A09

Giovanni Di Giorgio

Studi sui modelli e sui metodi di analisi degli incidenti aeronautici

Dai risultati della ricerca alle applicazioni

Aracne editrice

www.aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-3780-2

I edizione: novembre 2020

A mio fratello Francesco

‹‹La probabilità di un successo
è uguale al numero dei casi favorevoli
diviso per il numero di tutti i casi possibili››

(Regola di Laplace, anno 1774)

Indice

Prefazione

In letteratura scientifica ricorrono frequentemente diversi quesiti relativi al materiale documentale disponibile per la presentazione e per la guida alla conoscenza dei modelli e dei metodi di analisi ed investigazione degli incidenti nei settori complessi ad alta tecnologia. Viene altresì posta in evidenza l'importanza della fruibilità pratica degli studi, dovuta in larga parte alle analisi critiche in merito alle caratteristiche delle metodologie stesse, ed alle applicazioni significative affrontate dai ricercatori. Questa mole di lavori contribuisce notevolmente a facilitare la proliferazione e l'evoluzione dei modelli, delle tecniche disponibili, e della conoscenza dei relativi molteplici aspetti. Poi, gli studi che descrivono le condizioni di applicazione, la natura e la quantità delle risorse necessarie per l'utilizzo di ciascuna tecnica, i relativi benefici applicativi e le limitazioni, le conoscenze preliminari indispensabili all'analista, completano il quadro dell'evoluzione e dello stato dell'arte della materia.

Questo lavoro si inserisce in tale contesto, con l'obiettivo di raccogliere i principi di alcuni dei molteplici contributi fondamentali e disponibili sull'argomento in letteratura scientifica internazionale, e di facilitare la consultazione, in un unico compendio aggiornato, di materiale derivante da una quantità relativamente vasta di lavori, anche in arco temporale.

La pretesa di essere esaustivi e completi non appartiene a questo lavoro, in quanto diverso materiale non ha potuto trovare spazio all'interno dei percorsi presentati, per efficacia dell'esposizione.

Gli argomenti trattati nel testo sono affrontati mediante un approccio in cui il processo di investigazione di un incidente aeronautico è concepito come quel processo complesso il cui unico obiettivo è la prevenzione degli incidenti. Al Capitolo I è affidata l'introduzione agli strumenti di analisi. Il Capitolo II presenta i fondamenti dei modelli e dei metodi di analisi degli incidenti nei sistemi complessi, tipici dei settori ad alta tecnologia, nei quali generalmente il contesto degli

eventi e delle condizioni è caratterizzato dalla combinazione e dall'interazione di molti fattori. Inoltre, gli argomenti affrontati costituiscono una base di conoscenze propedeutiche ai successivi capitoli, ed evidenziano le differenze, i punti di forza e gli inevitabili limiti dei diversi strumenti di analisi. Il Capitolo III introduce alcuni tra i principali modelli e metodi di analisi degli incidenti di riferimento nel contesto internazionale del settore aeronautico, con applicazioni a supporto della parte teorica. La trattazione evidenzia anche il contributo notevolissimo che il settore aeronautico fornisce da decenni all'evoluzione degli strumenti di analisi degli incidenti e, in termini generali, degli eventi inattesi significativi. Il Capitolo IV riprende gli aspetti basici delle relazioni causa-effetto e degli elementi fondamentali che costituiscono la struttura portante di un modello. I Capitoli V e VI affrontano le metodologie fondamentali di analisi dal punto di vista dei processi di *Root Cause Analysis* (o di Analisi delle Cause Profonde) del settore aeronautico evidenziando, oltre all'approccio reattivo, anche le potenzialità di alcune tecniche dal punto di vista degli approcci di tipo proattivo e predittivo.

Giovanni Di Giorgio
Roma, 12 Settembre 2020

Note sull'autore

Giovanni Di Giorgio ha conseguito la Laurea in Ingegneria Aeronautica nel 2000 presso l'Università degli Studi di Napoli Federico II; nello stesso anno, ha conseguito l'abilitazione all'esercizio della professione di Ingegnere. Dal 2001 svolge la sua attività di Ingegnere Aeronautico in AgustaWestland, ora Leonardo Helicopters Division, presso cui è attualmente responsabile dell'area Manufacturing Process del Manufacturing Engineering dello stabilimento di Frosinone. Ha acquisito una lunga esperienza professionale attraverso numerosi e rilevanti programmi produttivi internazionali e nazionali per elicotteri per usi civili e governativi, nei sistemi rotori e comandi rotanti, trasmissioni e strutture di elicotteri leggeri, intermedi e pesanti (operando anche sugli elicotteri a doppio rotore in tandem e sul convertiplano *tilt rotor*). In particolare, ha acquisito una significativa esperienza professionale nell'ambito delle costruzioni aeronautiche, delle tecnologie dei processi speciali e dei materiali aerospaziali metallici ed in composito. Nel 2012 ha frequentato e superato lo Short Program *Data, Models and Business* presso il MIT, Massachusetts Institute of Technology di Boston MA (USA). Nel 2014, presso il Training Center di Ashburn VA (USA) del National Transportation Safety Board, ha frequentato e superato il Corso NTSB *Aircraft Accident Investigation*. È stato relatore e docente in seminari relativi all'investigazione degli incidenti aeronautici rivolti a Ricercatori universitari e ad Investigatori aeronautici. Ha partecipato a tavole rotonde operative sulla *Root Cause Analysis* in contesti internazionali dell'industria aerospaziale. Inoltre, dal 2018 è Docente a contratto presso il corso di Laurea Magistrale in Ingegneria Aerospaziale dell'Università degli Studi di Napoli Federico II, con incarico di didattica integrativa nel corso di Aerodinamica dell'Ala Rotante. È stato relatore, su invito, in numerosi seminari sulle Prestazioni di volo degli elicotteri per allievi di Ingegneria Aerospaziale dell'Università degli Studi di Napoli Federico II, e di seminari sull'introduzione all'Aerodinamica e principi del volo degli elicotteri

rivolti agli allievi Piloti dell'Accademia Aeronautica di Pozzuoli. È stato relatore in congressi internazionali per le prove di volo di lavori sull'analisi di missione di volo e sul calcolo delle prestazioni degli elicotteri mediante metodi della classe dell'Intelligenza Artificiale.
Il Dottor Ingegner Di Giorgio è l'autore dei seguenti libri:

— *Theory of Helicopter Flight. Aerodynamics - Flight Mechanics*. Editore Aracne, Roma, 2018;
— *Fondamenti di fenomenologia della fatica e della tensocorrosione nelle strutture aeronautiche*. Editore Aracne, Roma, 2014;
— *Teoria del volo dell'elicottero. Aerodinamica–Meccanica del volo*. Aracne, Roma. Prima Ediz. nel 2007, Seconda Ediz. nel 2009.

È iscritto all'Albo professionale, Sezione A, dell'Ordine degli Ingegneri della Provincia di Campobasso, ed è membro di SFTE - *Society of Flight Test Engineers.*

Sigle ed abbreviazioni

ATSB	Australian Transport Safety Bureau
DOE	U.S. Department of Energy
ECF	Events and Causal Factors
EEC	Eurocontrol Experimental Centre
ETTO	Efficiency-Thoroughness Trade-Off
FMEA	Failure Modes and Effects Analysis
FRAM	Functional Resonance Analysis Method (in precedenza anche Functional Resonance Accident Model)
FTA	Fault Tree Analysis
HA	Hazard Analysis
HFCAS	Human Factor Analysis and Classification System
ICAO	International Civil Aviation Organization
MA	Markov Analysis
MORT	Management Oversight and Risk Tree
RCA	Root Cause Analysis
RCCA	Root Cause Corrective Action

SCM	Swiss Cheese Model
STAMP	Systemic Theoretic Analysis Model and Processes
STPA	Systems-Theoretic Processes Analysis

Capitolo I

Introduzione ai modelli ed ai metodi di analisi degli incidenti

1.1. Gli incidenti nei settori complessi ad alta tecnologia

Risale al 1653 la rilevante corrispondenza tra Fermat e Pascal sugli aspetti matematici della Teoria della probabilità: le modalità logiche di analisi proposte, i problemi sulla prevedibilità degli eventi formulati dai due scienziati costituiscono di fatto le fondamenta della *Risk Analysis* quantitativa moderna. Per Fermat e Pascal il tentativo notevole da conseguire è quello di conciliare il rigore proprio delle dimostrazioni della scienza con il concetto di "incertezza del caso". A partire da tali concezioni fondamentali, Christian Huygens svilupperà i suoi studi che saranno poi ripresi da altri illustri scienziati (ad esempio Bernoulli), fino ad arrivare al periodo contemporaneo.

Nella società contemporanea, il concetto di incidente rilevante coincide, in termini generali, con un evento inatteso e di natura disastrosa, caratterizzato da danni che possono riguardare gli esseri umani, i beni mobili ed immobili, i servizi e l'ambiente.

A partire dalla seconda guerra mondiale, il progresso scientifico e tecnologico ha portato gli esseri umani ad operare in contesti caratterizzati da sistemi, servizi ed organizzazioni cresciuti rapidamente in complessità, di pari passo con il relativo progresso delle tecnologie impiegate. È evidente anche che l'interazione dell'uomo con il contesto circostante (pensiamo ad esempio alle prestazioni richieste agli esseri umani) ha dovuto subire inevitabili trasformazioni. In particolare, i settori aerospaziale, dei trasporti navali, delle telecomunicazioni,

dell'energia nucleare, dell'industria chimica e petrolchimica (citando solo alcuni dei campi interessati) sono chiaramente riconosciuti come settori complessi ad alta tecnologia, e sono sottoposti a proprie e specifiche normative, a regole di indagine e norme di prevenzione finalizzate a rispondere alle esigenze naturali ed universalmente condivise di sicurezza. Con riferimento a tali contesti (per i quali la sicurezza è una condizione fondamentale di sviluppo ed esistenza), le *lessons learned* relative ad eventi non catastrofici e, purtroppo, le esperienze provenienti da incidenti di tipo maggiore (occorsi in uno specifico campo) hanno fornito nel tempo anche un contributo rilevante allo sviluppo e all'evoluzione dei cosiddetti modelli e metodi di analisi degli incidenti, *accident analysis models and methods*, utilizzando una terminologia largamente riconosciuta [1.15]. Altrettanto importanti risultano essere le forme di condivisione, tra i diversi settori ad alta tecnologia, delle esperienze e dei risultati conseguiti inizialmente in specifici contesti, anche in virtù degli apporti provenienti proprio dai suddetti modelli e metodi e dai relativi risultati prodotti dalla ricerca.

Un esempio interessante sia per gli aspetti tecnico-scientifici sia per la sua collocazione storica è fornito all'interno del lavoro di Norm W. Knox e Robert W. Eicher (1992), MORT- *Management Oversight and Risk Tree- User's manual* [1.9], nel quale gli autori ricordano che il concetto di *Fault Tree Analysis* (FTA) viene sviluppato in origine dai Bell Telephone Laboratories nel 1962 come metodologia mediante cui eseguire le valutazioni di sicurezza del "Minutemen Intercontinental Ballistic Missile Lauche Control System". Inoltre gli autori precisano che, in seguito al *Safety Simposium* del 1965 presso la University of Washington, nell'ambito del quale furono presentati diversi *papers* sulla FTA, quest'ultima ottenne il riconoscimento della possibilità di essere estesa proficuamente dal settore della *safety* aerospaziale a quello della *safety* dei reattori nucleari e di altri settori commerciali.

La condivisione delle esperienze provenienti da settori diversi assume pertanto un ruolo molto importante. Da tale punto di vista, gli incidenti nucleari rilevanti occorsi presso la Three Mile Island (USA, Marzo 1979) e presso Chernobyl (URSS, Aprile 1986), gli incidenti occorsi a due aeromobili B747 presso Tenerife (Canary Island, Marzo 1977) ed alla navetta Challenger (USA, Gennaio 1986), nonché l'incidente occorso presso lo stabilimento chimico Bhopal (India, Dicembre 1984) sono alcuni esempi di una nutrita lista spesso citati nella letteratura tecnica internazionale per aver contribuito a segnare impor-

tanti punti di svolta sia nelle concezioni di approccio all'intera dinamica degli incidenti complessi, sia per l'introduzione del maggiore peso nel contesto dell'indagine dei concetti delle precondizioni, dei fattori organizzativi e della cultura della sicurezza (*safety culture*) rispetto ai precedenti modelli predominanti, i quali tendevano a focalizzare in via preponderante l'attenzione sugli errori umani degli operatori finali (i cosiddetti operatori di *front-line*) oppure sui cedimenti finali di impianti e di componenti meccanici [1.2].

Inoltre, gli incidenti rilevanti hanno influito notevolmente sulla comprensione delle interazioni tra gli esseri umani ed i sistemi con i quali essi operano.

In ambito aerospaziale, il progresso degli aeromobili e dei relativi apparati è stato accompagnato da una crescente quantità di dati disponibili all'investigatore (e poi ai ricercatori), ad esempio attraverso i registratori di volo (*flight data recorders*). Di conseguenza, l'incremento dei dati e dei parametri di volo disponibili ha contribuito notevolmente al miglioramento della comprensione delle problematiche di interfaccia e di interazione tra uomo e sistemi (*hardware* e *software*) e delle dinamiche di prestazione dell'uomo nel proprio contesto operativo.

1.2. Le funzioni principali dei modelli e dei metodi di analisi degli incidenti

In termini generali e dal punto di vista formale, la funzione principale che i modelli di analisi degli incidenti (*accident models*) si propongono di assumere è quella di fornire una rappresentazione o uno schema concettuale dell'incidente, che supporti l'analista e l'investigatore nella comprensione della complessità dei meccanismi di *failure* eventualmente presenti nei vari livelli del sistema coinvolto, avendo a disposizione un approccio teorico (o in modo maggiormente rigoroso, una proposta di approccio) per una comprensione razionale degli eventi, nonché per l'individuazione delle possibili connessioni tra gli eventi stessi.

In ogni caso, un modello vuole essere una forma di rappresentazione della realtà, ed avrà, per definizione, dei limiti.

La funzione principale dei metodi di analisi degli incidenti (*accident methods*) è quella di fornire un processo pratico e razionale di analisi basato su una struttura ed un'impostazione definite, tali da gui-

dare l'analista e l'investigatore passo dopo passo nella ricostruzione logica e razionale delle condizioni e degli eventi culminanti nell'evento finale inatteso, o incidente. Pertanto, un metodo si propone di pervenire al raggiungimento di specifici risultati coerenti con le premesse, presentando le relazioni logiche e razionali che intercorrono tra cause ed effetti; essi sono strumenti o tecniche di approccio chiaramente pratici.

Generalmente, i metodi di analisi (quali strumenti o tecniche operative) sono fondati sull'approccio precedentemente definito da un modello (quale strumento teorico).

In particolare, in alcuni casi un modello definisce direttamente un proprio metodo, in altri casi un modello può costituire il fondamento per diversi metodi.

Tuttavia, un metodo può non avere necessariamente un legame con determinato modello [1.8].

L'ambito dei processi, metodi e tecniche della *Root Cause Analysis* o Analisi delle Cause Profonde (utilizzando la terminologia della norma CEI EN 62740: 2015) è di natura operativa, ed è rivolto all'identificazione ed alla classificazione delle cause degli eventi indesiderati, mediante la distinzione dei fattori causali in cause dirette, cause che contribuiscono (o cause concorrenti), e cause alla radice (o cause profonde), nonché alla definizione di appropriate azioni correttive finalizzate ad evitare che l'evento finale indesiderato possa ripresentarsi nuovamente.

Come sarà evidenziato nei prossimi capitoli, i processi di *Root Cause Analysis* si prestano anche alle analisi richieste e conseguenti alla rilevazione di una condizione di non conformità, dove l'accertamento di quest'ultima non costituisce, ovviamente, il punto di arrivo: tale condizione è il punto di partenza per la ricostruzione degli eventi finalizzata all'individuazione delle cause profonde.

In letterature tecnica si riscontra che un metodo di analisi può essere incluso tanto nelle classificazioni classiche dei metodi di analisi ed indagine degli incidenti quanto nelle classificazioni classiche delle tecniche di *Root Cause Analysis* (in seguito si affronterà anche il tema delle catalogazioni, della conseguente utilità e delle limitazioni). Le motivazioni di tali molteplici ed inevitabili classificazioni sono generalmente dovute sia alle potenzialità ed alle caratteristiche intrinseche della struttura operativa proposta da una determinata tecnica sia all'evoluzione ed all'impiego pratico che la tecnica stessa ha avuto nel