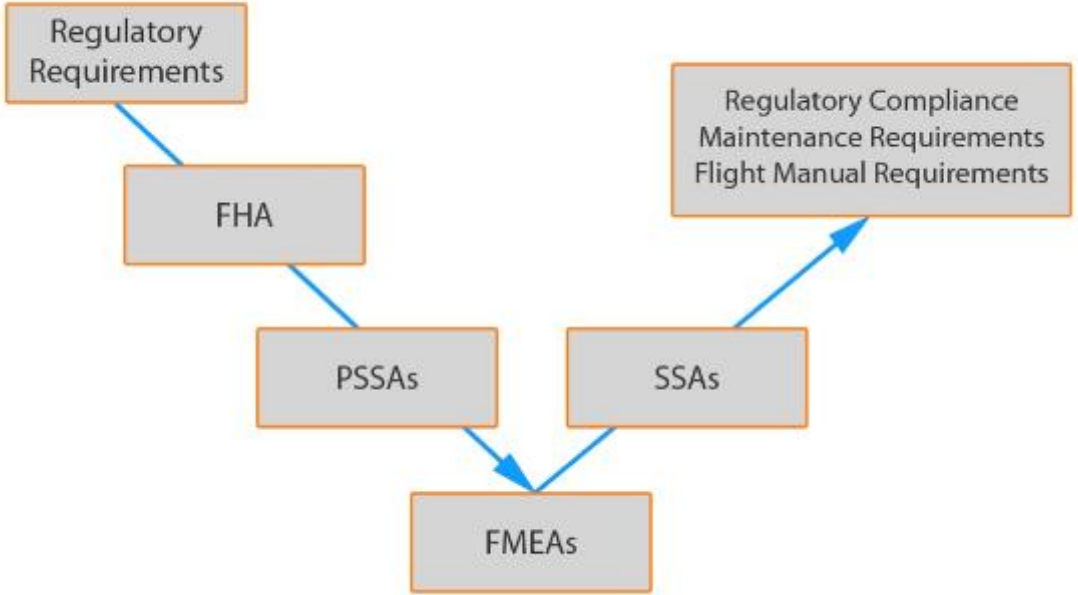
Identification of the faulty electrical connection

- Not the end-point of the safety investigation

Investigation of design process and vulnerabilities

- Evaluation of the soldering defect consequences in the safety analysis process?
- Validation of the safety analysis?
- Impact on aeroplane design and the serious incident?

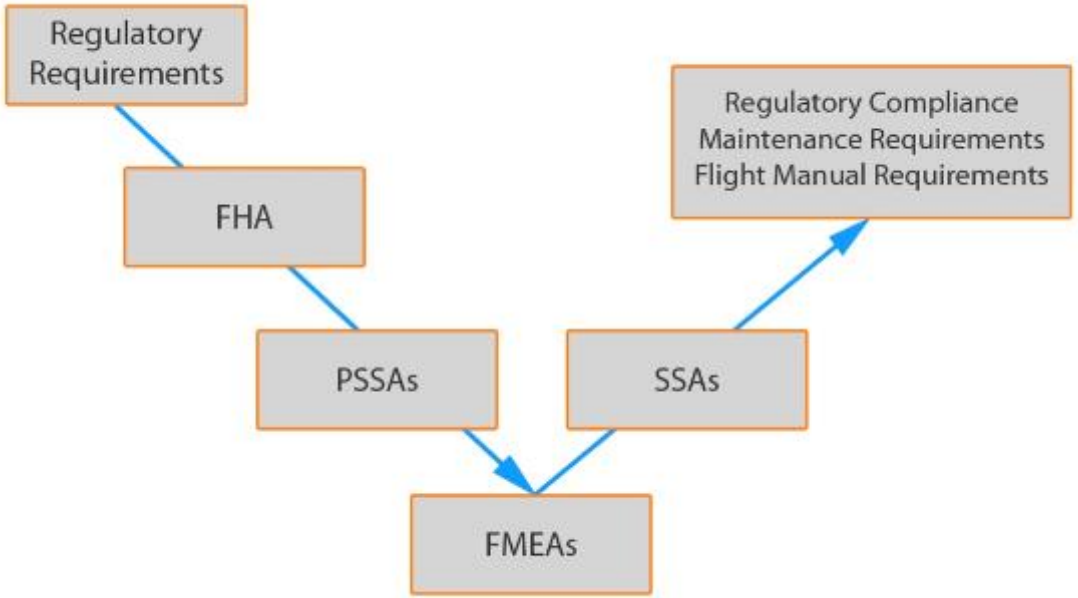
Safety Assessment Process



Example of an FMEA

Component	Failure mode	Cause of failure	Local effect	Overall effect	Failure rate (per FH)
Inductor	**Short circuit**	Part damage	Noise	Noise	XXX
	Open circuit	Part damage	Loss of –15 Volt power	No motor drive for actuator	XXX
	Change value	Aging	Potential latent failure	Potential latent failure	XXX

Safety Assessment Process



Single Failure

- Uncommanded THS runaway should not result from a single failure
- According to HSECU's FMEA, soldering defect on one induction coil:

Potentially Latent

- Most failure effects described as latent in FMEA
- Impact on safety assessment

FMEA Findings

- **3 months of analysis** to find out the behaviour of L4 on the THS system
- FMEA complete update
  - Same methodology, same people
  - significantly different results
- **Variability** and **uncertainty** in FMEA results
- FMEA key role in safety assessment process

FMEA Drafting

FMEA drafting depends on

- Human factors
- Organisational factors
- Factors inherent to FMEAs

FMEA process

- Late 1940s
- Simple electrical or mechanical equipment
- Poorly suited to complex equipment, particularly computers.

FMEA Verification and Validation

Rockwell-Collins : 3 people

Dassault-Aviation : General check of FMEA

EASA : No check

FMEA errors

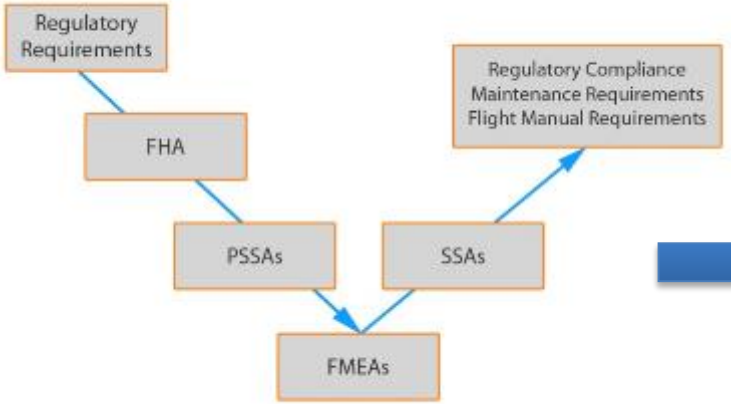
↳ Erroneous Safety Assessments

↳ Latent design errors

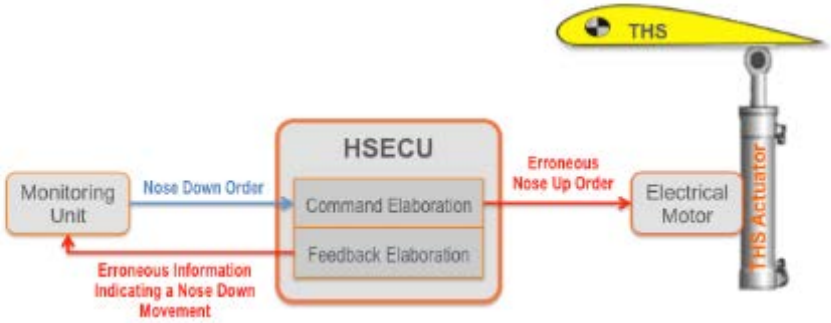
↳ Direct impact on :

- System safety
- Operations
- Maintenance

SSA Limitations



HSECU not mentioned in Flight Control System SSA



Monitoring function relied on HSECU to detect a runaway caused by HSECU

Lack of independence between control and monitoring

Conclusion

Safety assessment process vulnerable to errors

- Development and validation of FMEAs by an equipment manufacturer
- Design organisation's capability of managing and supervising subcontractors
- Validation of an SSA by a design organisation
- Approval by the certification authority

Safety Recommendations

- Raising weaknesses of:
  - FMEA methodology for electronic equipment and software
  - Means to check the independence of the control and the monitoring of systems
- Addressed to FAA and EASA in coordination with SAE and EUROCAE

BEA

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

Thank you for your attention

www.bea.aero

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE