UNA QUESTIONE DI ALGORITMI

Il 7 ottobre del 2008 l'Airbus 330 in volo da Singapore a Perth era in fase di crociera a 37.000 piedi quando uno dei tre ADIRU (Air Data Inertial Reference Units) iniziò a trasmettere valori incoerenti ("spikes") ai sistemi di guida di bordo. Appena due minuti dopo, a seguito dei dati sull'angolo di attacco (AOA) che questo ADIRU aveva processato, il computer primario di controllo volo (FCPC) comandava un *pitch-down* all'aeromobile.
A seguito di questo repentino e inaspettato comando 110 passeggeri (dei 303) e 9 membri di equipaggi (su 12) riportarono gravi ferite.
"L'evento del 7 ottobre 2008 è avvenuto a causa del combinarsi di una limitazione strutturale del software del FCPC dell'aeromobile A330/340, congiuntamente a un difetto che ha riguardato uno dei tre ADIRU" si può leggere nella pagina XV del rapporto finale AO2008070 dell'ATSB australiana il quale rapporto merita particolare attenzione in quanto per stessa ammissione degli investigatori autraliani

"including some that had rarely been considered in depth by previous aviation investigations."

L'evento

Alle **0440:26** l'ADIRU1 ha iniziato a inviare dati incorretti ai sistemi di bordo e due secondi dopo alle **0440:28** l'autopilota si disconnetteva. Da quel momento sull'ECAM (Electronic Centralized Aircraft Monitor) sono iniziati ad apparire vari messaggi di malfunzionamenti accompagnati da *aural stall warnings and overspeed warnings.*

In aggiunta agli allarmi e ai messaggi, l'equipaggio notava anche che sul display primario (PFD), lato comandante, l'indicazione della velocità e dell'altitudine erano fluttuanti, mentre sull'altro PFD le indicazioni non oscillavano e rimanevano costanti.

Alle **0442:27** mentre l'equipaggio si confrontava con questi problemi improvvisamente l'aereo scendeva con un angolo massimo *nose-down* di 8.4°.

Il registratore mostrerà che il capitano ha immediatamente richiamato a se il *sidestick* per fermare il movimento di discesa ma il sistema di controllo non ha risposto immediatamente al comando, bensì solo dopo 2 secondi l'aeromobile ha iniziato il suo recupero alla altitudine assegnata. Durante questi due secondi l'aereo è disceso di 150ft. Complessivamente l'aereo è sceso di 690 ft su 23 secondi prima di tornare a livello di volo 370. E' stato durante questa fase che si sono registrati feriti a bordo nonchè danneggiamenti alla parte superiore della cabina.

Mentre l'equipaggio era alle prese con la decifrazione dei messaggi ECAM alle **0445:08** un secondo *pitch-down*, questa volta di 3,5° , è occorso ed anche in questo caso si è verificata la stessa risposta ritardata da parte dell'aeromobile di circa 2 secondi.

Alle **0449:05** il comandante decideva per una diversione a Learmonth che si trovava a 154 km (84NM) avvertendo di avere "*flight control computer problems'* e in tal senso veniva lanciato un messaggio PAN il quale però alle **0454:25** si trasformava in un MAYDAY dopo che dai rapporti del personale di cabina appariva chiaro che molti feriti richiedevano cure immediate.

Dalle 0445.11 fino alle fine del volo i sistemi controllo saranno in fase "alternate law" ; nel frattempo in cabina continuavano i messaggi di allerta e, annota il rapporto (1.1.4) l'equipaggio *"could not effectively interact with the ECAM to action and/or clear the messages."*

Le indagini

I primi accertamenti avevano appurato che i movimenti di *pitch down* erano stati causati dai timoni di profondità ma bisognava appurare il motivo per cui gli stessi erano avvenuti in assenza di turbolenza, senza alcun problema di *weight and balance* o di altri malfunzionamenti evidenti.

Il rapporto passa poi ad analizzare la tecnica dei movimenti nei timoni di profondità (5.1):

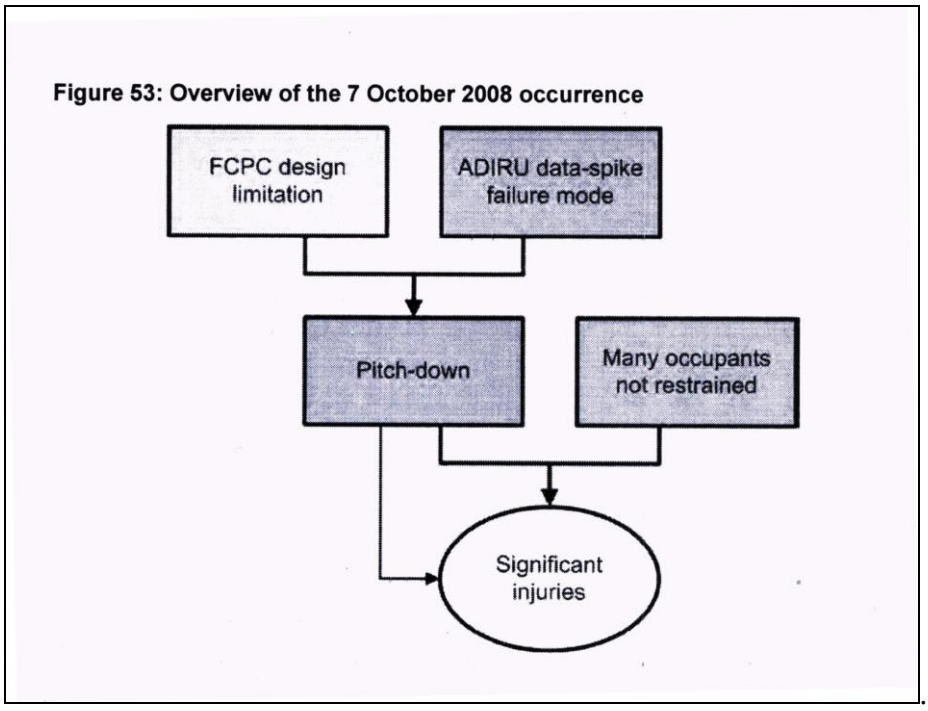
• L'FCPC è disegnato per comandare il *pitch-down* nel caso che l'angolo di attacco sia eccessivo.

• Una analisi degli algoritmi del FCPC usati per processare i dati dell'angolo di attacco hanno evidenziato uno specifico scenario, non intenzionale, nel quale un dato di AOA non corretto originato **solo da uno** dei tre ADIRU può azionare il comando di *pitch-down.* Questo scenario si verifica allorché vi sono due spikes di AOA nel quale il successivo viene dato 1,2 secondi dopo l'inizio del primo.

• Due minuti prima del *pitch-down*, l'ADIRU 1 ha iniziato a emettere spikes riguardanti i dati AOA; stessi dati e spikes erano presenti in entrambi i casi di pitch-downs.

• Simulazioni effettuate dal costruttore dell'aeromobile hanno confermato che spikes riguardanti l'AOA della stessa rilevanza di quelli registrati durante il volo in esame sono capaci di azionare il movimento dei timoni di profondità come appunto occorso all'A330 in oggetto.

Trattando di "spikes" e di una manciata di secondi temporali inizia ad apparire evidente a cosa gli investigatori australiani si riferissero allorchè accennavano nella loro premessa ad "*elementi raramente analizzati in dettaglio in precedenti indagini aeronautiche*".



Scendendo nel dettaglio (5.2.1) il rapporto annota come l'AOA sia un parametro di volo "*critically important*" , e un aeromobile con un "*full-authority flight control system*" quale è appunto l'A330 e 340 deve essere progettato in modo tale da disporre e usare accurati dati AOA. Ora, prosegue il rapporto, lo strumento

primario di difesa contro un ADIRU che fornisce erronei dati AOA al FCPC *"was the ADIRU itself, but this was not effective on the occurrence flight".*

Ci stiamo addentrando in aspetti di ingegneria elettronica e di progettazione software e, a questo punto per evitare malintesi, preferiamo riportare il testo integrale del rapporto:

"the aircraft had three ADIRUs to provide redundancy and fault tolerance. Using the median of three values for a parameter as the system input is a common and generally robust algorithm, and the A330/A340 EFCS used this approach for most parameters. However, in order to address aerodynamic issues associated with the locations of the three AOA sensors, the FCPCs based the system input on the average value of AOA 1 and AOA 2. Nevertheless, they still used all three AOA values to check for consistency, as a basis for filtering out deviating values of AOA 1 and AOA 2, and for triggering a 1.2-second memorisation period using the previous value if an errant value of AOA 1 or AOA 2 was detected.

The FCPC algorithm was generally very effective, and could deal with almost all possible situations involving incorrect AOA data being provided by one ADIRU. It could manage step-changes, runaways, single spikes, and most situations involving multiple spikes or intermittently incorrect data. For example, the ADIRU data-spike failure mode occurred on 12 September 2006 with spurious stall warnings (and therefore AOA spikes) occurring over a 30-minute period with no reported effect on the aircraft's flightpath. On the 7 October 2008 flight, there were a large number of AOA spikes transmitted by ADIRU 1, and almost all of these were effectively filtered by the FCPCs.

Nevertheless, the FCPC's AOA algorithm could not effectively manage a scenario where there were multiple spikes such that one triggered a memorisation period and another was present 1.2 seconds later. The problem was that, if a 1.2-second memorisation period was triggered, the FCPCs accepted the next values of AOA 1 and AOA 2 after the end of the memorisation period as valid. In other words, the algorithm did not effectively handle the transition from the end of a memorisation period back to the normal operating mode when a second data spike was present."

Quindi attenzione alla frase che specifica: "*gli algoritmi del computer primario controllo volo (FCPC) sono **generalmente** molto efficienti e possono trattare con **quasi tutte** le possibili situazioni che coinvolgono errati dati sull'angolo di attacco forniti da un apparato ADIRU"* , in quanto su questi termini che tendono a esprimere dubbi sulla copertura offerta dai sistemi di bordo da probabili malfunzionamenti, crediamo valga la pena di riflettere.

Andando al capitolo riguardante le risultanze (6) troveremo quale prima conclusione significativa per la safety:

"Vi è stata una limitazione negli algoritmi usati dal computer primario FCPC per processare i dati relativi all'angolo di attacco. Questa limitazione significa che, in una specifica determinata situazione, spikes multipli di AOA originanti anche da uno solo dei tre ADIRU possono impartire il comando ai timoni di profondità di nose-down. " Circa la classificazione di questa conclusione l'ente francese BEA non si è trovata d'accordo (pag. 291 del rapporto).

In chiusura vorremmo rammentare come stessa tipologia di incidente si è verificata in altre due *occurrences*, il 12 settembre 2006 stesso aereo (HV-QPA) ancora l'apparato ADIRU1 coinvolto, e il 27 dicembre 2008 un altro A330 (VH-QPG) ha registrato nuovamente un malfunzionamento dell'ADIRU1. Dal momento che questi incidenti sono avvenuti nella stessa area geografica qualcuno parlò addirittura di un nuovo triangolo delle Bermude.

Con tali premesse, se pensiamo che nell'analisi di questi incidenti si sono studiate anche le interferenze sugli apparati di bordo che potrebbero derivare da radiazione galattiche, solari o elettromagnetiche, avremo modo di apprezzare ancor più l'eccellente lavoro fatto dagli investigatori australiani i quali hanno tenuto a precisare che "a *seguito delle risultanze investigative passeggeri, equipaggi e operatori possono essere fiduciosi che lo stesso tipo di incidente non si verificherà di nuovo"* .

AAR- Safety Newsletter (2/12), 10 Gennaio 2012