Perché i due incidenti ai velivoli B 737 MAX sono stati causati dalla presenza simultanea di elementi eterogenei che hanno concorso a determinare gli eventi.

di *Dario Romagnoli*[1]

"Non troverai mai la verità, se non sei disposto
ad accettare anche ciò che non ti aspettavi di trovare."

Eraclito**.**

Il Boeing 737 MAX, prodotto di punta dell'industria aeronautica U.S.A, ha avuto in tempi relativamente recenti due catastrofici incidenti, il primo avvenuto in Malesia il 29 ottobre 2018, il secondo in Etiopia il 10 marzo 2019. Entrambi i velivoli sono andati completamente distrutti causando la morte di tutti i 346 occupanti fra equipaggi e passeggeri. Dopo il secondo incidente, la FAA[2] con l'Emergency Order Of Prohibition del 13 marzo 2019, ordinava la "messa a terra" fino a nuovo ordine del modello di velivolo.[3]

Le condizioni in cui l'incidente é maturato sono note e molto simili fra loro ed evidenziano in entrambi i casi l'attivazione dell'avvisatore di pre-stallo, l'elaborazione di erronei valori di AOA inviati all'ADC[4], nonché il trimmaggio continuo dello stabilizzatore Nose Down non comandato dai piloti.

Entrambe le investigazioni condotte sugli incidenti[5] hanno evidenziato anche alcuni fattori contributivi che sono indubbiamente indicativi delle realtà aeronautiche di alcuni Paesi in via di sviluppo e della degradata gestione operativa in cui alcune Compagnie aeree sono costrette, o decidono, di operare[6]. Su questo sarà opportuno tornare successivamente in altra sede, per il momento vorrei concentrarmi sulla causa "visibile" degli incidenti.

Sul banco degli imputati, in entrambi gli eventi, è stato messo un apparato denominato MCAS[7] la cui funzione é così schematizzata nella Relazione finale sull'incidente emessa dal KNKT indonesiano.

---

[1] Dario Romagnoli ha acquisito una consolidata esperienza di volo prima come ufficiale pil. dell'A.M. poi come pilota e comandante di linea in Alitalia. Successivamente ha ricoperto incarichi di ispettore di volo, rappresentante italiano presso il JAA nel sottogruppo AWO, e presidente di Commissione ministeriale per Malpensa 2000. Ha ricoperto incarichi direttivi in ENAC e di Investigatore presso ANSV. E' "expert" aeronautico presso l'EASA dove ha seguito per l'Italia la formulazione del Reg (UE) 996. Attualmente è coordinatore del Dipartimento sicurezza del centro studi sulla sicurezza STASA.

[2] FAA, Federal Aviation Administration- United States Department of Transportation

[3] L'Emergency Order Of Prohibition, tecnicamente si applica a tutti gli operatori US o certificati dalla FAA, tutte le altre autorità di certificazione hanno adottato simili provvedimenti.

[4] AOA, Angle Of Attack; ADC, Air Data Computer.

[5] Final Report Komite Nasional Keselamatan Transportasi Republic of Indonesia: Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018. Ethiopian Ministry of Transport , Aircraft Accident Investigation Bureau , Aircraft Accident Investigation Preliminary Report: Ethiopian Airlines Group B737-8 (MAX) Registered ET-AVJ 28 NM South East of Addis Ababa, Bole International Airport ; March 10, 2019 . Report No. AI-01/19.

[6] Inter alia: KNKT Report findings da n.38 a n.61, ICAO USOAP reports. The Aviation Herald 11 Oct 2019: " FAA (…) listing more than 60 findings identifying a systemic failure of the whole quality management and training management systems…"

[7] MCAS, Maneuvering Characteristics Augmentation System.

“Il MCAS è una funzione all’interno dello Speed Trim System che (solo durante il pilotaggio manuale n.d.r.) quando attivato, muove lo stabilizzatore durante manovre con anomalo alto angolo d’attacco a bassa velocità con flaps retratti, fornendo un opportuno incremento del gradiente di sforzo sulla barra di comando riducendo la tendenza a cabrare.”

Della presenza e funzionalità di questo apparato (presente solo sulla serie MAX del B737) la casa costruttrice Boeing non aveva fornito informazioni complete, sia agli utilizzatori, per consentire l’addestramento dei piloti e tecnici, soprattutto ed ancora più sciattamente all’ente federale USA di certificazione, la FAA.

“*L’addestramento dei piloti avrebbe dovuto aiutare a riconoscere situazioni anormali e le (conseguenti) azioni (necessarie n.d.r.). La Boeing non ha fornito informazioni e specifiche d’addestramento supplementari per il 737-8 (MAX) poiché ha ritenuto che le condizioni fossero simili a quelle dei precedenti modelli di 737.”*

La Boeing aveva perciò installato sulla nuova serie MAX un apparato che per la prima volta nella storia dell’aviazione oltre che avere funzioni di “Monitor” e “Warning” o anche “Interruzione” di manovre errate del pilota, aveva anche funzionalità autonome d’intervento sulla elaborazione delle leggi di azione sui comandi di volo. Ciò accadeva senza che i principali interessati, i piloti, ne fossero a conoscenza!

La insufficiente considerazione di Boeing sulle possibili implicazioni dell’utilizzo del sistema MCAS e la mancanza d’informazioni adeguate agli utilizzatori finali e frammentarie al certificatore, purtroppo non sono le sole nella serie di problemi che, a cascata, sono stati identificati. Per l’intrinseca funzione dello MCAS era stato anche modificato il software dello FCC[8] e le leggi d’intervento sui comandi di volo cioè le logiche con cui li comanda.

Pensando ai due incidenti ed alle modalità con cui si sono sviluppati, spesso mi sono chiesto se piloti esperti e addestrati (non ovviamente nella specifica emergenza), inseriti in una Compagnia aerea efficiente, sarebbero riusciti ad uscirne?

Con tutti i “se” e “ma” d’obbligo, ho maturato l’idea che l’emergenza poteva essere risolta nell’ambito delle risorse professionali di un pilota di linea.

L’emergenza era “rognosa” ma valutando attentamente come si sono svolti i fatti (di questo fanno fede le registrazioni del DCVR[9]) la lotta impari che i piloti hanno ingaggiato per “tenere per aria” il velivolo mentre una “mano misteriosa” li faceva sempre più sprofondare verso terra, poteva essere risolta con l’attivazione degli interruttori di Cut Out del trim, manovra che dovrebbe essere a conoscenza di un pilota di linea professionista. Manovra, del resto messa in atto con successo dall’equipaggio Lyon Air del volo precedente a quello dell’incidente, che aveva subito la stessa avaria.

Secondo Boeing gli effetti pratici di un anomalo intervento dello MCAS potevano essere contrastati con l’utilizzo del trim elettrico (che prevale sullo MCAS) essendo i sintomi i medesimi di una avaria codificata “Runaway Stabilizer”, come tale doveva essere gestita.

Le osservazioni prevalenti che sono apparse sulla stampa, sono relative alla validità del progetto Boeing e l’attività di certificazione svolta dalla FAA.

---

[8] FCC, Flight Control Computer.
[9] DCVR, Digital Cockpit Voice Recorder.

La prima è così riassumibile: “Il progetto B 737 è vecchio di 50 anni, ha subito troppe varianti ed aggiornamenti che ne hanno snaturato la concezione originaria, non tenendo in considerazione le possibili e non note interazioni fra i diversi successivi componenti installati nel corso della sua evoluzione”.

Se effettivamente il B 737 ha avuto rilevanti modifiche nel corso degli anni, bisogna però convenire che ciò, più che essere un difetto, conferma la vitalità di un progetto che ha dimostrato dopo 50 anni, di potersi adeguare alle innovazioni tecnologiche e alle esigenze del mercato. Vitalità che pochi progetti analoghi possono vantare.

In campo aeronautico l’adeguamento progressivo di progetti con l’introduzione di modifiche anche maggiori, sono una pratica corrente ampiamente diffusa. Ad esempio un aereo di grande successo, il DC9, la cui produzione è durata 41 anni, ha avuto tra modifiche e varianti circa 23 diverse versioni[10]. I francesi di versioni dello Airbus A 300 ne hanno prodotte una quarantina, partendo dall’A300 B1 con strumentazione analogica ed equipaggio di 2 piloti + Tecnico di volo, per arrivare alla versione “600” con strumentazione digitale glass cokpit ed equipaggio con 2 piloti senza tecnico di volo[11].

Il problema perciò non è “se”, ma “come” le modifiche vengono introdotte.

Il B737 in tutte le sue versioni e varianti ha sempre volato con ottimi “records” di sicurezza ed affidabilità superando le analisi strutturali agli elementi finiti, FEM[12]in ogni fase di implementazione dei progetti di nuove varianti. Le stesse versioni NG sostanzialmente uguali a quelle MAX non hanno avuto particolari inconvenienti.

L’installazione di un motore diverso, il LEAP 1B in sostituzione dello CFM 56 (con ciò che ha comportato) non è di per se un motivo sufficiente per affermare che il progetto 737 MAX sia decotto. Il problema è stato essenzialmente commerciale non tecnico.

Il commerciale di Boeing premeva per affrettare la certificazione, il commerciale voleva presentare il B 737 MAX come variante che per il conseguimento del rating dei piloti non richiedeva addestramento neanche “per differenze”, il commerciale doveva evadere le migliaia di ordini pervenuti da tutto il mondo e i tecnici si sono adeguati.

“They gambled, we lost!” (Loro hanno giocato d’azzardo, noi abbiamo perso!), è stato l’amaro commento di un familiare di una vittima comprensibilmente impotente e disperato di fronte alla complessità di individuare dei responsabili per i mortali incidenti.

Purtuttavia, gli osservatori più competenti comprendono che analisi sommarie e non approfondite, fatte sull’onda emotiva degli eventi, non fanno giustizia ed ancora più importante chiarezza, su quanto è realmente accaduto.

---

[10] DC-9-11, DC-9-12, DC-9-13, DC-9-14, DC-9-15, DC-9-15F, DC-9-21, DC-9-31, DC-9-32, DC-9-32 (VC-9C), DC-9-32F, DC-9-32F (C-9A, C-9B), DC-9-33F, DC-9-34, DC-9-34F, DC-9-41, DC-9-51, DC-9-81 (MD-81), DC-9-82 (MD-82), DC-9-83 (MD-83), DC-9-87 (MD-87) MD-88, MD-90-30, 717-200

[11] A300 B1 A300 B2-1A A300 B2-1C A300 B2K-3C A300 B2-202 A300 B2-203 A300 B2-320 A300 B4-2C A300 B4-102 A300 B4-103 A300 B4-120 A300 B4-203 A300 B4-220 A300 C4-203 A300 F4-203 A310-203 A310-221 A310-222 A310-204 A310-203C A310-322 A310-304 A310-324 A310-308 A310-325 A300 B4-620 A300 B4-601 A300 B4-603 A300 B4-622 A300 C4-620 A300 B4-605R A300 B4-622R A300 F4-605R A300 F4-622R A300 C4-605R variant F

[12] FEM, Finite Element Method.

A tal proposito è di estremo interesse riportare alcuni brani dallo "*Safety Recommendation Repor*t" elaborato dallo NTSB[13] americano dal titolo:

" Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance" (Presupposti utilizzati nel processo di verifica di sicurezza e sugli effetti di multipli avvisi e indicazioni sulle prestazioni dei piloti).

"(…) lo NTSB conclude che Boeing nell'utilizzare i presupposti nella sua verifica del rischio funzionale della attivazione non comandata dello MCAS del 737 MAX, non ha considerato e tenuto conto adeguatamente dell'impatto che multipli avvisi e indicazioni in cabina di pilotaggio possono avere sulla reazione dei piloti in risposta al pericolo."

"Inoltre, le direttive FAA consentono che tali presupposti vengano utilizzati nelle analisi di certificazione di velivoli categoria- trasporto senza fornire ai richiedenti (la certificazione n.d.r.) chiare direttive in merito:"

"Poiché la FAA routinariamente armonizza standards e direttive (di certificazione n.d.r.) con gli altri regolatori internazionali che emettono certificati per tipo di velivolo categoria – trasporto, lo NTSB segnala che codesti velivoli potrebbero essere stati progettati usando standards simili e conseguentemente potrebbero essere impattati da medesime problematiche. Lo NTSB quindi raccomanda che la FAA notifichi agli altri regolatori internazionali che certificano i progetti di velivoli per tipo categoria- trasporto (per esempio l'EASA dell'Unione Europea, Transport Canada, l'Agenzia per l'aviazione civile del Brasile, l'Amministrazione per l'aviazione civile della Cina e la Agenzia per il trasporto aereo della federazione Russa), la raccomandazione A-19-11[14] e li esorti a valutarne l'importanza nei loro processi (di certificazione n.d.r.) introducendo modifiche se necessarie."

Dunque: a) la Boeing nel processo di certificazione dello MCAS ha seguito gli standards e le direttive emanate dalla FAA e b) gli stessi standards e direttive potrebbero essere stati utilizzati da tutti gli altri Paesi. Insomma, ci stanno dentro tutti "fino al collo".

Il problema connesso con multipli e contrastanti avvisi (luminosi, tattili e sonori) che in presenza di talune avarie si attivano contemporaneamente in cabina di pilotaggio e che sono disorientanti perché "oscuranti"[15], richiama in pieno[16] ciò che hanno tragicamente sperimentato i piloti nel corso del fatale volo dello Airbus A330 AF 447 [17] che il 1° giugno del 2009 si è inabissato nell'oceano Atlantico.

---

[13] NTSB,National Transport, Safety Board. Agenzia investigative USA sulle cause degli incidenti nel settore dei trasporti.

[14] (A-19-11) Recommendations to the Federal Aviation Administration. .Require that for all other US type-certificated transport-category airplanes, manufacturers (1) ensure that system safety assessments for which they assumed immediate and appropriate pilot corrective actions in response to uncommanded flight control inputs consider the effect of all possible flight deck alerts and indications on pilot recognition and response; and (2) incorporate design enhancements (including flight deck alerts and indications), pilot procedures, and/or training requirements, where needed, to minimize the potential for and safety impact of pilot actions that are inconsistent with manufacturer assumptions.

[15] Ad esempio, il rumore prodotto dallo Stik Shaker potrebbe coprire l'allarme sonoro del movimento continuo dello stabilizzatore.

[16] Si veda: Recommandations de securité - BEA Rapport final Ministère de l'Ecologie, du Développement durable et de l'Energie Accident survenu le 1er juin 2009 à l'Airbus A330-203 immatriculé F-GZCP exploité par Air France vol AF 447 Rio de Janeiro – Paris.

[17] https://www.bea.aero/fileadmin/documents/docspa/2009/f-cp090601/pdf/f-cp090601.pdf

Se effettivamente vogliamo capire, dobbiamo guardare anche altrove ed in profondità.

La seconda osservazione é: *" che si sia realizzato negli anni un progressivo asservimento dello Stato (USA n.d.r) alle esigenze dell'industria con la contemporanea perdita della visione di lungo periodo; quella che dovrebbe caratterizzare un Paese che vuole mantenere la leadership internazionale*."[18]

Una affermazione siffatta, indubbiamente grave, pone quesiti che implicano oltre che penali, gravi responsabilità morali: "La certificazione del prodotto da parte dell'ente certificatore, che ne attesta la conformità ai regolamenti, solleva il costruttore da responsabilità? Ed anche: " La certificazione consiste nell'esame del prodotto *tel quel* oppure le verifiche e le prove possono essere sostituite da documentazione appropriata fornita dallo stesso produttore? Fino a che punto le prove di certificazione devono estendersi?"

L'Amministratore della FAA, Stephen Dickson durante la sua audizione di fronte alla Commissione d'inchiesta del Senato USA ha ammesso*:" Il costruttore ha fatto errori, anche la FAA ha fatto errori nella sorveglianza del costruttore. Boeing ha fornito all'Agenzia informazioni incomplete e frammentarie".*

Ciò che nessuno però fino ad ora ha sollevato è una questione legata alla visione che progressivamente si è instaurata sull'attuale e sul futuro modo di concepire il sistema aviazione 2.0.e che interessa tutti gli attori[19].

La domanda che tutti dovremmo porci è se enti certificatori come FAA o EASA, hanno le risorse e le competenze per sorvegliare giganti industriali delle dimensioni di Boeing o Airbus che dispongono di budget stratosferici. Boeing ad esempio, nel 2019 ha fatturato più di 75 Miliardi di dollari, più o meno corrispondente al PIL di uno stato di medie dimensioni.come la Croazia. Airbus impiega circa 56.000 dipendenti, il numero degli abitanti di Viterbo, un gigante rispetto al pigmeo EASA i cui dipendenti sono circa 900 e solo una frazione di questi sono addetti alla certificazione dei prodotti.

La risposta implicita al quesito precedente è la constatazione che la FAA per cercare di capire come stiano le cose sugli incidenti del B 737 MAX, e coinvolgere i principali utilizzatori, ha promosso assieme ad alcuni Stati, una commissione JATR[20] appaltandola ad una società privata a responsabilità limitata la Hart Solutions LLC, il cui presidente è Cristophere Hart già per 15 anni Safety Regulator in FAA e 12 anni allo NTSB di cui è stato anche presidente[21].

La pratica del riconoscimento reciproco delle certificazioni dei prodotti aeronautici è ormai oltre che economicamente razionale una pratica consolidata che consente per esempio ad

---

[18] Silvano Manera, "La gestione della complessità"(Copyright TM-CHE) www.centrostudistasa.eu
[19] Gli anglosassoni meglio definiscono con il termine "Stakeholders".
[20] JATR, Joint Authorities Technical Review.
[21] "June 1, 2019, Dear Mr. Bahrami, you chartered the Boeing 737 MAX Flight Control System Joint Authorities Technical Review (JATR), consisting of technical representatives from the FAA, National Aeronautics and Space Administration (NASA), and civil aviation authorities from Australia, Brazil, Canada, China, Europe, Indonesia, Japan, Singapore, and the United Arab Emirates. The members of the JATR team wish to thank you for the opportunity to conduct this review and to share our observations and findings. (Dalla lettera di accompagnamento dello JATR di Hart a Bahrami, FAA's Associate Administrator for Aviation Safety.)

EASA, in base ad accordi pluri-laterali, di riconoscere automaticamente la certificazione ai prodotti brasiliani, come quelli canadesi o degli Stati Uniti.

Come se non bastasse, con l'ascesa esponenziale della presenza a bordo dei velivoli di apparati elettronici che hanno bisogno per il loro funzionamento di software, si evidenzia l'impossibilità pratica di verificarne realmente la congruità.[22]

Questi programmi software, sono normalmente appaltati all'esterno ad aziende come l'indiana HCL Technologies Ltd. che per ridurre i costi utilizza anche personale temporaneo che lavora per 9 $ l'ora senza avere esperienza in campo aeronautico.[23]

Simon Hradecky[24] esperto assai autorevole, già anni fa in tempi non sospetti, criticava alcuni sotware aeronautici:" *Conosco I codici sorgente di sotware in uso su velivoli reali. Sono scioccato da questi codici sorgente che essenzialmente consistono non più che di grandi, alberi (ramificazioni n.d.r.) decisionali profondamente annidati: " se l'input è questo, o se l'input è quest'altro, o ancora questo,…allora la risposta deve essere questa". Migliaia e migliaia di linee d'istruzione annidate profondamente. E' facile predire che in questi grandi alberi decisionali una specifica condizione sia stata omessa e non controllata e che più tardi potrà diventare fatale all'equipaggio. Nel corso della mia esperienza professionale come sviluppatore di software, (posso dire che n.d.r.) questi alberi decisionali rappresentano l'ammissione che lo sviluppatore (analisti, matematici, programmatori e verificatori), non ha conoscenza della materia e che programma basandosi esclusivamente sugli indicatori forniti dal cliente."*

Il vero problema è che un programma informatico, anche volendo, non può essere del tutto verificato e garantito a prova d'errore. "*Il test dei programmi può essere usato per dimostrare la presenza di malfunzionamenti, non per dimostrare la loro assenza."* Questa affermazione di Edsger Dikjastra[25] è la sintesi dei limiti che un test di software ha, poiché il funzionamento corretto dell'applicazione in un numero finito di casi non ce ne garantisce la correttezza in generale. Il programmatore è moralmente solo di fronte al compito assegnato e solo la sua competenza, conoscenza approfondita di "cosa" deve servire il programma e la sua professionalità, sono le barriere disponibili per avere programmi affidabili.

Nell'impossibilità di estendere capillarmente i propri controlli sui progetti, prodotti, organizzazioni o personale, le verifiche si sono spostate sui processi, assegnando la responsabilità della conformità dei prodotti agli stessi soggetti coinvolti.

Nonostante ciò, le stesse indagini sugli incidenti aeronautici continuano ad essere focalizzate sul prodotto o sull'equipaggio piuttosto che sull'organizzazione che lo ha costruito o addestrato.

---

[22] KNKT Report, Ibidem. Finding n. 64. The lack of an AOA DISAGREE message did not match the Boeing system description that was the basis for certifying the aircraft design. The software not having the intended functionality was not detected by Boeing nor the FAA during development and certification of the 737-8 MAX before the aircraft had entered service.

[23] Business Insider: Rachel Premaeck, 2 luglio 2019.

[24] The Aviation Herald: Simon Hradecky, intervistato da Roman Payer per Austrian Aviation. Net

[25] Edsger Wybe Dijkstra (Rotterdam, 11 maggio 1930 – Nuenen, 6 agosto 2002) è stato un informatico olandese.

Il mondo dell'aviazione è ormai diventato globalmente un sistema auto-referente che ha fatto un lungo percorso dai suoi albori, vantandosi di essere il settore maggiormente (iper) regolato ma probabilmente nel corso del tempo, meno "veramente" controllato.

Questo approccio al problema di come sorvegliare efficacemente un sistema ad alti contenuti tecnologici e specialistici che per definizione si sposta in continuazione, utilizzando prodotti frutto della globalizzazione, non è stato ancora risolto; anzi è stato risolto affidandosi ad auto certificazioni, ad enunciati come quello della "Just culture".

Nonostante le grandi speranze che gli ambienti di lavoro "Ad alto rischio" hanno riposto in questo nuovo modo di accostarsi ai problemi di sicurezza[26] che previlegia la prevenzione, la consapevolezza responsabile e la fiducia reciproca, piuttosto che la "caccia al colpevole", bisogna sconsolatamente ammettere che mettere in paratica i principi di una Just culture è molto più complicato del previsto e soprattutto è complicato farla "transitare" dalla letteratura ai comportamenti concreti.

"Dalla carta all'attuazione", potrebbe essere il tema dominante sui fattori di sicurezza per il prossimo decennio, altrimenti non ha senso continuare ad elaborare nuove teorie e studi su modelli comportamentali in attività ad alto rischio, se quei pochi che conosciamo non vengono ancora compiutamente utilizzati.

[26] J. Reason described a "Just Culture" as an atmosphere of trust in which people are encouraged, and even rewarded, for providing essential safety-related information, but in which they are also clear about where the line must be drawn between acceptable and unacceptable behaviour."