AUTOMAZIONE E SICUREZZA DEL VOLO

del Ten. Col. Gian Luca Greco

“David, mi spiace...” disse il computer senziente e autocosciente ***HAL 9000*** al capitano David Bowman che gli chiedeva di spegnersi per scollegare i circuiti cognitivi ed il controllo di molte funzionalità della navicella spaziale *Discovery One*.

Questo estratto dal film di Stanley Kubrick, *2001: Odissea nello spazio*, è una delle rappresentazioni più iconiche di Intelligenza Artificiale (IA) nel genere fantascientifico e ha avuto un profondo impatto sulla cultura popolare.

La rappresentazione di HAL 9000 e delle sue interazioni con l’equipaggio ha avuto un profondo impatto sullo sviluppo dell’IA nel mondo reale, sollevando importanti questioni etiche e filosofiche.

Da decenni la ricerca accademica e industriale analizza come l’evoluzione tecnologica possa avere riflesso sulle performance operative del mondo dell’aviazione e dell’aerospazio.

Le attuali risorse e capacità tecnologiche non impongono limiti all’automazione di una determinata funzionalità, ma oggi si estrinsecano su cosa automatizzare nell’ottica di un’applicazione intelligente e affidabile della tecnologia.

Alla base della filosofia di implementazione della tecnologia nel mondo dell’aviazione esiste il cosiddetto **dilemma dell’automazione** che contrappone, come spesso accade nell’operare sistemi complessi e tecnologicamente avanzati, una dicotomia tra il ruolo del progettista e quello dell’operatore (in volo o a terra) allorquando lo scopo primario delle continue evoluzioni sistemiche, procedurali e tecniche è di ridurre l’errore e mitigarne gli effetti.

L’approccio del progettista tende a dare priorità alle funzionalità/modalità automatiche e autonome integrate quando si opera in regime di “*normal operation*” e sistemi non degradati, lasciando il controllo del velivolo all’equipaggio in caso di avarie o malfunzionamenti.

Dal punto di vista dell’operatore, l’approccio desiderato è letteralmente l’opposto. Difatti, l’operatore dà priorità a un supporto da parte degli automatismi in condizioni di emergenza per diminuire il carico di lavoro, allo scopo di concentrare l’attenzione sulla condotta basica del velivolo o per portare a termine operazioni.

L’operatore è indissolubilmente legato al fattore umano, così come lo sono le sue azioni nel condurre il velivolo impiegandone gli equipaggiamenti, tenendo contro che le capacità umane, le relative prestazioni e limitazioni sono chiamate in gioco anche nelle fasi di progettazione, costruzione e manutenzione di un velivolo e dei sistemi che lo compongono.

In Tabella 1, alla pagina seguente, vengono riportati gli incidenti con vittime che hanno visto come fattore contributivo la cosiddetta “*automation surprise*” ovvero un’integrazione essere umano/automazione/procedure non ottimale, potenzialmente determinata anche da un addestramento non efficace; le cause degli incidenti derivano da risposte inappropriate o dal mancato riconoscimento di comandi impartiti in modo automatico dall’aeromobile.

Negli anni Ottanta fu introdotto il concetto dei **paradossi dell’automazione** emersi nella progettazione di un sistema automatico, affidando all’automazione compiti che in precedenza venivano svolti da un operatore umano.

Con il progredire della tecnologia e delle tecniche, la domanda su “cosa automatizzare” è stata sostituita da

"come automatizzare" una certa funzionalità: il limite non è ormai più rappresentato dai vincoli tecnici, ma piuttosto dalla complessità di ottimizzare le procedure e le interazioni essere umano-tecnologia, proprio per evitare che le opportunità date dall'automazione si possano trasformare in "insidie" con potenziali conseguenze negative, come quelle che hanno caratterizzato gli eventi descritti in Tabella 1.

Il **primo paradosso** sta nella scelta di far riprendere il controllo manuale all'operatore umano solo quando quello automatico non funziona. Così facendo, non si tiene però conto che l'operatore potrebbe non avere più le abilità necessarie a svolgere il compito.

Se infatti determinati compiti non vengono sperimentati per un lungo periodo, diventa difficile per l'operatore svolgerli con la stessa rapidità, efficacia e precisione di quando era sempre lui ad eseguirli.

Strettamente legato al primo è il **secondo paradosso**. Se l'azione dell'operatore è richiesta solo in caso di guasti o problemi dell'automazione, i sistemi automatici più affidabili saranno proprio quelli che daranno all'operatore meno occasioni di esercitare le proprie abilità manuali, rendendolo quindi meno preparato ad agire in caso di emergenza.

Il **terzo paradosso** riguarda invece la scelta di trasferire all'automazione i compiti di tipo esecutivo, lasciando all'operatore un ruolo di supervisione di ciò che l'automazione sta eseguendo.

Certamente questa scelta ha il merito di ridurre il carico di lavoro dell'operatore.

Tuttavia, è noto che il sistema cognitivo umano è inadatto a svolgere compiti di vigilanza per lunghi periodi, specie quando l'informazione da osservare non mostra cambiamenti significativi. In questi casi, la prestazione dell'operatore è facilmente soggetta a errori.

Infine, uno dei motivi principali che giustificano la presenza degli operatori umani in ambienti operativi complessi è per intervenire in caso di difficoltà di gestione di eventuali situazioni impreviste da parte dei dispositivi automatici. Questo può avvenire quando le condizioni cambiano improvvisamente, in modi non contemplati dalla logica di funzionamento dell'automazione.

Tabella 1

	Colgan Air Q400 Feb 12, 2009 (NTSB, 2010)	Turkish Airlines B737-800 Feb 25, 2009 (DSB, 2010)	Air France A330 June 1, 2009 (BEA, 2012)	Asiana B777 July 6, 2013 (NTSB, 2014)	Air Asia A320 Dec 28, 2014 (KNKT, 2015)
Manner by which automation surprise was evident	Crew surprised by stick-pusher operation and responded inappropriately.	Crew unaware that auto-thrust reduction was triggered by faulty radio altimeter.	Aircraft response to control input when in alternate law at high altitude not understood by crew.	Crew failed to recognize that selection of the autopilot mode cancelled the auto-thrust speed protection.	Crew failed to recognize that pulling the autopilot mode circuit breakers in-flight keeps the aircraft in alternate law.

Automation surprise as a contributing factor in recent, high-profile, fatal aviation accidents.

Un caso emblematico accadde il 7 ottobre 2008 durante il volo Qantas 72, quando un guasto al *software* a bordo di un Airbus A330 (registrato come VH-QPA) ha messo in pericolo i 315 occupanti.

L'evento, le cui conseguenze sono state mitigate grazie al pronto intervento dell'equipaggio, provocò il ferimento di oltre 100 persone e l'investigazione sulle cause portò Airbus a modificare gli algoritmi e le logiche di funzionamento di alcuni sistemi critici per la sicurezza del volo.

Per un'avaria una delle tre unità inerziali dell'aeromobile, i sistemi disingaggiarono l'auto-pilota fornendo all'equipaggio messaggi acustici di emergenza che indicavano che l'aeromobile era in stallo e si trovava in una situazione di *over-speed* aggiungendosi a una serie di *caution* e *warning* che si contraddicevano a vicenda.

I sistemi dei comandi di volo reagirono comandando erroneamente due movimenti improvvisi di *pitch-down* (il primo evento è stato di 8,4° *nose down*). I comandi di volo non risposero agli input dell'equipaggio per almeno 2 secondi e l'aereo perse 400 piedi di quota per poi tornare autonomamente a FL370.

L'equipaggio dichiarò inoltre che non riuscì a silenziare i continui avvisi acustici di emergenza che costituirono di fatto una significativa fonte di distrazione rendendo ancor più complessa e articolata la gestione dell'emergenza e delle comunicazioni *intra-cockpit* e quelle radio con gli organi del traffico aereo.

Dopo una settimana dall'evento Airbus emise un bollettino tecnico operativo che descriveva le azioni dell'equipaggio in caso di avaria simile a quella accaduta al velivolo Qantas inserendola nel Manuale delle operazioni dell'equipaggio di volo.

Inoltre, Airbus modificò il *software* del computer primario di controllo del volo apportando successivamente delle modifiche all'algoritmo di gestione delle avarie e degli *input* erronei per evitare che un simile evento si possa ripetere.

L'operatore, a differenza della macchina, ha la potenziale capacità di comprendere lo stato inusuale del sistema, osservare l'ambiente esterno, verificare cosa sta accadendo, e mettere in relazione tutte le informazioni disponibili per capire come rimettere in moto il processo.

Tuttavia, questo tipo di prestazione necessita di elaborazioni mentali complesse, che richiedono tempo e non possono essere svolte in parallelo con altre attività.

Esattamente quello che non è possibile fare - e qui sta il **quarto paradosso** - in sistemi aeronautici, in cui le emergenze sono quasi sempre *time critical* e c'è pochissimo tempo per trovare una soluzione.

Nel primo rischieramento effettuato in Giappone da una formazione di F-22 (Fig.1), i velivoli hanno oltrepassato la linea internazionale del cambio di data e i loro sistemi di navigazione si sono bloccati.

Per raggiungere la base di destinazione hanno avuto bisogno del supporto delle informazioni provenienti dal velivolo *tanker* (velivolo KC-10).

In questo caso, il sistema di gestione della navigazione e dei dati di volo non ha elaborato correttamente la posizione attuale dei velivoli quando hanno superato la linea di data internazionale provocando il cosiddetto "*crash*" dei sistemi che erano asserviti al dato della posizione; da qui la necessità di ricorrere ai dati di navigazione

Fig. 1 Velivolo F-22 *Raptor*

forniti dal velivolo *tanker* (velivolo KC-10) il cui *cockpit* (Fig. 2) è analogico e non soggetto a bug del *software*.

Il sistema di bordo, infatti, non ha elaborato correttamente i dati di localizzazione mentre l'F-22 volava da Hickam AFB (157°W) e attraversava la Linea della Data Internazionale (Fig. 3), che rappresenta allo stesso tempo il meridiano 180°W e 180°E.

L'evento descritto è stato oggetto di studio per far emergere le cause tecniche e a fattore umano che hanno portato un sistema tecnologicamente avanzato a mettere a repentaglio vite umane a seguito di un cambio di input dati noto sin dai tempi che precedono la progettazione del F-22 (es. il cambio di data in corrispondenza del 180° meridiano).

La rapida evoluzione della tecnologia dai controlli di volo analogici a quelli digitali ha portato a un crescente sviluppo di *software* deputato alla gestione di informazioni critiche per la sicurezza del volo.

Con il crescere della complessità dei sistemi le linee di codice di *software* necessarie sono cresciute esponenzialmente (vds. Fig. 4) e a tale incremento spesso non è stato associato un opportuno dimensionamento dei controlli con opportune metodologie di "*regression testing*", tecnica che mira a verificare che un cambiamento in una parte del sistema, pur funzionando per quello che era stato progettato, non abbia creato un errore o una *failure* in un'altra parte del sistema.

Nel caso del F-22, l'uso dell'automazione nei sistemi sociotecnici complessi si è rivelato un'arma a doppio taglio.

Da un lato, il sistema automatizzato prometteva un'affidabilità senza precedenti, una riduzione del carico di lavoro, un miglioramento dell'economia e una riduzione degli errori; dall'altro, conteneva "costi" meno tangibili, ma non per questo meno reali, per gli operatori in termini di degrado delle competenze, isolamento mentale e oneri di monitoraggio, con possibili influenze sui processi di comunicazione (c.d. *Crew Resource Management - CRM*).

Ogni nuova tecnologia richiede un periodo di adattamento per eliminare i problemi residui e per consentire agli utenti di adattarsi.

La ragione principale di questo lungo processo di adattamento è la necessità di armonizzare la nuova progettazione da un lato e le politiche, le procedure e la mentalità del sistema dall'altro.

Fig. 2 *Cockpit* "analogico" velivolo *Tanker KC-10*

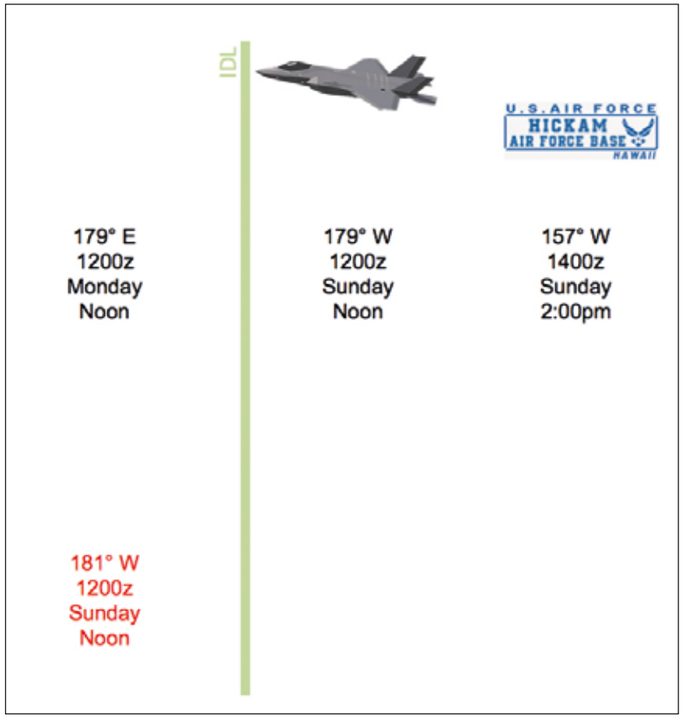
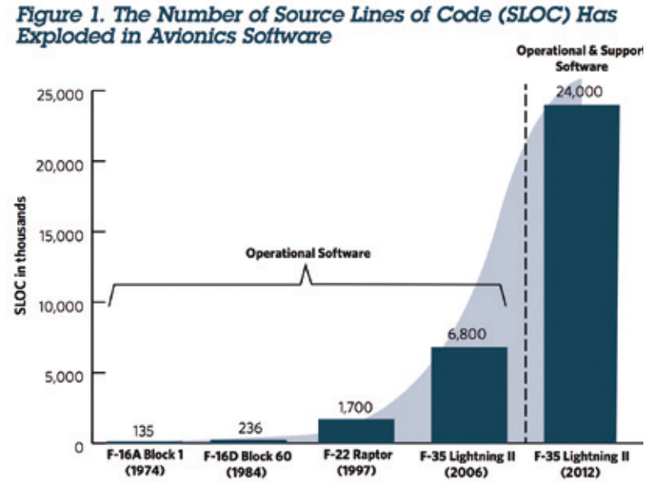


Fig. 3 Attraversamento IDL *(International Data Line)*

Fig. 4 Numero di linee di codice nei software installati a bordo di velivoli



Fonte: *"Delivering Military Software Affordably" in Defense AT&L*

Nessun esperto di Fattori Umani si sognerebbe mai di sostenere che la tecnologia, in quanto tale, abbia effetti negativi sulla sicurezza.

D'altro canto i successi dell'aviazione nel ridurre il numero di incidenti, anche grazie a un costante miglioramento della tecnologia e delle relative interfacce essere umano-macchina, sono molto evidenti e in continua evoluzione.

Possiamo tuttavia asserire che l'automazione non ha la flessibilità della mente umana e tanto meno la sua duttilità, punti di forza che fanno la differenza, soprattutto in attività di sperimentazione allorquando, proprio per la natura del *flight test*, si possono presentare casi di emergenza imprevedibili e imprevisti dai progettisti che vengono affrontati con la prevista metodologia suffragata dall'esperienza.

L'introduzione di sistemi altamente automatizzati ha apportato un importante contributo alla sicurezza al volo, in termini di precisione ed efficienza, ma ha introdotto potenziali nuove opportunità di errore.

È quindi necessario che ogni operatore, nel corso della propria carriera, acquisisca la convinzione che la tecnologia non è infallibile laddove concetti come CRM, *Decision Making*, *Task Sharing*, *Threat and Error Management (TEM)*, *Communication*, *Situational Awareness* integrati in opportuni programmi di addestramento uniti all'esperienza dell'equipaggio, rappresentino l'ultima barriera per spezzare la catena degli eventi.

Federico Faggin, autore del libro "Irriducibile", padre del microprocessore e uno dei più influenti innovatori del nostro tempo in merito alla sempre più prorompente presenza di innovazioni tecniche, sostiene che la scienza e la nostra coscienza rimarranno due ambiti distinti sui quali bisogna lavorare per metterli in condizione di cooperare al fine di portare a termine ogni compito e superare insieme eventuali difficoltà e, ancora una volta, a collaborare.

Certamente la tecnologia ha migliorato e potrà ancora migliorare l'efficienza e la produttività in molti ambiti, ma non potrà mai sostituire la coscienza umana, il potere dell'intuizione, la capacità di creare vera innovazione e soprattutto, di farlo con emozione.