ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

The Boeing 737 MAX 8 Crashes

System-based Approach to Safety — A Different Perspective

Sanjeev Appicharla

System Safety Researcher

Abstract

This review article presents in a brief manner the lessons learnt from the Boeing 737 MAX 8 crashes using the System approach to safety perspective. Learning the right lessons from past accidents is a huge challenge from the organisational learning perspective; as Professor James Reason cautioned us, "Being blessed with both uninvolvement and hindsight, it is a great temptation for retrospective observers to slip into a censorious frame of mind and to wonder at how these people [i.e. those involved in design and development, safety assurance of these planes] could have been so blind, stupid, arrogant, ignorant or reckless" (Reason 1990, p.214). To distinguish it from the classical approach to safety, the "System approach" perspective used in the paper additionally includes human and organisational aspects. Drawing upon a brief review of case studies published by Chizek (2020) and Daniels (2020), this paper highlights the need to conduct accident case study analysis based upon the concept of System approach to safety. Such an approach will focus attention on two basic kinds of failures, namely, active and latent failures conditions. Latent failure conditions relating to human and organisational factors in particular refer to fallible decisions made at the higher levels of a socio-technical system; these were defined by Reason (1990, 1993). That identification of latent failure conditions, and addressing them, is a continuing challenge for both System safety research and System safety practice domains is also noted.

1 Introduction

From a systems engineering perspective, incorporating System safety, Human factors and Organisational factors (H & OF) into a comprehensive assessment process with a dynamic model to help implement pro-active risk management methods, is a research challenge posed to researchers and practitioners alike as noted, *inter alia*, by Rasmussen et al. (1994), Reason et al. (2006), and Leveson (2011).

The FAA Human Factors Team (1996) made some recommendations to improve aviation safety, including: "*In accident/incident investigations where human error is considered a potential factor, the FAA and the National Transportation Safety Board should thoroughly investigate the factors that contributed to the error, including design, training, operational procedures, the airspace system, or other factors. The FAA should encourage other organizations (both domestic and foreign) conducting accident/incident investigations to do the same. This recommendation should apply to all accident/incident investigations involving human error, regardless of whether the error is associated with a pilot, mechanic, air traffic controller, dispatcher, or other participant in the aviation system*".

© Sanjeev Appicharla 2023.

As an editor of the book on H & OF concerns, Gilbert (2020) noted the idea has been largely accepted in academia as well as in business that the main vulnerabilities in industrial safety come from human and organisational factors. Despite this acceptance, the H &OF perspective is not, in general, integrated into system safety as part of the systems engineering activity (Appicharla 2006) (Appicharla 2022b).

The system safety concept calls for a risk management strategy based on identification and analysis of hazards, with application of remedial controls using a systems-based approach (System safety 2007). The system safety discipline involves the application of special technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project, programme, or activity (Roland and Moriarty 1990) (FAA Safety Team n.d.). System safety engineering using techniques of systems engineering analyses a (socio-technical) system as an interacting set of elements generating hazards is described by Roland and Moriarty (1990).

Appicharla (2006) noted that a complex system or a situation may be approached from three perspectives:

1. the technical perspective (science, technology);
2. the organisational perspective (social, informal, or formal); and
3. the personal perspective (Individual, self).

To manage the complexity of the situation, all three perspectives need to be taken into account. Insights from each perspective cannot be obtained from other perspectives. Technical perspectives can be based on several models and data interpretations: "realities." From a systems point of view, all three perspectives need to be properly taken into account.

Assessing the safety of complex systems is of vital importance to stakeholders in many industry sectors, such as railway transportation, aviation, and other industries, where there is a likelihood that accidents can happen. These accidents may result in loss of lives and/or cause damage to property and the environment. Further, this approach is different from traditional safety strategies for simpler systems, which rely on control of conditions and causes of an accident based either on epidemiological analysis or as a result of investigation of individual past accidents (Rasmussen et al. 1994, Chapter 6) (System safety 2007).

This tendency to omit H & OF concerns from risk assessments and accident analysis can be seen from papers discussing two Boeing 737 MAX 8 accidents published by the Safety Critical System Club (Daniels 2020) (Daniel and Tudor 2022). Also, Appicharla (2022b) critiqued Chizek (2020) for omission of H & OF concerns and failing to identify latent failure pathways to both accidents.

At the end of Sub-section 4.4 of their paper "Software Reliability and the Misuse of Statistics", in the section on Requirements Engineering, Daniel and Tudor (2022) state:

> *Finally, in the two recent Boeing 737 MAX accidents on 29 October 2018 and 10 March 2019, the Manoeuvring Characteristics Augmentation System (MCAS) software implemented its requirements correctly, but the requirements caused full nose down trim to be applied following an Angle of Attack sensor failure (Daniels 2020). As Nancy Leveson has said, "Software-related accidents are usually caused by flawed requirements". It therefore follows that our efforts should be focused on writing better requirements. Formal methods can help with writing better requirements by using formal requirements languages with unambiguous semantics and formal methods tools that can ensure the requirements are complete and consistent.*

The author's objections to the above claim and arguments made about the two Boeing 737 MAX 8 accidents are threefold, as set out in the subsequent sections.

1. The first objection is that they did not pay attention to the H & OF called "latent failure conditions" that contribute to accidents[1] (Appicharla 2006) (Appicharla 2022b). The theme of paying attention to H & OF concerns through accident causation models is taken up in a greater detail herein at Section 2. Following from the first hypothesis is the corollary that systems engineering activity and its contribution to latent failures conditions is to be noted as well. This theme is taken up in Section 3.
2. The second objection is that that learning lessons from past accidents is not easy if such lessons learning exercise is subject to biases on the part of accident analysts or investigators, and this theme is discussed, inter alia, by Reason (1990), Leveson (2004b), and Johnson & Botting (1999). A dynamic model is introduced to show who how unsafe outcomes are produced using the control systems theory whilst discussing this objection in Section 4.
3. The third objection is related to the theme of estimating probabilities of unsafe outcomes and related biases in risk assessments. Biases in risk assessments and accident analysis emerge when companies seek to follow the ISO 31000 risk management standard as part of the systems engineering activity (ISO 31000:2018) (ISO/IEC/IEEE 15288:2015) (Conrow et al. 2021). This theme is taken up in Section 5.

2 Identification of Causal Factors

From a systems engineering perspective, the scope of accident analysis is the socio-technical system of which humans form a part directly, or indirectly through organisations, and interact either for utilisation or developing engineering systems through activities of thinking, problem solving, decision making and rely upon standards, models, methods, and frameworks to engineer acceptable systems (Rasmussen et al. 1994, p. xi) (ISO/IEC/IEEE 15288:2015).

Tozer and Wharton-Street (1993), drawing upon James Reason sponsored research, discussed the need for identifying latent failure conditions, as attention was focussed on active failures of front-line staff, but these staff are the inheritors of latent failures, not the source. They developed REVIEW, showing the sixteen distinct Railway Problem Factors[2]. The results of application of the REVIEW in the Australian railway sector were published by Edkins and Pollock (1996). However, the privatisation of British Railways is assumed to have impeded further developments on the application of pro-active safety risk management.

Tozer and Wharton-Street, (1993) discussed four shortcomings of the British Railways Safety Management System:

1. Current limited amount of feedback from ground-level staff.
2. Different perceptions of safety at each level of organisation.

[1] This objection is to details of the Daniels (2020) paper; Daniels and Tudor (2022) concentrate on whether one can quantify software reliability.

[2] The Railway Problem Factors are Training, Tools and equipment, Materials, Design, Staff communication, Rules, Supervision, Working environment, Staffing and rostering, Staff attitudes, Housekeeping, Planning, Departmental communication, Management, Contractors, Maintenance.

3. A general failure of management to recognise latent problems until accidents happen.
4. A reactive assessment of accidents.

Appicharla (2006) took up the concern of latent failure conditions and reactive approach to safety management and this is a continuing research theme for the author. With variety of theories, models and techniques being available for organisations to select from, it is understandable that under the concept of "Satisficing Behaviour" (Appicharla 2010) organisations may fail to integrate their knowledge base to inform their processes for accident prevention. An example of this lack of integrated knowledge base can be seen from the Network Rail (2016) Safety Central web page, Prevention through Engineering and Design. We find there that two different approaches, one at the level of disciplinary process level such as CDM Regulations[3] and another at the company level mandatory processes, the CSM-RA Regulation[4], are presented in the same graphic as providing input apart from the inputs from System safety engineering and Safety by Design Groups to the Prevention through Engineering and Design approach. Further, the web page describes the activity of Prevention through Engineering and Design is based on STAMP[5] related concepts and the concept of Szymbersk's Time-Safety Influence Curve, but extended to cover the asset whole-life and not just change phase. Various concepts and accident models are confused within the lifecycle activity on the web page, probably leading to an impasse in making progress in identifying and addressing the latent failure conditions.

In 2006, the author was surprised to learn that Airbus had applied a system approach at the aircraft level *for the first time* in the aviation industry, and thereby affirming a fly-fix-fly approach was the norm in the industry (Lawrence 2006, p.9) (Roland and Moriarty 1990).

Appicharla (2022b) suggested that the concept of System safety had its beginning with Bell Labs in the form of Fault Tree Analysis, and was adopted by Boeing dating back to 1962 (Ericson 2005). The aviation industry is a pioneering industry in terms of System safety techniques and its adoption of Fault Tree Analysis in the nineteen sixties led to its adoption by the nuclear industry, and subsequently by UK railways (Ericson 1999) (Ericson 2005) (Rasmussen 1981) (Leihton and Denis. 1993). However, integrating H & OF concerns was noted as a problem in the aviation industry by the FAA Human Factors Team (1996). The UK Human Factors Integration Defence Technology Centre[6] raised the HF concern as well (HFIDTC 2006). Despite these Guidance notes and recommendations, the practitioners' apparent lack of interest in H & OF concerns is a common theme in the accident literature (Reason et al. 2006) (Gilbert 2020). That Roland and Moriarty (1990) trace the history of System safety back to 1947 is to be noted.

A research paradigm effort to include all levels of a socio-technical system in system safety activity over the last few decades developed into what is called "Unbounded thinking" or "Systems thinking" or "System approach to safety" (Rasmussen et al. 1994) (Rasmussen 1997) (Appicharla 2010) (Leveson, 2011).

Jens Rasmussen (1997, Figure 1) developed a risk management framework integrating all the levels of socio-technical system involved in generating system hazard. Leveson (2011, Figure 2) presents an example of a hierarchical safety control structure involving all stakeholders in generating the system hazard. Leveson (2009) (2011) claims that chain of

[3] The Construction (Design and Management) Regulations 2015 — UK legislation

[4] The Regulation on a Common Safety Method for Risk Evaluation and Assessment — EU legislation

[5] Systems-Theoretic Accident Model and Processes

[6] The UK Human Factors Integration Defence Technology Centre (HFIDTC) is a virtual centre of excellence funded by the MOD which undertakes research to develop and evaluate processes methods and tools

events is included at all levels of system; Rasmussen (1997, Figure 1) is a limitation and her model overcomes this limitation. However, Leveson (2019) noted, while not required to start a CAST[7] analysis, identifying the proximate events preceding the loss may sometimes be useful in starting the process of generating questions that need to be answered in the accident investigation and causal analysis. Therefore, in light of the above discussions, the author's first objection is that the case study analysis of Boeing 737 MAX 8 accidents by Daniels (2020) does not capture all related causal factors.

The author's contention is that the contribution of all stakeholder organisations involved, all disciplines including systems engineering, software engineering and their contribution together with all other relevant causal factors to the accident flights as per the various levels of socio-technical system are required as per the System approach to safety. The question of subjective rule to where to stop in the search of causal factors in the accident investigation is addressed by Rasmussen (1997) includes all levels of a socio-technical system.

Sub-section 2.3 of the ICAO website "Safety Management System Implementation" (ICAO 2022) states on Accident Causation, thus:

> *Safety risks can be generated by active failures and latent conditions. The concept of accident causation is an active field of study, and many types of models exist to illustrate the events taking place leading up to an accident.*

As noted in the quotation above, Reason (1993) argued that modern high-hazard, low-risk systems (such as nuclear power, and chemical plants or contemporary 'fly by wire' commercial aircraft) are prone to breach of several defences due to unlikely combinations of two basic kinds of failures. These are known as active and latent failures or resident pathogens. Definition of these concepts are presented later in the section.

Appicharla (2006) accepted the idea that complex systems can suffer from 'organisational accidents': Complex system(s) are defined as integrated composites of components of people, processes, assets, procedures, rules, and organisations. Complex systems always suffer from latent failures (errors in the original) which pose greatest threat to the safety of the system. These failures combine with the active failure to give rise to what are known as 'organizational accidents' (see Figure 1, derived from (Reason, 1993)).

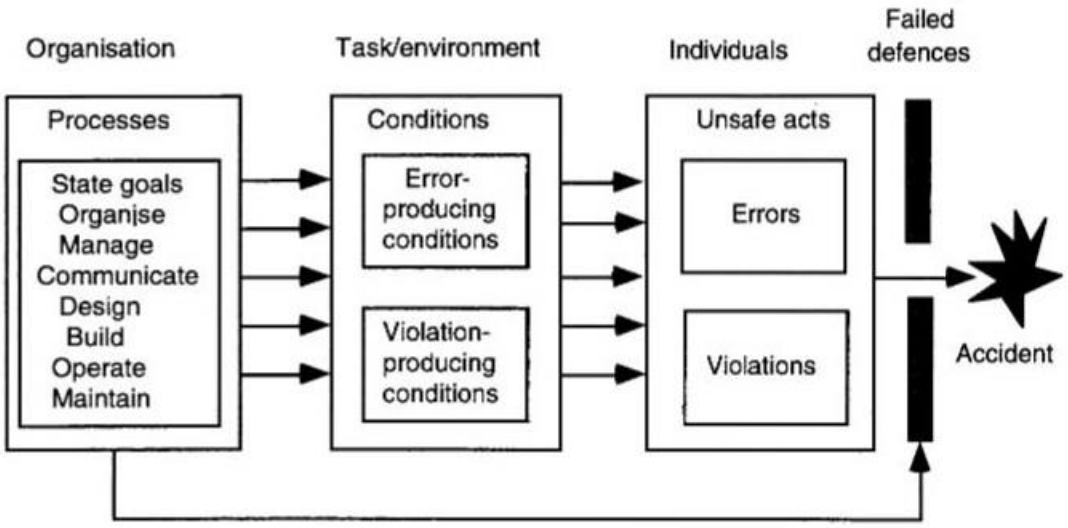


Figure 1 ~ Common Elements in the Development of Accident

[7] Causal Analysis based on System. Theory

The model of accident causation shown in Figure 1 is called the Swiss Cheese Model Mark II model by James Reason et al (2006). From the ICAO website quotation above, Reason's (1993) model of accident causation, and use of Swiss Cheese Model to investigate the 2002 Überlingen air accident and publication of the results in the EUROCONTROL Agency report, implies that both ICAO and EUROCONTROL accept the Swiss Cheese Model of Accident Causation as a framework for explanation.

James Reason, *et alia*, (2006) presented the history of Swiss Cheese Model and extended it to include international regulatory frameworks, and discussed the criticisms of the model and explanation of the Überlingen air accident in an open access article. Reason (1993) explained the development of the Swiss Cheese Model in terms of general pattern of accident causation advanced by Heinrich's (1931) "dominoes" model, the Bird & Germain (1985) model, and a fourth element of failed or absent defences was added to these models. Johnson (1973) focussed on management as being responsible for the planning of the context within which accidents unfold, that is, he stressed the role of 'less than adequate' management decisions and developed MORT, the 'Management Oversight and Risk Tree' tool, for accident analysis. Jens Rasmussen (1997), a cognitive systems engineering expert, commented on relations of the MORT technique and the Swiss Cheese Model to accident analysis, thus: "*The combination of the two basic views that (1) accidents should be understood in terms of an energy related process and (2) hazard management therefore should be directed towards planning of the release route*". Later Reason (1990) has focused analysis on management errors and organisational factors, such as 'resident pathogens making organisations vulnerable to accidents'.

The definitions of active and latent failure conditions are presented hereafter. These are presented here as the author learned that some professional systems engineers in the UK railway domain were not aware of these concepts[8].

Definition: James Reason (1993) defined **Active Failures**: unsafe acts committed by those at the "sharp end" of the system (pilots, air traffic controllers, ships' crews, train drivers, [signallers], control room operators, maintenance crews, and the like). They are the people who are at the human-system interface whose actions can do, and sometimes have immediate consequences. These may be acts of omissions or commissions on the part of front-line operatives.

Definition: James Reason (1993) defined **Latent Failures**: usually fallible decisions taken at the higher-level echelons of the organisation whose damaging or adverse consequences may lie dormant within the system for a long time, only becoming evident when they combine with local triggering factors (i.e. active failures, technical failures, atypical system states, etc.) to breach a system's defences.

In the safety research domain, we find that despite the criticism of the Swiss Cheese Model by Nancy Leveson, discussed by Reason et al. (2006), researchers continue to use the concept of latent failure conditions. For example, Swuste et al. (2020) stated on the theme of latent failures, thus: "*The origin of latent failures lies in the company's organisation and in its decision-making processes. Decision making within an organisation is determined by the context and limitations of the decision-makers, who tend to recycle known solutions for technical problems*" (Halpern 1989). These latent failures are present in a system for a long period of time without causing problems, but are activated in combination with other system failures, breaking through barriers. The psychologist

[8] In July 2022, communication with the UK INCOSE Railway Industry Group Chair revealed this fact prior to the INCOSE RIG Annual General Body Meeting. After explaining the meaning of the latent failure conditions or "resident pathogens" in systems engineering activity, the author addressed the AGM to consider the role of "resident pathogens" in systems engineering activity.

Reason described these latent failures using a medical metaphor: "*resident pathogens caused by designers, procedure writers, and top managers representing the 'blunt end' of an organisation*".

Reason (1993) noted that apart from the lifecycle errors in the system development and design processes that may occur[9], there would be cultural factors of competence, commitment, and cognizance that are impacted by the quality of decision making.

- Competence factor deals with organisational capability to meet the safety goals. Elements of such competence are related to the organisation processes and standards for systems engineering process and their application. Ericson (2005) describes the hazard identification and analysis techniques used by system safety professionals.
- Commitment relates to the motivation and resources for the pursuit of the safety goals in terms of either meeting regulatory targets or pursue leadership status in overcoming the hazards inherent in design and operations. Safety Management Policy, together with the ways and means to pursue the safety objectives define the motives. Most importantly, capability and commitment must be tailored to cognizance of hazards.
- Cognizance of hazards must include managerial attention to latent failure conditions contributed by means of human and organisational factors and their contribution to accidents. Senior managers must look beyond the active failures to understand the resident pathogens in organisational and management practices.

James Reason (1990, p.53-96) drawing upon the insights of economists, such as Daniel Kahneman and Herbert A. Simon and related human error research, developed a conceptual framework — the Generic Error Modelling System, "GEMS" — within which to locate the origin of basic human error types. Using Jens Rasmussen's skill-rules-knowledge classification of human performance, Reason (1990) mapped the three error types of slips and lapses, rule-based mistakes, and knowledge-based mistakes in the form of failure modes at the three levels of human performance a problem solver is likely to face, and determined their cognitive origins. Using these failure modes of skill-rules-knowledge-based mistakes, it is feasible for an accident analyst, using the data derived from the accident reports, to locate the cognitive origins of active and latent failures within this error classification system.

The quality of decision making and role of risk-based decision-making play in the organisational context was examined, *inter alia*, by James Reason (1990) and Charles Perrow (1999). Reason (1990, Chapters 2 & 3), Perrow (1999, Chapter 9), and Kahneman (2012b, Chapter 31) all discuss the role of risk policy, risk assessment, ways and means to address the problems of decision making. These referenced texts may be consulted to understand in a greater detail the sources of errors (biases and their sources) in decision making process in the industrial setting.

In this section, two types of failures, active failures and latent failures in terms of cultural factors, and their contribution to the development of accidents were briefly presented.

[9] Perrow (1999, p. 77) uses a DEPOSE (Design, Equipment Procedures, Operators, Supplies and materials, and Environment) framework to identify the potential sources of failures.

3 Systems Engineering Activity and Contribution to Latent Failures

Daniels and Tudor (2022) claim that behaviour specified by the requirements of the Boeing 737 MAX 8 caused full nose down trim to be applied following an Angle of Attack (AoA) sensor failure. Further, as noted in the introductory section, drawing upon Nancy Leveson's quote, they suggest improving the requirements engineering approach, because the software implemented requirements correctly, but this led to accidents. To illustrate their perception of this phenomena, they discuss two run-away accidents as well as the Boeing 737 MAX 8 crashes.

The Boeing 737 MAX 8 crashes, as per the ICAO classification of accidents, fall into the category of "Loss of Control in Flight" (Appicharla 2022b). Further, a previous paper by Daniels (2020, Sub-section 8.3.3) failed to recognise the Human-MCAS Interface failure but suggested how display of good airmanship skills by the ETH 302 accident flight crew could have saved the aircraft and its passengers. Analyses by Daniels (2020) and by Daniels and Tudor (2022) seems to contradict the concepts of System safety and ideas advanced by Leveson (2004a) (2011) as well as the official reports. This theme is taken up in the paragraphs to follow to illustrate the idea that safety of software is to be examined in the context of its use.

The abstract of Leveson (2004a) states:

> *The … most important step in solving any problem is understanding the problem well enough to create effective solutions. To this end, several software-related space-craft accidents were studied to determine common systemic factors. Although the details in each accident were different, very similar factors related to flaws in the safety culture, the management and organization, and technical deficiencies were identified. These factors include complacency and discounting of software risk, diffusion of responsibility and authority, limited communication channels and poor information flow, inadequate system and software engineering (poor or missing specifications, unnecessary complexity and software functionality, software reuse without appropriate safety analysis, violation of basic safety engineering practices in the digital components), inadequate review activities, ineffective system safety engineering, flawed test and simulation environments, and inadequate human factors engineering...*

Further, official reports cited the inadequate MCAS operations and design. For example the NTSB (2019) questioned the role of "*unintended MCAS operation*" and assumptions made by Boeing regarding MCAS operation. The NTSB reviewed sections of Boeing's system safety analysis of the stabilizer trim control that pertained to the MCAS on the Boeing 737 MAX 8 planes. The NTSB Review showed that the specific failure modes that lead to "*uncommanded MCAS activation*" were not simulated (such as an erroneous high AoA input to the MCAS) in the safety validation tests. This omission led to non-consideration of consequences of these failure conditions, i.e. additional flight deck effects (such as the IAS DISAGREE and ALT DISAGREE alerts, and stick shaker activation.

Firesmith (2010, p.115) discusses interactions between various team members participating in danger analysis. The author does not agree with the idea of abuse analysis used by Firesmith (2010) but accepts that, even from traditional safety engineering perspective, such a hazard analysis at Boeing Commercial Airplanes business division would have revealed the problems with the MCAS design and operations. But, from an organisational perspective, the economic imperative to compete on costs with Airbus may have resulted in a less than adequate safety culture perspective, and organisation dynamics may have driven the decision towards setting up of the latent failure pathway (Appicharla 2022b).

The JATR (2019) stated: "*The MCAS design was based on data, architecture, and assumptions that were reused from a previous aircraft configuration without sufficient detailed aircraft-level evaluation of the appropriateness of such reuse, and without additional safety margins and features to address conditions, omissions, or errors not foreseen in the analyses*". This finding has implications for inter-operable systems in the railways, but that is out of the scope of this paper.

Moreover, Johnston and Harris (2019) accept the idea that MCAS software played a role. They argued on the contribution of software to the crashes, thus:

> *The initial analyses suggest that the MCAS software system was poorly designed and caused two plane crashes. But this is a complex situation, involving many people and organizations. In addition, other pilots had successfully struggled against the MCAS system and safely guided their passengers to their destination. Four contributing factors, observed in the Boeing case, have also been observed in other catastrophic software failures. They are poor documentation, rushed release, delayed software updates, and humans out of the loop.*

The report produced for Peter A. Defazio, Chair of US Committee on Transportation and Infrastructure and Rick Larsen, Chair of Sub-Committee on Aviation, stated that: "*Boeing's software supplier, Collins Aerospace, also falsely believed that Boeing had communicated the AoA Disagree alert issue to its 737 MAX customers*" (US House Committee on Transportation and Infrastructure 2020, p.23).

In the following paragraphs, we look at important systems engineering tasks and their possible contribution to accidents, if not performed adequately.

Bahill and Henderson (2005) identified Requirements Development, Requirements Verification, Requirements Validation, System Verification, and System Validation as important systems engineering tasks. In their examination of twenty-three 'famous failures', they used the following 'definitions' to generate a classification system:

Requirements Development: A functional requirement has to define what, how well, and under what conditions one or more inputs must be converted into one or more outputs at the boundary being considered in order to satisfy the stakeholder needs. Besides functional requirements, there are dozens of other types of requirements. Requirements Development includes:

(1) eliciting, analysing, validating, and communicating stakeholder needs,

(2) transforming customer requirements into derived requirements,

(3) allocating requirements to hardware, software, bio ware, test, and interface elements,

(4) verifying requirements, and

(5) validating the set of requirements.

There is no implication that these five tasks should be done serially, because, like all systems engineering processes, these tasks should be done with many parallel and iterative loops.

Verifying Requirements: Proving that each requirement has been satisfied. Verification can be done by logical argument, inspection, modelling, simulation, analysis, [audit,] expert review, test, or demonstration.

Validating Requirements: Ensuring that

(1) the set of requirements is correct, complete, and consistent,

(2) a model can be created that satisfies the requirements, and

(3) a real-world solution can be built and tested to prove that it satisfies the requirements.

If Systems Engineering discovers that the customer has requested a perpetual-motion machine, the project should be stopped…

Verifying a System: Building the system right: ensuring that the system complies with the system requirements and conforms to its design.

Validating a System: Building the right system: making sure that the system does what it is supposed to do in its intended environment. Validation determines the correctness and completeness of the end product and ensures that the system will satisfy the actual needs of the stakeholders.

As per the above definitions, the report to the US House Committee on Transportation and Infrastructure. (2020, p.119) noted that MCAS did not meet its own design requirements. The Boeing Aerodynamics Stability & Control Requirements included:

- "*MCAS shall not have any objectionable interaction with the piloting of the airplane*." (US House Committee on Transportation and Infrastructure 2020, foot-note 708)
- "*MCAS shall not interfere with dive recovery*." (US House Committee on Transportation and Infrastructure 2020, foot-note 709)

Based on the admission of John Hamilton, then-Chief Engineer for the Boeing Commercial Airplanes division, that one of the above two design requirements were not met, the House Committee Report (ibid) concluded that MCAS was poorly designed, not adequately tested, and had received flawed oversight by the FAA.

Thus, the MCAS verification and validation contained mistakes in addition to the mistakes in Requirements development and Validating requirements of MCAS design at Collins Aerospace (US House Committee on Transportation and Infrastructure 2020).

Contrary to a claim by Daniels (2020) that the FAA ODA Organisation *was not* a contributor to the Boeing 737 MAX 8 crashes, the report produced for the US House Committee on Transportation and Infrastructure (2020) states that the FAA ODA Organisation Delegation Act *was* a contributor. Also, Leveson et al. (2019) observed:

> *For example, one possible factor that can be hypothesized as being part of the cause of the B737 MAX losses is that the past success of Boeing in promoting safety and a lack of adequate resources provided by Congress helped to convince the FAA to relax the oversight in the DER [Designated Engineering Representative] process, essentially changing it into a self-certifying process for Boeing. This process was probably fine at first but degraded over time by pressures on the company that conflicted with safety. It is this type of change that usually precedes an accident — the system slowly and inadvertently changes to one where an accident is inevitable. Basically, the system migrates slowly toward a state of higher risk. Doesn't that provide a more useful causal explanation than "the pilot zigged when he/she should have zagged"?*

Appicharla (2022b) noted that organisational dynamics playing out between the system safety engineers and the business unit management in the examination of hazard controls and this dynamic contributing a latent failure pathway to future accident scenarios; this was not studied by Johnston and Harris (2019). Therefore, given the evidences regarding the Boeing Aerodynamics Stability & Control Requirements, NTSB (2019) findings, JATR (2019) findings, and (in the context of Leveson (2004b) having introduced a new accident model to explain accidents based on control theory to replace the chain of event models), the hypothesis of improving the Requirements Engineering activity alone by Daniels and Tudor (2022) and Daniels (2020 is untenable. Further, such blame actions on a single discipline or organisation or aircraft crew cannot help us learn from adverse events

is noted by the Ergonomics and Human Factors society (CIEHF 2020). The argument to support this hypothesis are further discussed in Sections 4 and 5.

Appicharla (2022b) modelled the evidence(s) from the report produced for the US House Committee on Transportation and Infrastructure (2020) using the hybrid Swiss Cheese Model (Reason 1990) and the MORT technique (Johnson 1973). From a systems engineering perspective, the model showed following latent failures at the regulatory and systems integrator levels:

- The FAA's and Boeing's lack of leadership to enforce positive safety culture,
- Boeing's efforts to describe MCAS as simply an extension of the existing speed trim system was an effort to "*give shade and cover*" to the notion that MCAS in the 737 MAX 8 was not new,
- Boeing's reliance upon production pressures, failure to classify single point failures as safety-critical events, and failure to communicate risk to the airlines/operators based on less than adequate risk assessments, dismissal of warnings from the engineers,
- FAA regulatory failure to implement its own Human Factors team recommendations show that the commitment, capability, and competence of decision takers in all organisations involved was less than adequate, and
- The way the work objectives were set by Boeing and FAA shows that the senior managerial levels attitude towards duty of care towards their customers in the aviation industry by the FAA, Design Organisation and even Airlines/Operators was less than adequate.

McDermott, *et alia*, (2020) discussed the need of addressing cognitive biases in systems engineering teams. As an example, they briefly discussed the Space Shuttle Challenger accident as an example of randomness bias in engineering domain. Engineers' intuition regarding the correlation of seal failure with the low temperature at the time of launch could not be translated into the data to support the decision to delay the launch as per Appicharla (2012), McDermott et al. (2020).

4 Learning The Right Lessons From Past Accidents

My second objection to Daniels (2020) is that learning lessons from past accidents is not easy if such lessons learning exercise is subject to biases on the part of accident analysts or investigators, and this theme is discussed by Leveson (2004b), Johnson and Botting (1999), to name just a few academics in the System Safety discipline.

Synthesizing the work on the Swiss Cheese Model of accident causation and the MORT technique cited in the previous section, Sanjeev Appicharla (2022a) published a cybernetic risk model (see Figure 2, derived from that paper) adapted from Reason (1990) and Kahneman (2012a), and used it to study the Boeing 737 MAX 8 crashes.

The model assumes the knowledge base of controls system theory and introduces the "Heuristics and Biases" as disturbances in a control system theoretic representation. Further, the author's intention is to highlight the fact that a cognitive system approach to risk management is feasible conceptually. Due to space limitation, full results of the study cannot be presented here. Appicharla (2022b) may be consulted for the process used to derive the following results.

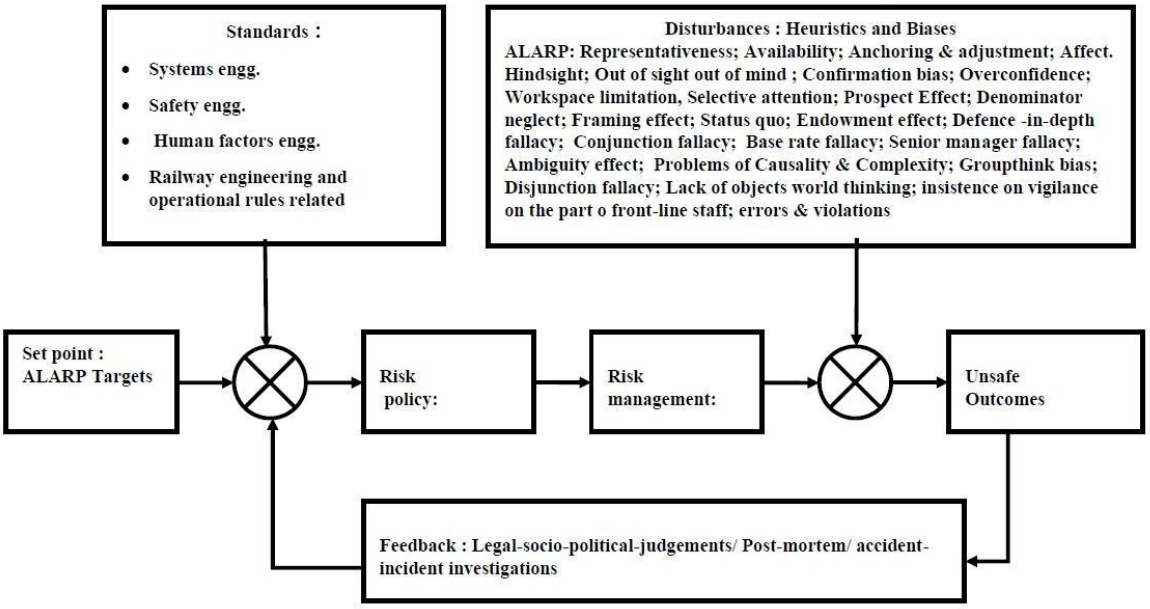


Figure 2~ Cybernetic Model of Risk Management

The following high level latent failures in the Boeing 737 MAX 8 crashes were identified using the cybernetic risk management model of Figure 2. Appicharla (2022b), drawing upon a management article by Sandra Sucher and Shalene Gupta (2021), presented a more-nuanced picture of the regulatory environment and the stakeholders involved with their contributions to what is called in risk literature as "system" or "organisational" accident (Perrow 1999, p. 70) (Reason, 1997) (Leveson, 2004a). The latent failures investigated at Boeing Board level and inadequate feedback from past accidents were:

- Boeing 737 MAX 8 airplane was a complex system product and an outcome of a safety culture prevailing at Boeing Commercial Airplanes that did not pay sufficient attention to the biases in its Engineering Review and Safety Review Boards.
- The Boeing board had five committees (Audit; Finance; Compensation; Special Programs; and Governance, Organization & Nominating). Audit oversaw risk, but its charter focused on financial risk, and it had no mandate to discuss safety. Moreover, the committee had no mechanism for receiving alerts from whistle-blowers. Several different airlines, including Southwest, JetBlue, and Delta have board committees specifically established to address safety. Boeing did not establish a board committee to address safety until 4th April 2019, which was six months after the first crash in Indonesia, and nearly a month after the second crash in Ethiopia. Instead, safety issues were reviewed by a "Safety Review Board" run by employees, which had neither a mandate nor a mechanism for reporting to the board. Meanwhile, the Boeing board was not even aware that the Safety Review Board existed until after the 737 MAX 8 had been grounded in 2019.
- Research shows that when there is an impending disaster, up to 70% of people enter a state of denial call the "normalcy bias". It is called "normalcy" because our desire to flee from disaster goes so deep that when a terrible event occurs our first instinct is to deny reality instead of dealing with it. And it's a "bias" because it interferes with our ability to imagine the scale and impact of a situation that we have never encountered before. Boards need to mitigate for the normalcy bias.
- Boards are fiduciaries, which means that their duty is to protect other people's interests, generally defined as consisting of a duty of care, a duty of loyalty, and some legal scholars would argue, a duty of candour. The responsibilities of boards that include

approving a company's strategy, budgets and plans and monitoring progress against them; approving the company's capital structure, major expenditures, and Merger & Acquisition activity; appointing the CEO and approving senior executive compensation; ensuring risks to the company are identified and managed; ensuring compliance with legal and community requirements; and establishing ethical standards for the company. Operationalizing these duties is harder than it sounds, and Boeing's fall from grace offered management lessons other boards can learn from.

- If Dekker (2009) had made his investigation into the Turkish Airlines TK1951 accident[10] public when he shared them with the academic community, then the Boeing and FAA business management level may have had a chance to reflect upon the single sensor-based architecture that was chosen. This document on the Turkish Airlines crash was made public only after the second 737 MAX 8 accident by the New York Times investigation. Therefore, the non-availability of Professor Dekker's report (Dekker 2009) became a contributory factor to the Boeing 737 MAX 8 accidents. That Boeing's decision to allow MCAS to operate off a single AoA sensor has been roundly criticized by a wide range of aviation safety experts is noted in the report produced for the US House Committee on Transportation and Infrastructure (2020, footnote 100).

Swuste et al. (2020) noted on the nature of cognitive system, thus:

> *Automation[11] does not decrease the incidence of major accidents but changes their nature. An example is the Turkish Airlines* [TK1951] *crash at Schiphol in 2009, caused by a conflict between the automated systems of the aircraft and pilots. Complexity is also caused by the different time scales of departments within a company, which are essential for the process or production. For example, workers, operators, drivers, and pilots have a time horizon of a few minutes in control rooms and cockpits. All operational problems and process disturbances at this level must be solved within a short period of time, adjusting process parameters, and detecting failing process components.*

Further, Daniels (2020) did not apparently use any accident models such as the Swiss Cheese Model (Reason, 1993), or consider the role of bias play in accident investigations (CIEHF 2020), apply systems thinking in the like manner of the Systems-theoretic model of Leveson (2004), or any other formal accident investigation model recommended by IEC 31010:2019 to investigate the causal and contributory causes. Daniels (2020) relied upon his own subject matter expert judgement. However, there is extensive risk literature available on the matter of applying the subjective matter expert judgement and limitation of such expertise (Kahneman 2012a), (Kahneman 2012b). Further, the application of the Swiss Cheese Model by Lawton and Ward (2005) enabled the Ladbroke Grove Inquiry to go beyond the single causal factor of SPAD caused by an active error on the part of train driver to several latent factors in the operational and management side of the organisation (HSC 2000).

Lawton and Ward (2005) argued that the net result of a systems-based analysis is a more comprehensive understanding of the crash in order to provide a more effective strategy for preventing future crashes by addressing all levels of factors and the critical interactions among them. Leveson (2004b) argued that a new approach is needed to human error is needed beyond the Swiss Cheese Model. However, Haddon-Cave (2009) used a hybrid model of bow-tie model (a fault and event tree model) and the Swiss Cheese Model to gain a more comprehensive understanding of the Nimrod Crash in Afghanistan.

[10] This accident was to a Boeing 737-800

[11] Sheridan and Parasuraman (2006) may be consulted regarding definition of automation and automation related incidents and accidents.

Subsequently, CIEHF (2017) expressed concerns with current practices of bow-tie analysis. Further, the CIEHF Working Group noted that the Swiss Cheese Model has found widespread application and is still used globally as a means of thinking about safety management (CIEHF 2017). It has however been developed and elaborated in many directions: while the core ideas continue to have great value and are easily understood, variations of the model are now in widespread use. Leveson (2019) argued against the use of chain of event models for their inability to represent process errors. For example, Leveson et al. (2019) state, thus:

> *Can we really explain the B737 MAX accidents with a simple chain of events, with the pilot actions highlighted along with perhaps the MCAS design as the only actions worthy of attention? Competitive pressures, regulatory policies, basic design features are not 'events', so they don't appear in the chain of events and therefore can be dismissed without consideration by those who find it convenient to ignore these factors?*

The Daniels and Tudor (2022) citation of Nancy Leveson was out of context, was done without giving reference to her paper, and is based on the premise that, "*Software-related accidents usually caused by flawed requirements*" and concluded erroneously that "*requirements engineering needs improvement*". This is a classic error in logic where the conclusion does not follow from premise as noted by Kahneman (2012b) and Leveson (2019) clearly rejects the conclusion can be seen from the previous paragraph as well.

CIEHF (2020) discussed, in their white paper, system engineering principle #4 thus: "*Most adverse events in socio-technical systems are systemic. They arise through the relationship and interactions between numerous functional elements involved in delivering the overall purpose of the system (Reason 1997)*".

Omission bias and confirmation bias on the part of Daniels and Tudor (2022) through their neglect of MCAS design requirements as stated in the Boeing Aerodynamics Stability & Control Requirements, and affirming Nancy Leveson's hypothesis of "*Software-related accidents usually caused by flawed requirements*", without considering the interaction between the regulatory and regulated organisations (See Section 4). Review the literature; it is clear that the learning of lessons from Boeing 737 MAX 8 accidents has been less than adequate.

5 Probability Distribution Model in Probabilistic Risk Assessments

My third objection is related to measure of risk in risk assessments. Daniels and Tudor (2022) cite Mandelbrot and Hudson (2004) who claim thus:

> *…the mathematical models used were flawed and that it was mistaken to assume that the normal distribution was a useful model for tracking price changes in the stock markets. Most economists responded that independence and normality are just assumptions that help simplify the mathematics. However, the inappropriate application of the normal distribution underestimated the probability that many borrowers would default on their subprime mortgages at the same time.*

Estimation of probabilities of rare or adverse events is not an easy task. Measuring risk in terms of F-N[12] curve statistics (Evans 2003), or in terms of Normal distribution curve applied to the stock market movements are fallible in nature. That point estimation of risk

[12] F-N curves are graphs relating the probability per year of causing N or more fatalities (F) to N.

can lead to erroneous perception of risk is noted by Rasmussen (1981). Despite these facts, the above claim by Daniels and Tudor (2022) is erroneous as taken up in this section.

As regards 2008 financial crisis, it is a mistake on the part of Daniels and Tudor (2022) to draw conclusion based just two factors to explain the crisis: (1) of inappropriate application of the normal distribution; and (2) many borrowers would default on their subprime mortgages at the same time, without considering all other factors that contributed to the 2008 financial crisis.

Disciplines of cognitive psychology, economics, social psychology, and statistical analysis relying upon the two-system model of human thinking provide a better explanation of 2008 financial crisis where collective blindness to risk and uncertainty developed. Kahneman (2012b, p. 262 & Chapter 24) may be consulted for psychological factors of planning fallacy, optimism bias, overconfident forecasts, and how risk-taking phenomenon emerged in the financial industry. David Hand stated that the probabilities of 25 standard deviation events that occurred in August 2007 were better predictable using the Cauchy distribution (Hand 2015, Chapter 7). It is true that Mandelbrot (2005) uses the fractal model of risk to better represent the risk phenomenon, but science cannot be limited to fitting statistical curves to the data[13] in a parsimonious manner without considering the social and organisational factors involved (Kahneman 2012a), (Gilbert 2020). Further, Gaussian normal distribution is used in physics and the reference cited in the footnote may be consulted.

Future Nobel laureate Eugene Fama (1965) commented on the Mandelbrot's hypothesis, thus: "*In light of this* [stable Paretian distribution] *discussion we see that Mandelbrot's hypothesis can actually be viewed as a generalization of the central-limit theorem arguments of Bachelier and Osborne to the case where the underlying distributions of price changes from transaction to transaction are allowed to have infinite variances. In this sense, then, Mandelbrot's version of the theory of random walks can be regarded as a broadening rather than a contradiction of the earlier Bachelier-Osborne model*".

Further evidence that Daniels and Tudor (2022) concept of risk measurement needs improvement comes from the research on F-N curves by Professor Andrew Evans for a UK HSE Research project. Using the putative model of risk, Andrew Evans placed a constraint on the use of F-N curves for taking decisions on the risk (Evans 2003). Weakness of bow-tie (fault and event tree) based models in their treatment of human errors was highlighted by (Reason,1990). CIEHF (2017) concerns were noted in the Section 4 may be recalled here.

Moreover, Daniels and Tudor (2022) do not pay attention to concepts of organisational leaning and psychological safety (Edmondson et al. 2005)[14]. The role played by the concept of bounded rationality and satisficing behaviour (Simon 1979) in risk management was noted in the SCSC Newsletter (Appicharla 2010). Contrary to rational human cognition, the tendency of firms is to settle for satisfactory option than choose an optimal course of action is to be recognised. Less than adequate awareness of emergent property of system safety using the analogy of water that has properties to support life and at the same time has the hazard potential to cause floods and devastation was discussed in the context of ALARP risk-based decision taking. And the role of less than adequate interaction between technical understanding, decision maker's risk preferences and organisational viewpoint that form three components of a firm to trigger hazard potential

[13] For discussions on the roots of science, Chapters 1 and 34 of Penrose (2004) may be consulted. Penrose, R. (2004). *The Road to Reality: A complete guide to the laws of the universe*. Jonathan Cape, Random House, London.

[14] This is understandable, considering that it is a paper concentrating on the reliability of software.

and it was argued that action to prevent the drift into the unsafe operating zone is necessary to keep risk level tolerable.

In terms of the main lesson for their organisation and management, senior management and boards must pay attention to fiduciary duty of care towards their customers and staff (Appicharla 2022b). Further, understanding and modelling of automation-human interaction is challenging in nature due increased automation (Sheridan and Hennessey 1984) leading to greater complexity (Perrow 1999), and systems are prone to latent failures apart from fallible managerial decisions due to host of factors such as less than adequate understanding of human automation interaction (Bainbridge 1997), systems becoming opaque (Rasmussen 1988), computer being at the centre of action (Moray 1986), increased use of multiple automatic safety devices (Rasmussen and Pedersen,1984) leading to less than adequate human supervision of automated systems, maintenance related omissions (INPO 1983), and the operator in the control room takes up co-ordinating activity during emergencies and temporal judgements may be prone to error (Javaux and De Keyser 1998) (Reason,1990). The study of automation-human interaction is an active research area in search of an objective function of human automation interface property (Bolton et al. 2013).

From the foregoing paragraphs, it can be concluded that improvement of the requirements engineering practice or using the right probability distribution to model the risk phenomenon may be necessary but not sufficient solutions because there are several other cognitive biases (see Figure 2) that may impact decision making in an adverse manner. Therefore, the risk management discipline needs to take a system approach to safety.

6 Conclusion

In conclusion, we should be advancing models that include human, technical *and* organisational factors, *and their interactions*, when assessing the risks posed by complex systems.

Note that the concept of System-based approach to safety management is not new and goes back at least seventy years (Roland and Moriarty 1990). See also Ericson (2005) and Appicharla (2006; 2010; 2022a; 2022b).

Acknowledgments

The author thanks the editor and peer reviewers for many useful suggestions on the earlier drafts of the paper. The author also expresses gratitude to professors from his college, Karnataka Regional Engineering College, Surathkal, India.

Figure 1 herein was derived from Reason (1993), the copyright holder of which is Springer-Verlag Berlin Heidelberg.

References

Appicharla S. K. (2006). *System for Investigation of Railway Interfaces*. 2006 1st IET International Conference on System Safety. London. pp. 7-16. https://ieeexplore.ieee.org/document/4123683.

Appicharla S. (2010). *Letters to Editor - Tolerability of Risk: ALARP. Safety Systems*. The Safety-Critical Systems Club Newsletter. SCSC-112. May 2010, 19(3), pp. 8-10.

Appicharla S. (2012). *Analysis and Modelling of NASA Space Shuttle Challenger Accident using Management and Oversight Risk Tree (MORT)*. 7th IET International System Safety Conference (p. 8). Edinburgh: IET. Retrieved 7th May 2013 from https://ieeexplore.ieee.org/document/6458956

Appicharla, S. K. (2022a). *From Nobel Prize (s) to Safety Risk Management: How to Identify Latent Failure Conditions in the Railway Safety Risk Management Practices*. 13th World Congress on Railway Research (WCRR) (p.6). Birmingham: (Proceedings volume is still under development at time of writing; a pre-print is available at https://www.researchgate.net/publication/361230614_From_Nobel_Prizes_to_Safety_Risk_Management_How_to_Identify_Latent_Failure_Conditions_in_the_Railway_Safety_Risk_Management_Practices).

Appicharla S. (2022b). *Lessons Learnt from Boeing 737 MAX 8 Crashes as Safety Data: Needles in the Haystack*. International System Safety Conference ISSC-2022 Safety Data: Needles in the Haystack, August 18th, 2022, Cincinatti, Ohio (Proceedings volume is still under development at time of writing; a pre-print is available at https://www.researchgate.net/publication/362833335_Lessons_Learnt_from_Boeing_737_Max_8_Crashes_as_Safety_Data_Needles_in_the_Haystack).

Bahill A. T., and Henderson S. J. (2005). *Requirements Development, Verification, and Validation Exhibited in Famous Failures.* Systems Engineering, 8(1), Retrieved 30th March 2012 from http://sysengr.engr.arizona.edu/publishedPapers/FamousFailures.pdf.

Bainbridge L. (1997). *The change in concepts needed to account for human behavior in complex dynamic tasks*. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on. 27(3), pp. 351 - 359. DOI:10.1109/3468.568743

Bird F. E., and Germain G. L. (1985). *Practical Loss Control Leadership*. Loganville, GA: International Loss Control Institute, Inc.

Bolton M. L., Bass E. J., and Siminiceanu R. I. (2013). *Using formal verification to evaluate human-automation interaction: A review*. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 43(3), pp. 488-503. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6472094

CIEHF. (2017). *Human Factors in Barrier Management*. White Paper. The Chartered Institute of Ergonomics & Human Factors (CIEHF). Retrieved 5th September 2022, from: https://ergonomics.org.uk/resource/human-factors-in-barrier-management.html

CIEHF. (2020). *Learning from Adverse Events*. White Paper. The Chartered Institute of Ergonomics & Human Factors (CIEHF). Retrieved 5th September 2022 from https://ergonomics.org.uk/resource/learning-from-adverse-events.html

Chizek M. (2020). *Tutorial: 737 MAX Case Study - Lessons for Safety Professionals*. 38th International Systems Safety Conference. St. Paul, MN 55114. Retrieved 31st March 2021 from https://system-safety.org/store/viewproduct.aspx?ID=17536206.

Conrow E., Madachy R., Roedler G., and Turner R. (2021, May 19th). *Risk Management*. Retrieved 9th December 2022from https://www.sebokwiki.org/wiki/Risk_Management.

Daniels D. (2020). *The Boeing 737 MAX Accidents*. Proceedings of SSS'20, the Twenty-eighth Safety-Critical Systems Symposium, York, UK. Accessed 9th November 2021 from https://scsc.uk/rp154.1:1.

Daniels D., and Tudor N. (2022). *Software Reliability and the Misuse of Statistics*. Safety-Critical Systems eJournal 1(1), SCSC-174, Safety-Critical Systems Club, January 2022. Available from https://scsc.uk/r174.3:1. Accessed 14th July 2022.

Dekker S. (2009). *Report of the Flight Crew Human Factors Investigation Conducted for the Dutch Safety Board into the Accident of TK1951, Boeing 737-800 near Amsterdam Schiphol Airport, February 25, 2009*. Lund University. Retrieved 15th May 2022 from https://www.onderzoeksraad.nl/en/media/inline/2020/1/21/human_factors_report_s_dekker.pdf

Edkins G. D., and Pollock G. M. (1996). *Pro-active safety management: Application and evaluation within a rail contex*t. Safety Science, 24(2), 83-93. Retrieved 9th April 2021, https://www.sciencedirect.com/science/article/abs/pii/S0925753596000276

Edmondson A., Ferlins E., Feldman L., and Bohmer R.(2005). *The Recovery Window: Organizational Learning Following Ambiguous Threat*s. In Farjoun M., and Starbuck *W.* (Editors). *Organization at the Limit: Lessons from the Columbia Disaster*. pp. 220–245. Wiley-Blackwell.

Ericson C. A. (1999). *Fault Tree Analysis – A History*. Retrieved 12th May 2022, from https://ftaassociates.files.wordpress.com/2018/12/C.-Ericson-Fault-Tree-Analysis-A-History-Proceedings-of-the-17th-International-System-Safety-Conference-1999.pdf

Ericson C. A. (2005). *Hazard Analysis Techniques for System Safety*. First Edition. New Jersey: Wiley & Sons. ISBN 0-471-72019-4

Evans A. W. (2003). *Transport fatal accidents and FN-curves: 1967-2001*. UK HSE Research Project 073. Health & Safety Executive. Retrieved 28th July 2021 from https://www.hse.gov.uk/research/rrpdf/rr073.pdf

FAA Human Factors Team. (1996). *The Interfaces Between Flightcrews and Modern Flight Deck Systems*. Federal Aviation Administration Human Factors Team Report. Retrieved May 15th, 2022, from https://www.tc.faa.gov/its/worldpac/techrpt/hffaces.pdf.

FAA Safety Team. (n.d.). *System Safety Process*. Retrieved 12th December 2022, from https://www.faasafety.gov/gslac/alc/libview_normal.aspx?id=6877.

Fama E. F. (1965). *The Behavior of Stock-Market Prices*. The Journal of Business, Vol. 38, No. 1 (Jan. 1965), pp. 34-105. Retrieved 20th September 2022 from https://www.jstor.org/stable/2350752

Firesmith D. G. (2010). *Engineering Safety- and Security-Related Requirements for Software-Intensive Systems*. One-Day Tutorial 32nd International Conference on Software Engineering, 4th May 2010. Retrieved 10th December 2022 from https://resources.sei.cmu.edu/asset_files/presentation/2010_017_001_23269.pdf

Gilbert C. (2020). *What Is the Place of Human and Organisational Factors in Safety? An introduction.* Retrieved 28th February 2022 from https://link.springer.com/content/pdf/10.1007%2F978-3-030-25639-5.pdf.

Haddon-Cave C. A. (2009). *The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006*. London: The Stationery Office. Retrieved 25th December 2019 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf

Halpern J. J. (1989). *Cognitive factors influencing decision making in a highly reliable organization*. Industrial Crisis Quarterly, 3(2), pp. 143–158. https://doi.org/10.1177/108602668900300204.

Hand D. (2015). *The Improbability Principle: Why coincidences, miracles and rare events happen all the time*. London: Penguin. ISBN 9781448170661.

Heinrich H. W. (1931). *Industrial accident prevention; a scientific approach*. First Edition. McGraw-Hill, New York, 1931.

HFIDTC. (2006). *Cost Arguments and Evidence for Human Factors Integration*. UK Human Factors Integration Defence Technology Centre. Wiltshire: Systems Engineering & Assessment Ltd.

HSC. (2000). *The Ladbroke Grove Rail Inquiry: Part 1 Report of The Rt Hon Lord Cullen PC*. Health & Safety Commission (HSC). Accessed 1st October 2022 from https://www.jesip.org.uk/wp-content/uploads/2022/03/Ladbroke-Grove-Rail-Inquiry-Report-Part-1.pdf.

ICAO. (2022). *Safety Management Implementation*. ICAO, The International Civil Aviation Organization. Uniting Aviation website accessed 26th September 2022 from https://www.unitingaviation.com/publications/safetymanagementimplementation/content.

IEC 31010:2019. *Risk management — Risk assessment techniques*. ISO 31010, Edition 2. International Electrotechnical Commission. Geneva.

INPO. (1983). *An Analysis of Root Causes in 1983 Significant Event Reports* (INPO 84-027), plus addendum. Institute of Nuclear Power Operations. Atlanta, GA.

ISO/IEC/IEEE 15288:2015. *Systems and software engineering — System life cycle processes*. ISO/IEC/IEEE 15288, Edition 1. International Organization for Standardization and International Electrotechnical Commission. Geneva. Institute of Electrical and Electronics Engineers. New York 2015.

ISO 31000:2018. *Risk management — Guidelines*. ISO 31000, Edition 2. International Organization for Standardization. Geneva. Retrieved July 17th, 2022, from https://www.iso.org/standard/65694.html.

JATR. (2019). *Boeing 737 MAX Flight Control System, Observations, Findings, and Recommendations*. Joint Authorities Technical Review. Retrieved 4th September 2020 from U.S. Federal Aviation Administration website: https://www.faa.gov/news/media/attachments/Final_JATR_Submittal_to_FAA_Oct_2019.pdf

Javaux D., and De Keyser V. (1998). *Complexité et conscience de la situation*. Rapport final SFACT/DGAC.

Johnson C. W., and Botting R. M. (1999). *Using Reason's Model of Organisational Accidents in Formalising Accident Reports*. Retrieved 9th September 2022 from https://link.springer.com/article/10.1007/s101110050037.

Johnson W. G. (1973) *The Management Oversight And Risk Tree – MORT*. United States Atomic Energy Commission. Retrieved 25th January 2023 from https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/MORT%20Bill%20Johnson%20for%20AEC%201973%20SAN8212.pdf.

Johnston P and Harris R. (2019). *The Boeing 737 MAX Saga: Lessons for Software Organizations*. Retrieved 1st October 2022 from https://embeddedartistry.com/wp-content/uploads/2019/09/the-boeing-737-max-saga-lessons-for-software-organizations.pdf.

Kahneman D. (2012a). *Of 2 Minds: How Fast and Slow Thinking Shape Perception and Choice [Excerpt]*. Scientific American, June 15. Retrieved 18th September 2022 from https://www.scientificamerican.com/article/kahneman-excerpt-thinking-fast-and-slow/

Kahneman D. (2012b). *Thinking, Fast and Slow*. London: Penguin Books.

Lawton R., and Ward N. J. (2005). *A systems analysis of the Ladbroke Grove rail crash*. Elsevier Accident Analysis & Prevention, 37(2), 235-244. Retrieved 18th May 2022 from https://www.sciencedirect.com/science/article/abs/pii/S0001457504000879

Lawrence B. M. (2006). *A380 Aircraft Safety Process*. 2006 1st IET International Conference on System Safety. London. pp. 96-115. Retrieved 4th September 2020 from https://ieeexplore.ieee.org/document/4123694

Leihton C. L., and Denis C. R. (1993). *Risk assessment of a new high-speed railway*. IMA Journal of Management Mathematics, 5(1), pp. 211-225. Retrieved 22nd April 2021 from https://academic.oup.com/imaman/article-abstract/5/1/211/804267

Leveson N. G. (2004a). *The Role of Software in Spacecraft Accidents*. Journal of Spacecraft and Rockets, 41(4), 564-575. Accessed 1st October 2022 from http://sunnyday.mit.edu/nasa-class/jsr-final.pdf.

Leveson N. G. (2004b). *A New Accident Model for Engineering Safer Systems*. Safety Science, 42(4), 237-270. Retrieved 15th May 2019 from http//sunnyday.mit.edu/accidents/safetyscience-single.pdf.

Leveson N. G. (2009). *Engineering a Safer World: Systems Thinking Applied to Safety*. Retrieved 12th December 2022 from http://sunnyday.mit.edu/safer-world.pdf

Leveson N. G. (2011). *Applying Systems Thinking to Analyse and Learn from Events*. Safety Science, 49(1), 55-64. Retrieved 1st December 2021 from http://sunnyday.mit.edu/Safety-Science-Events.pdf.

Leveson N. G. (2019). *CAST Handbook: How to Learn More from Incidents and Accidents*. MIT. Retrieved 25th August 2021 from http://sunnyday.mit.edu/CAST-Handbook.pdf.

Leveson N. G., Straker D., and Malmquist S. (2019). *Updating the Concept of Cause in Accident Investigation*. International Society of Air Safety Investigators (ISASI), The Hague. Retrieved 18th September 2022 from http://sunnyday.mit.edu/ISASI-Cause.pdf.

Mandelbrot B. B. (2005). *Parallel cartoons of fractal models of finance*. Annals of Finance 1, 2005. pp. 179–192. Retrieved 18th September 2022 from https://link.springer.com/article/10.1007/s10436-004-0007-2

Mandelbrot B. B., and Hudson R. L. (2004). *The (Mis)Behavior of Markets: A Fractal View of Risk, Ruin and Reward*. New York: Basic Books.

McDermott T. A., Folds, D. J., and Hallo L. (2020). *Addressing Cognitive Bias in Systems Engineering Teams*. INCOSE International Symposium, 30(1), 257-271. Retrieved 23rd May 2021 from https://doi.org/10.1002/j.2334-5837.2020.00721.x

Moray N. (1986). *Monitoring behavior and supervisory control*. In K. R. Boff, L. Kaufman, & J. P. Thomas (Eds.), *Handbook of perception and human performance*, Vol. 2. *Cognitive processes and performance.* (pp. 1–51). John Wiley & Sons.

Network Rail. (2016). *Prevention through Engineering and Design*. Safety Central. Retrieved 11th December 2022, from https://safety.networkrail.co.uk/safety/prevention-through-engineering-and-design

NTSB. (2019). *Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance*. Safety Recommendation Report ASR-19-01. The National Transportation Safety Board. Retrieved 8th March 2020 from https://www.ntsb.gov/investigations/AccidentReports/Reports/ASR1901.pdf

Perrow C. (1999). *Normal Accidents; Living with High-Risk Technologies*. Princeton: Princeton University Press. Second Edition. ISBN 9780691004129

Rasmussen J. (1988). *Coping Safely with Complex Systems*. American Association for Advancement of Science, Annual Meeting, Boston, February 1988; In: Risø-M-2769, https://backend.orbit.dtu.dk/ws/portalfiles/portal/137538338/COPESAF.PDF

Rasmussen J. (1997). *Risk management in a dynamic society: a modelling problem*. Safety Science. 27(2-3), pp. 183-213. Retrieved 4th July 2020 from http://sunnyday.mit.edu/16.863/rasmussen-safetyscience.pdf.

Rasmussen J., and Pedersen O. M. (1984). *Human Factors in Probabilistic Risk Analysis and in Risk Management*. In: Operational Safety of Nuclear Power Plants. Vol. 1, pp. 181-194, IAEA, Wien, 1984.

Rasmussen J., Pejtersen A. M., and Goodstein L.P. (1994). *Cognitive Systems Engineering*. New York: John Wiley and Sons, Inc.

Rasmussen N. C. (1981). *The application of probabilistic risk assessment techniques to energy technologies*. Ann. Rev. Energy. 1981. 6:123-38. Retrieved 12th May 2022 from https://www.annualreviews.org/doi/pdf/10.1146/annurev.eg.06.110181.001011

Reason J. (1990). *Human Error*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139062367.

Reason J. (1993). *The Identification of Latent Organizational Failures in Complex Systems*. In: Wise J.A., Hopkin V.D., Stager P. (editors) *Verification and Validation of Complex Systems: Human Factors Issues*. NATO ASI Series, Vol 110. pp. 223-237. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-02933-6_13.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Chapter 1: *Hazards, Defences and Losses*. Retrieved 22nd August 2020 from https://www.taylorfrancis.com/

Reason J., Hollnagel E., and Pariès J. (2006). *Revisiting the "Swiss Cheese" model of accidents*. EUROCONTROL Experimental Centre (EEC). 2006-017EEC Note 2006/13. Available via https://www.eurocontrol.int/publication/revisiting-swiss-cheese-model-accidents Accessed 24th January 2023.

Roland H. E., and Moriarty B. (1990). *System Safety Engineering and Management*. Second Edition. New York: John Wiley & Sons, Inc. Retrieved 25th December 2007 from https://onlinelibrary.wiley.com/doi/book/10.1002/9780470172438.

Sheridan T. B., and Hennessy R. T. (1984). *Research and Modelling of Supervisory Control Behavior. Report of a Workshop*. National Research Council, Washington. Retrieved 25th January 2023 from https://apps.dtic.mil/dtic/tr/fulltext/u2/a149621.pdf.

Sheridan T. B., and Parasuraman, R. (2006). *Human-automation interaction*. Reviews of Human Factors and Ergonomics, Volume 1, Issue 1, pp. 89-129. Retrieved 25th January 2023 from https://doi.org/10.1518/155723405783703082 1

Simon H. A. (1979). *Rational decision making in business organizations*. The American Economic Review. 69 (4), pp. 493–513. https://www.jstor.org/stable/1808698

Sucher S. J., and Gupta S. (2021). *What Corporate Boards Can Learn from Boeing's Mistakes*. Harvard Business Review, 2nd June 2021. Retrieved 2nd December 2021 from https://hbr.org/2021/06/what-corporate-boards-can-learn-from-boeings-mistakes

Swuste P., van Gulijk C., Groeneweg J., Zwaard W., Lemkowitz S. and Guldenmund F. (2020). *From Clapham Junction to Macondo, Deepwater Horizon: Risk and safety management in high-tech-high-hazard sectors: A review of English and Dutch literature: 1988–2010*. Elsevier Safety Science Vol. 121 January 2020, pp.249-282. Accessed 1st October 2022 from https://doi.org/10.1016/j.ssci.2019.08.031

System safety. (2007). *System safety*. Version ID: 931313550. In Wikipedia. https://en.wikipedia.org/wiki/System_safety Retrieved 15th March 2020.

Tozer S., and Wharton-Street D. (1993, October). *Development of pro-active system for measuring organisational safety health in a railway environment*. Retrieved 11th December 2022, via: https://www.sparkrail.org/Lists/Records/DispForm.aspx?ID=19944.

US House Committee on Transportation and Infrastructure. (2020). *Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX*. US House of Representatives. Washington DC. Retrieved 20th September, 2020, from https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf.