ISSN 2754-1118
Vol.2 No.1

The Safety-Critical Systems Club

SAFETY-CRITICAL SYSTEMS eJOURNAL

SCSC

ISSN 2754-1118 Vol.2 Iss.1

Editorial to the 2023 Winter Issue

Welcome to the first issue of the second volume of the Safety-Critical Systems eJournal, which is published by the Safety Critical Systems Club (SCSC).

We have a new cover image for this volume, designed by Alex King. It has an environmental theme to mark the Club's new Working Group, which started up last Summer. The Systems Approach to Safety of the Environment Working Group is intending to apply Systems Safety practices to systems that are embedded within the natural environment, while focussing on that environment. The group aims to produce clear guidance on how engineered systems should be developed and managed throughout their entire lifecycle so as to preserve, protect and enhance the environment. If you would like to join, or find out more about this group, please go to their page on the SCSC website: https://scsc.uk/ge.

This issue contains three papers:

- Sanjeev Appicharla (UK), in "*The Boeing 737 MAX 8 Crashes: System-based Approach to Safety — A Different Perspective*", contends that, despite all the literature on considering human and organisational factors in safety assessment, fewer researchers and practitioners than hoped actually do this as a matter of course. He concludes that we should be advancing models that include human, technical *and* organisational factors, *and their interactions*, when assessing the risks posed by complex systems.
- Derek Fowler (UK) and Nicolas Fota (France) build upon Derek's paper in the last issue, on using IEC 61508 in the Transport Sector, by providing a worked example, "*Safety Assessment of Point Merge Operations in Terminal Airspace — An IEC 61508 Viewpoint*". Point Merge is a systemised method for sequencing air traffic arrival flows that was developed by the EUROCONTROL Experimental Centre in Brétigny.
- Peter Bernard Ladkin, Lou Xinxin, and Dieter Schnäpp (Germany) present a method for the semantic analysis of electrotechnological definitions appearing in IEC standards: "*The Terminological Analysis Method SemAn and its Implementation*". The method is accompanied by a software tool, the SemAn Analyser, which provides outputs in a pretty-printed and annotated format that retains the symbol-for-symbol syntax of the original text of the *definiens*.

My thanks go to the authors for contributing their papers, and also to the peer-reviewers (at least three per paper) for suggesting improvements. Apologies to those reviewers who made some recommendations that were not taken up.

The editorial to the first issue of this journal said, "*You may find some of this material controversial, or you may think that it does not go far enough. Subsequent issues of this journal will have provision for readers' letters to the Editor responding to individual papers.*" Such a letter was published in the last issue, which itself prompted some correspondence. Apparently, it is accepted practice that letters for publication to journal editors should be between 300 and 800 words long, and someone even suggested that the maximum should be 400 words. The published letter was over 1600 words; twice as long as people seem to expect. Not wanting to be quite so constrained, I have now adopted a limit of (about) 1000 words (not counting title, attribution or references). That would take up two pages of this journal. Note that a letter should ideally address a single concern with few, if any, external references.

John Spriggs, SCSC Journal Editor

January 2023

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*".

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)).

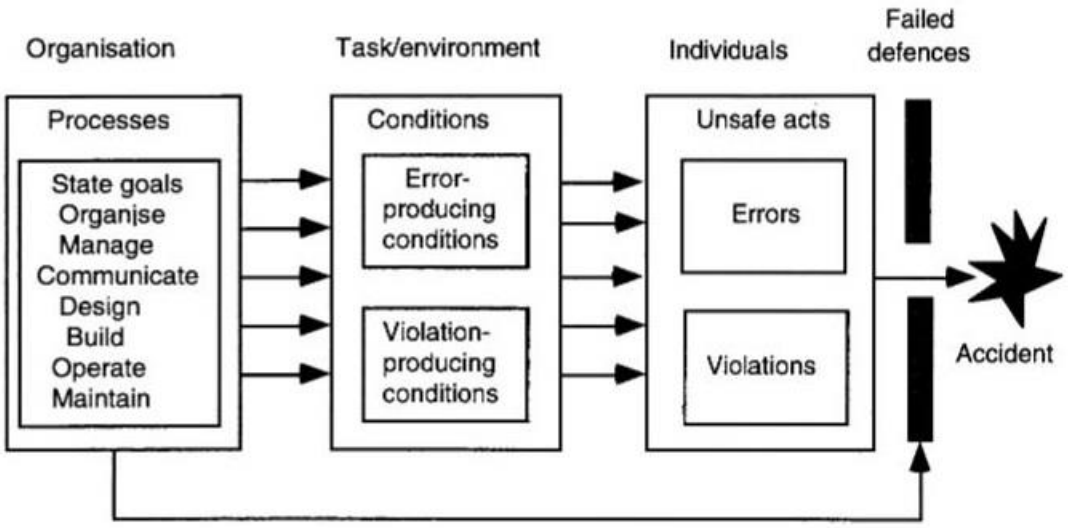

Figure 1 ~ Common Elements in the Development of Accident

[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.

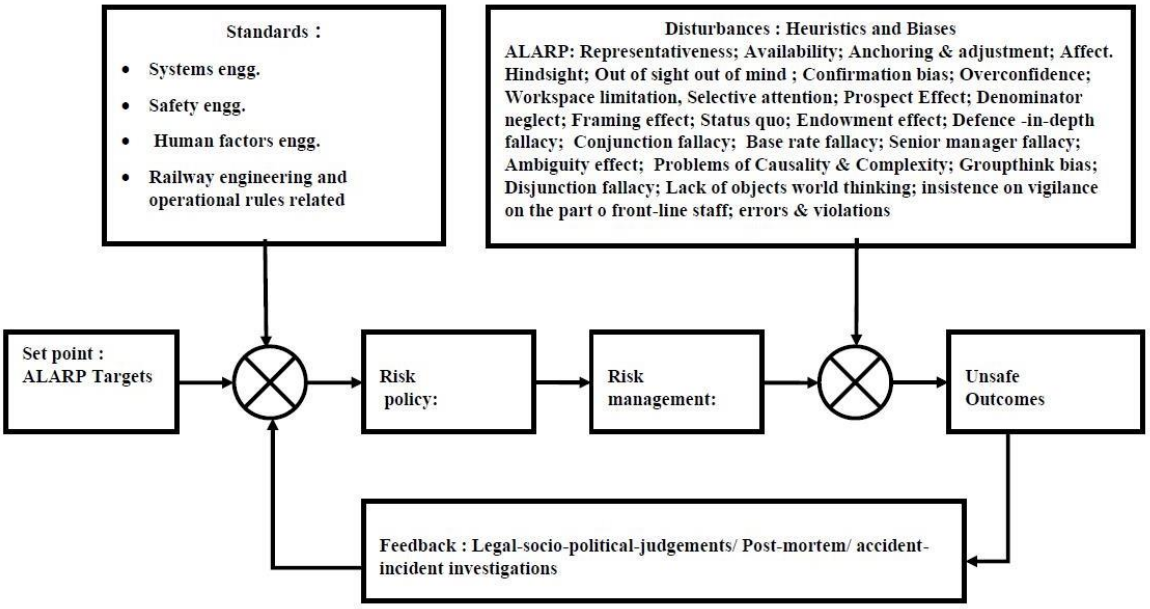

Figure 2~ Cybernetic Model of Risk Management

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.

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

Safety Assessment of Point Merge Operations in Terminal Airspace

An IEC 61508 Viewpoint

Derek Fowler[1] and Octavian Nicolas Fota[2]

1. Independent Safety Engineering Consultant, Reading, UK
2. EUROCONTROL Innovation Hub, Brétigny, France

Abstract

An article entitled "An IEC 61508 Viewpoint on System Safety in the Transport Sector", in Volume 1, Issue 2, of the Safety-Critical Systems Club eJournal, proposed a way of thinking about the safety assessment of transportation systems that is based on the fundamental principles of international functional-safety standard IEC 61508. Now, in this article, the example of Point Merge — a systemised method for sequencing arrival flows developed by the then EUROCONTROL Experimental Centre and first deployed in Oslo in 2011 — is used to outline how an IEC 61508 approach to safety assessment could be applied to the Air Traffic Management sector in general.

1 Introduction

IEC 61508 (IEC 2010) is probably the most widely-accepted, international generic standard on functional safety. Although its ancestry can be traced back to process industries, the intention behind the standard has always been to provide a solid, comprehensive basis for adaptation, as necessary, to meet the needs of a wide range of industry sectors.

Fowler (2022), proposed 'a way of thinking' about the assessment of the various safety-related systems deployed in the Transport sector — especially commercial-aviation and rail applications — based on the key principles and safety lifecycle set out in IEC 61508-1 and IEC 61508-4.

This article now takes an example application, from the Air Traffic Management (ATM) sector, of an operational concept for sequencing arrival flows in Terminal airspace, known as Point Merge, and uses it to outline how an IEC 61508 approach to safety assessment could be applied effectively to the ATM sector, and what the results thereof might look like, starting from the viewpoint of the traffic in the airspace being "virtual Equipment Under Control".

It is important to note that it is *not* the intention herein to prescribe IEC 61508-compliant processes for ATM applications — rather, it is to use the IEC 61508-1 lifecycle cycle model to shape thinking about system safety assessments away from a mindset that "*focussed too much on system reliability and not enough on system functionality, contrary to, inter alia, the most basic principles of the international functional-safety standard IEC*

61508" (Fowler 2022). *Nor* is it the intention to carry out a detailed compliance assessment of any existing ATM safety standards against IEC 61508 — the latter is left to readers with a sector-specific interest, and for whom the findings of Fowler (2015) might be relevant.

Like Fowler (2022), the scope of this article is limited to the following, initial phases of the IEC 61508 safety lifecycle, which result in the specification of detailed *functional safety requirements*[1] and *safety integrity requirements* necessary and sufficient for the subject safety-related systems to achieve a tolerable level of risk:

- Concept (Phase 1);
- Overall scope definition (Phase 2);
- Hazard and risk analysis (Phase 3);
- Overall safety requirements (Phase 4);
- Overall safety requirements allocation (Phase 5);
- Safety -related System (SRS) Safety Requirements Specification (Phase 9)[2];
- Other Risk-reduction Measures (ORRM) Safety Requirements Specification (Phase 10).

As we work herein through these lifecycle phases for Point Merge, it might appear that some of the steps could be simplified by, for example, subsuming them into other steps. Indeed, IEC 61508 allows for this to be done, where applicable, but, for the purposes of this paper, we decided to adhere exactly to the lifecycle detailed in Fowler (2022), except where indicated otherwise below.

2 Operational Context

Arrival procedures in Terminal airspace have historically involved open-loop vectoring of aircraft by Air Traffic Controllers. However, since the 1990s, Area Navigation (RNAV) procedures have gradually been introduced to systematise operations in most areas. A major drawback of both of these techniques, however, is that, under conditions of high traffic flows, their use tends to favour capacity at the cost of low flight efficiency and high environmental impact.

Therefore, the then EUROCONTROL Experimental Centre[3], Brétigny, France developed Point Merge operations (EUROCONTROL 2021) as a new method for integrating arrival flows, safely and efficiently, by combining the systematic use of lateral guidance by the aircraft's flight management system (FMS), with continuous descent approaches (CDAs), even at high traffic throughput.

Point Merge operations make use of Precision RNAV (P-RNAV)[4] procedures in terms of airspace design and functionality in the aircraft, but applied in a very specific way for arrival traffic in Approach airspace. The main difference between radar-vectoring (or

[1] The term *functional safety requirements* was coined in Fowler (2022) in preference to the (arguably ambiguous) IEC 61508 term of *safety functions requirements*; it covers safety requirements for both functionality (what has to be done) and performance (how well it has to been done).

[2] IEC 61508 phases 6 to 8 are concerned only with the planning of subsequent lifecycle phases and so are outside the scope of this paper

[3] Now called the EUROCONTROL Innovation Hub.

[4] Or equivalent

conventional P-RNAV) operations[5] and Point Merge operations is that in the former, arrivals are typically merged on to a line, whereas in the latter, they follow predefined routes until they are merged on to a point, known as a Merge Point.

Point Merge was first deployed in Oslo in 2011 and now operational at 37 or more airports across 4 continents, where it has been shown to provide significant potential benefits in terms of flight efficiency and the environment.

The question for the remainder of this paper is, however, would its introduction to a hypothetical airport be safe, and how would we demonstrate this, if we were to follow the IEC 61508 safety lifecycle?

3 Safety Assessment

3.1 Concept (IEC 61508-1 Phase 1)

3.1.1 Aim

The aim of this phase is to gather as much information about what IEC 61508 calls the *Equipment Under Control* (EUC), its *Environment*, and the *EUC Control System*, as necessary and sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.

It is important to note that, as an enabling activity, this would be a precursor to, but not form part of, the safety assessment *per se* and would require substantial operational and system-engineering specialist input, relevant to each specific application. In practice, such material may be found in a typical Concept of Operations document.

3.1.2 EUC

As with other ATM applications, we can understand the EUC as being, in general, the flow of aircraft through the airspace, during landing or taking off, and/or taxiing on the airport surface — in this case, it is the flow of arrival traffic through Approach airspace, until each aircraft intercepts the Instrument Landing System (ILS) Glidepath beam for its final descent to the runway. This understanding is consistent with the core IEC 61508 principle that the EUC is the main source of hazards, which Safety Related Systems (SRSs) are required to mitigate in order to achieve a tolerable level of risk.

The key inherent properties of the EUC that we will assume for this Point Merge example are as follows:

- traffic is a mix of commercial jets / turbo-props and general aviation;
- arrivals per year: 100,000;
- maximum sustained arrival rate: 28 per hour;
- average arrival flight time in Approach airspace: 12 minutes;

[5] For example in "tromboning", where P-RNAV routes define a complete path from the Initial Approach Fix (IAF) to the final approach fix (FAF), including an extended down-wind leg, base leg, and initial approach path, but aircraft are vectored off the downwind leg to merge on to the runway extended centreline.

- on average, at least 95% of aircraft in the main arrival flow are certified and approved for P-RNAV approaches;
- aircraft wake-turbulence category mix is dependent on time of day; during peak times it averages 1.5% super; 25% heavy; 65% medium; 8.5% light.

3.1.3 Environment

IEC 61508 defines the environment in terms that include its physical, operating, legal and maintenance properties.

The environment properties for Point Merge operations are assumed to be as follows, the list covering most of the key points necessary for the safety assessment:

- Airspace Parameters and Flight Rules:
  - applies to Approach airspace / Approach control phase, corresponding to Approach arrival sectors, typically between the IAF and the FAF or transfer to the Tower;
  - all traffic operates under Instrument Flight Rules.
- Transition Altitude is 18,000 ft, well above the highest part of the Point Merge structure.
- Adjacent Airspace / Operations:
  - adjacent surrounding airspace is En-route;
  - airport served by the Point Merge structure has two, parallel, main runways (26L and 26R), one for landing and one for take-off (interchangeable), with ILS Cat II.
- Climate and Terrain:
  - climate is temperate, liable to dense fog in winter and occasional heavy thunderstorm activity in summer; prevailing winds are westerly;
  - terrain is generally undulating but with high mountains starting at 35 nautical miles South-west of the runway.
- Environmental Constraints: for the purposes of this paper, we will assume that no particular environmental constraints apply to Point Merge operations.

3.1.4 EUC Control System

Given the above interpretation of the EUC itself, we can understand the EUC Control System as being a functional system, encompassing people, procedures and equipment, and comprising, in general:

- The usual Air Traffic Services (ATS) and facilities to be found at a typical busy airport, irrespective of the specific type of Approach operations in place; and
- The Flight Crew actions related to flying the P-RNAV routes and following the ATS procedures and instructions, together with airborne equipment supporting the execution of those actions.

It is important to emphasise that, in the description of the EUC Control System which follows, the focus is on the business / operational *rationale* for Point Merge, and the text

deliberately makes little or no explicit reference to the safety constraints that, of course, must be applied to Point Merge operations — these will be addressed in Phase 3 *et seq*.[6]

The Point Merge configuration applicable to this safety assessment is a single structure, as shown in Figure 1.

The Point Merge structure comprises two continuous P-RNAV routes, linking two IAFs (IAF1 and 2) to the FAF[7] and the start of final descent into a single arrival runway (RWY 26L), with waypoints signified by the star symbols. It includes the following key stages:

- Two Sequencing Legs, which are centred on the Merge Points; the inner Leg (i.e. the one closer to the Merge Point) is, wherever practicable, higher than the outer Leg;
- Two Run-off Legs, each one of which connects the end of a Sequencing Leg to the Merge Point;
- The FAF, by which time the aircraft will have acquired the ILS Glidepath for final approach and landing.

A holding point is provided prior to each Point Merge entry point, for use as required.

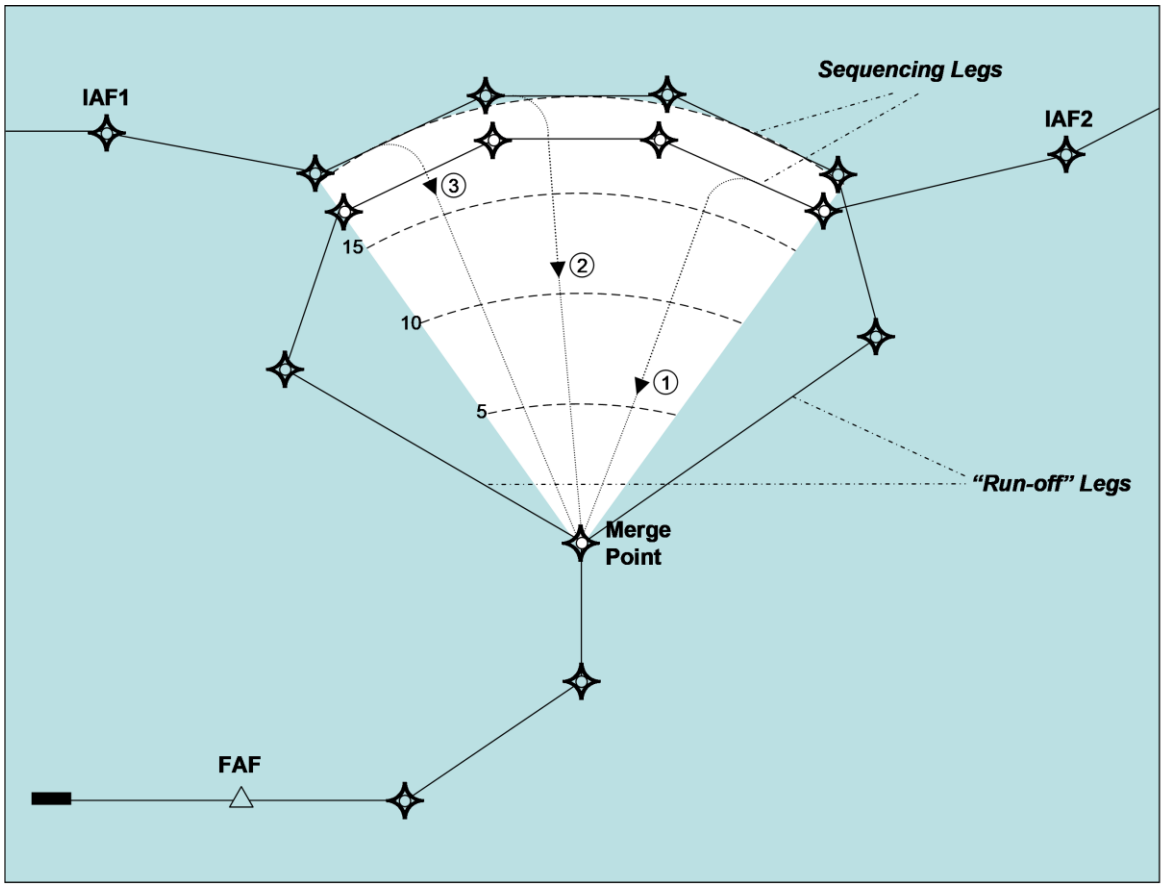

Figure 1 ~ Point Merge Route Layout

The boundary between Approach airspace and adjacent En-route / Terminal airspace sectors occurs before the IAF in each case.

[6] It is acknowledged that this distinction might seem somewhat artificial; however, it serves to emphasise the point made, at Sub-section 3.1.1 herein, that this phase is a necessary precursor to, rather than a part of, the safety assessment *per se*.

[7] A dual configuration is also possible, based on an additional, mirror-image structure to the south of the runway centreline, with the two Merge Points linked to a Common Point, which itself has a single route linking it to the FAF.

What we have identified as the "EUC Control System", is required, under *normal* operating conditions[8], to establish and maintain the arrival sequence, within this structure, i.e. to order the arrivals, and *space* them in accordance with the runway metering requirements, so as to maximize runway throughput while taking account of the safety and other needs of individual flights[9]. This is achieved as follows:

- non-arrival traffic in the area is handled as follows:
  - departing traffic (usually from RWY26R) follows standard instrument departure (SID) routes, above the Point Merge structure, to the top of climb;
  - overflying traffic follows conventional Airways route structure;
  - low-level transits of traffic operating under Instrument Flight Rules, and Arrivals to proximate aerodromes, are radar-vectored though Approach airspace, whilst avoiding the Point Merge structure;
- the required aircraft-arrival rate is derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as "metering" requirements based on runway capacity and the limited ability of Approach airspace to absorb momentary traffic overloads;
- sequencing and spacing of traffic are established initially in En-route/ Terminal airspace according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the maximum runway throughput commensurate with the need to maintain adequate spacing between aircraft in the same flow;
- arriving traffic is cleared initially, by ATC[10], to follow standard P-RNAV Terminal airspace arrival routes (STARs) from the top of descent to the IAF;
- prior to reaching its IAF, ATC clears each P-RNAV-capable arrival to continue to follow the remainder of the appropriate P-RNAV route, i.e. down to the FAF but subject to contrary instructions from ATC as necessary;
- aircraft that are not P-RNAV capable (i.e. not equipped or suffering from P-RNAV equipment failure) are vectored along the appropriate Point Merge route, to emulate P-RNAV-capable aircraft, as per the rest of the sequence;
- ATC issues a Direct-to instruction (or a vector, in the case of a non-P-RNAV aircraft) to each aircraft to leave its Sequencing Leg, and head to the Merge Point, once sufficient spacing has been established behind the aircraft immediately preceding it in the overall landing sequence — note that the preceding aircraft might not be on the same Sequencing Leg;
- if the spacing requirements cannot be met before the aircraft reaches the end of the Sequencing Leg[11], the aircraft will, by default, continue on its P-RNAV route (and / or vectors) to the Merge Point — i.e. following the associated Run-off Leg;
- once ATC clears the aircraft to start its descent towards the Merge Point (having ensured safe separation from traffic on the parallel sequencing leg), it will converge vertically (and laterally) with the other aircraft in the flow;
- finally, from the Merge Point to the FAF, there is now only one horizontally-merged flow in which all the aircraft are spaced longitudinally. Along this segment, each

[8] i.e. what we want, and expect, to happen in day-to-day operations (Fowler 2022).

[9] The use of the term "space" here includes *implicitly* the need to also apply the required longitudinal separation minima, wherever other separation *modes* are not available. The way in which the various separation modes are applied throughout the Approach airspace is addressed explicitly in Phase 3 *et seq*.

[10] ATC = Air Traffic Control

[11] Or, for example, and aircraft is unable to respond to a Direct-to instruction

aircraft is cleared to continue its descent until it eventually acquires the final-approach path to the runway.

3.2 Overall Scope Definition (IEC 61508-1 Phase 2)

3.2.1 Aim and Objectives

The aim of this phase is to define the scope of the Hazard and Risk Analysis, for Phase 3.

It seeks to achieve that aim through determining the boundary of the EUC / EUC Control System and its Operational Environment and, within those constraints, specifying the scope of the Hazard and Risk Analysis.

This would be particularly important when assessing the safety of a change to an existing operation and/or system so as to identify, and exclude, the unnecessary safety assessment of those elements that are not affected by the change. It should be noted, however, that we can do this only in general terms herein because of the necessarily generic nature of the operational context for which this example safety assessment is being carried out.

3.2.2 Boundary Constraints

For the purposes of the safety assessment of Point Merge operations, the flow of arrival traffic, which constitutes the EUC, is that which lies between the IAF and the FAF, though it might be necessary to consider the conditions for handover from the adjacent En-route airspace and to final approach and landing. The functioning of the EUC Control System and the properties of the Operational Environment are similarly limited spatially.

3.2.3 Scope of the Hazard and Risk Analysis

Within the above constraints, it is *not* intended to address:

- any hazardous event or situation that does not involve at least one arriving aircraft; nor
- hazards associated with failure onboard an aircraft that leads to a loss of control, other than the effects that such events might have on other aircraft in the vicinity.

3.3 Hazard and Risk Analysis (IEC 61508-1 Phase 3)

3.3.1 Aim

The aim of this phase is to determine, and characterise, all the hazards and risks associated with the EUC[12], in the stated Environment, and within the scope already identified in Phase 2.

Note: it is acknowledged that these EUC hazards (and some of the detail that follows, up to and including Sub-section 3.4.3 below), which are not specific to Point Merge operations, might have already been identified and documented adequately in, say, a safety

[12] Strictly speaking, IEC 61508 includes "EUC Control System Hazards" here as well. We have taken the view that, for ATM, failures with the EUC Control System are among the *causes* of EUC hazards.

case for the airspace concerned. For the purposes of this paper, however, we do not assume this to be the case.

3.3.2 EUC Hazard Identification

The objective here is to determine the hazards relating to the EUC, within the scope defined in Sub-section 3.2 above.

From the IEC 61508 definition of a hazard, which can be paraphrased as "*a potential **source** of death, physical injury or damage to the health of people or damage to property or the environment*" (Fowler 2022), it follows that we must first identify the types of harmful **outcome,** i.e. accident, that fall within ATM's general sphere of responsibility and specifically within the above scope of Point Merge operations.

Table 1 shows accident types relevant to ATM, in Approach airspace, and has been adapted from ICAO (2011)[13] and, in each case, involves death or serious injury to one or more of those on board.

Table 1 ~ Accident Types Relevant to ATM in Approach Airspace

Accident Type	Description
Mid-air collision (MAC)	All collisions between aircraft (or between an aircraft and an unmanned aerial vehicle or missile), while both are airborne
Controlled Flight into Terrain (CFIT)	Inflight collision with terrain, water, or obstacle without loss of control
Uncontrolled Flight into Terrain (UFIT)	Inflight collision with terrain, water, or obstacle following loss of control, *except* where such loss is caused by failure(s) internal to the aircraft
Abrupt, Violent Manoeuvre (AVM)	Sudden, large, intentional or unintentional departure from the intended flightpath and/or attitude, *except* where such departure is caused by failure(s) internal to the aircraft

The EUC hazards derived from the above, and in relation to what are seen to be credible accident outcomes, are shown in Table **2**. The hazards are (by definition) those that are inherent in aviation, in the stated Operational Environment. It is crucial to note that these hazards apply directly to the EUC (the flow of arrivals through Approach airspace) and exist *before* any form of EUC-hazard mitigation has been applied (Fowler 2022).

The numbers in parentheses in Table **2** refer to the notes that follow the table.

Table 2 ~ EUC Hazards and Precursor States

ID	EUC Hazard Title (1)	Immediate Precursor State (2)	Related Accident(s)
Hp#1	Conflicts between pairs of aircraft 4-D flight trajectories	The trajectories concerned intersect, at the approximately same altitude, and the two aircraft would arrive at the crossing point at approximately the same time	MAC or AVM (3)

[13] ICAO (2011) Categories are intended for use in *a posteriori* categorisation of actual occurrences, rather than *a priori* safety assessment — hence the need for some adaptation

ID	EUC Hazard Title (1)	Immediate Precursor State (2)	Related Accident(s)
Hp#2	Aircraft in conflict with terrain or obstacle	Aircraft, under the control of the flight crew (or autopilot), is on a downward trajectory that would bring it in contact with the ground or fixed obstacle, *other* than at a suitable runway touchdown point at an appropriate speed and in an appropriate configuration	CFIT or AVM (3)
Hp#3	Aircraft in conflict with unauthorized areas	Aircraft is on a trajectory that would pass through active restricted airspace without authority	MAC (4)
Hp#4	Aircraft in conflict with severe weather conditions	Aircraft is on a trajectory that would pass through an area of weather conditions that are severe enough for its ability to continue its flight safely to be significantly impaired	AVM or UFIT (5)
Hp#5	Aircraft in conflict with wake turbulence	Aircraft is on a trajectory that would put it in an area of wake turbulence that is severe enough for its ability to continue its flight safely to be significantly impaired	AVM or UFIT (5)

Notes:

1. "Conflict" is used here in its broadest sense – see column 3.
2. IEC 61508 requires that the sequence of events be described for each EUC hazard, but it would be impracticable for ATM, at this stage in the process, because of the number of causal factors involved. What we can usefully do *here* is to describe the immediate precursor to each hazardous event, and leave it to the modelling approach described in Sub-section 3.4.2 below, which does capture how such states are arrived at in the first place, and thus satisfy this IEC 61508 requirement.
3. AVM here is the result of *onboard* actions to avoid an imminent collision
4. Incudes collision with another airborne vehicle and from being hit by some form of munitions.
5. AVM would be the more likely outcome except when the aircraft is closer to the ground and timely recovery from the departure is more difficult.

What we have not said thus far is anything about the probability that each EUC hazardous event would lead to the related accident except, that the probability would, by definition, be finite. That is addressed next, in Sub-section 3.3.3.

3.3.3 EUC Risks

Severity of a hazard could, in general be deduced from the probability that the hazard would lead to the associated accident(s)[14], and the seriousness of the accident in term of the number of fatalities and/or degree and extent of serious injury involved; in ATM, however, the latter has traditionally *not* been considered in *a priori* safety assessments.

In theory, we could then determine either:

[14] Otherwise known as the probabilistic "distance" to the accident

- the EUC risks: i.e. by *estimating* the frequency of occurrence of each EUC hazard and combining it with an assessment of the hazard's severity; or
- the tolerable frequency of occurrence for each hazard: i.e. by setting a *target* tolerable level of EUC risk for each hazard and dividing it by the assessed hazard severity.

Fowler (2022) discussed the potential problems of identifying EUC risk, and Sub-section 3.4 below explains why its determination is actually not necessary under IEC 61508, though it is clear that a method of determining hazard severity is needed in *either* case. Unfortunately, in ATM, predicting the outcome of any hazard is not that simple because:

- as shown in Table 2, each EUC hazard has more than one potential, credible accident outcome;
- any given probability of such an outcome would vary according to, *inter alia*, phase of flight, traffic patterns and density;
- the probability and harmful effects would vary between accident types, e.g. between MAC and AVM, notwithstanding the fact that, traditionally, most ATM harmful events are treated as being of the same severity, irrespective of the number of people affected.

Concerns about hazard-severity / risk-classification schemes, in general, are not new; indeed, as long ago as 2006, the then EUROCONTROL Safety Case Development Manual (EUROCONTROL 2018), expressed concerns about the potential misuse of such schemes unless the user understands:

- at what level in the system hierarchy the values are intended to be applied;
- where the probability/frequency values used in the scheme came from and whether they are (still) valid;
- to what operational environment the values apply, eg type of airspace, traffic patterns, traffic density, spatial dimension, phase of flight, etc;
- how the aggregate risk, as specified in ESARR 4[15] for example, can be deduced from analysis of individual hazards, in restricted segments of the total system.

With all of the above issues in mind, Sub-section 3.4 below introduces a more rigorous approach to hazard and risk assessment, which has been developed by the EUROCONTROL Innovation Hub (EIH) for the Single European Sky ATM Research (SESAR) programme (SESAR 2021). It is based on a set of Accident Incident Models (AIMs), one per accident type, from each of which an RCS can be derived. More information on AIMs is provided in SESAR (2018a) and SESAR (2018b) but, essentially, they model the contributions that the ATM functional system makes to aviation safety, both when working as specified, and in the event of failure. The RCSs derived from the AIMs have four key advantages over the more traditional schemes referred to above:

- they are based on real, historical accident and incident data;
- they more accurately capture the progression of a hazardous event through to an accident;
- they provide safety criteria at many levels in the ATM functional-system hierarchy and for specific phases of flight;
- they provide safety criteria that take account of future changes to the ATM functional system and/or operational environment.

[15] ESARR 4 was the EUROCONTROL Safety Regulatory Requirement "Risk Assessment and Mitigation in ATM", which has since been overtaken by Single European Sky legislation.

3.4 Overall Safety Requirements (IEC 61508-1 Phase 4)

3.4.1 Aim

The aim of this phase is to produce a specification of the Overall Safety Requirements for each Overall Safety Function in order to achieve the required level of functional safety. These requirements cover both functional-safety and safety-integrity properties.

3.4.2 Introduction

According to IEC 61508, an Overall Safety Function is the highest-level abstraction of the "*Means of achieving, or maintaining, a safe state for the EUC, in respect of a* specific *hazardous event*", and therein lies a problem — the relationships between accidents and hazards (as explained above) is "many-to many" and so is the relationship between EUC hazards and the safety functions that are intended to mitigate them.

This can be illustrated by expressing the three layers of ATM, described in the ICAO Global ATM Concept (ICAO 2005), in the form of a generic Barrier Model[16], as shown in Figure 2 (Fowler et al 2009).

The inputs to the model are the relevant EUC hazards and the barriers, acting in rough sequence from left to right, effectively "filter out" a proportion of the EUC hazards. The final barrier reflects the point that, even when all three layers of ATM have been unable to remove a hazard, there is still a relatively high probability that an actual accident will not result, as indicated by the Providence barrier. This probability depends on a number of factors, including the type of the resulting accident, the volume of the available airspace, the density of traffic therein, and the geometry of the encounter.

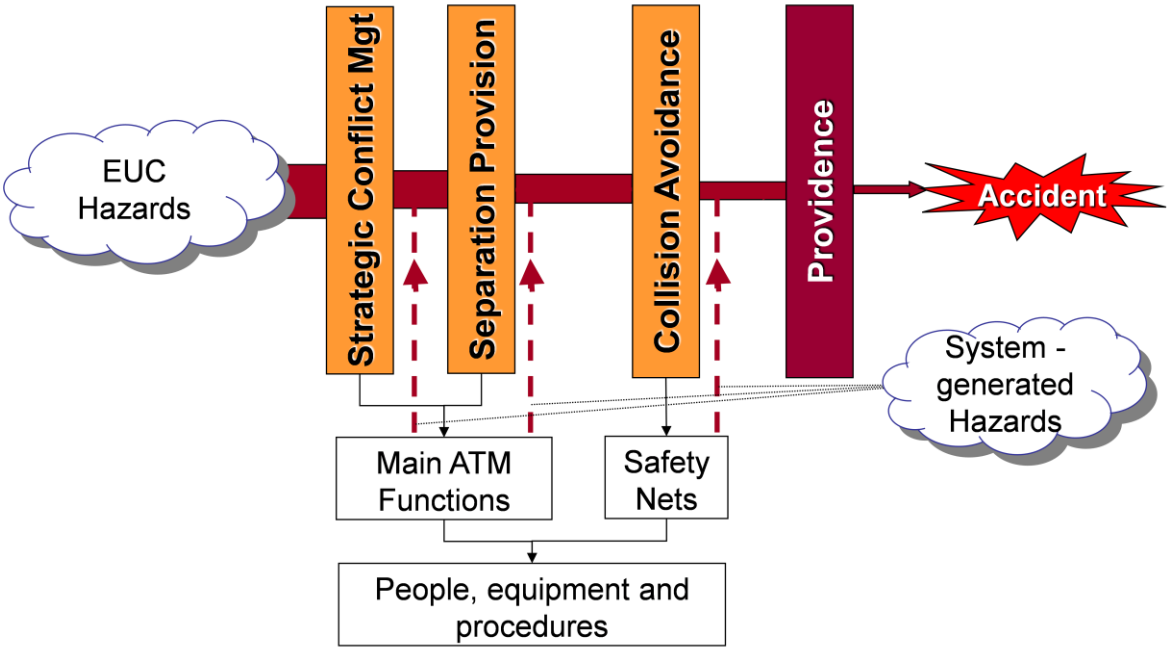

Figure 2 ~ ATM Barrier Model

[16] Derived from James Reason's "Swiss Cheese" model (Reason 2000)

The main three barriers are provided by the primary ATM safety functions and ground-based / airborne safety nets, implemented in the elements of the end-to-end ATM system. Of course, these elements can fail to operate, effectively reducing the probability of success of the barrier, or operate incorrectly, giving rise to new, *system-generated* hazards.

Fowler (2022) presented a simple fault tree model of a generic safety function and showed how its safety properties govern its ability to prevent, i.e. to act as single a barrier to, the progression of an EUC hazard through to an accident. That idea, based on a low-demand situation, is extended, in Figure 3 to represent the multi- barrier model of Figure 2.

Apart from its slightly unconventional layout, this model has one very important feature that distinguishes it from most other Fault Trees — i.e. it has an external input (EUC hazards)[17], which enables the computation of the risk of an accident (R_A) from:

- the EUC hazards (those hazards inherent in aviation) and their frequencies (F_U);
- the net probability of success ($P_S n$) of each barrier in mitigating those risks, taking account of its functionality and performance, and of the probability that it might occasionally fail to operate at all; and
- the frequency ($F_F n$) with which corrupt-operation failure of each of the main barrier introduces new, system-generated hazards / risks.

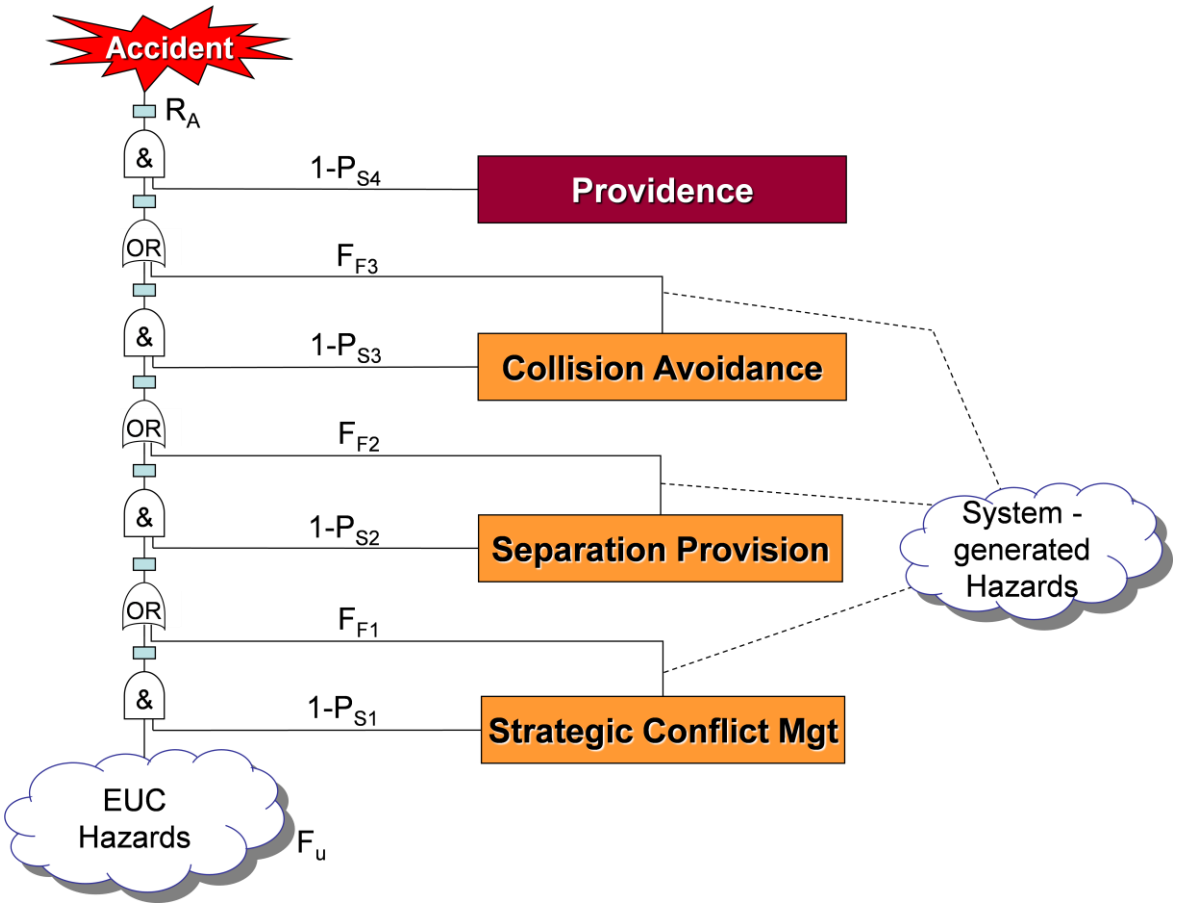

Figure 3 ~ Fault Tree Version of the ATM Barrier Model

[17] Without this input, a Fault Tree could model only *failures internal* to the system on which the Fault Tree is based – i.e. it could model only *negative* effects on safety

Alternatively, of course, if we make the top-level risk our target (R_T) then, given F_P and access to historical accident and incident data, we can make informed judgements about what $P_S n$ and frequency $F_F n$ are required to be in order to satisfy R_T.

Thus the model captures the net positive, as well as the negative, contributions of ATM to aviation safety, and it is this form of risk model on which the SESAR Accident Incident (AIM) models (SESAR 2018a) are based.

Of course, the model, as presented here, is purely illustrative and very high-level. In reality, each AIM model is very much more comprehensive, and actually represents the Barrier model as an Event Tree which integrates the Fault Trees dedicated to each Barrier.

In seeking to overcome many of the shortcomings of traditional hazard-severity / risk-classification schemes, discussed in Sub-section 3.3.3 above, the SESAR approach:

- has, at a detailed level, separate models for each phase of flight and accident type;
- uses real accident and incident data to populate the model with the required probability and frequency values; and
- is capable of modelling the interdependencies between barriers, including lower-level common-cause and common-mode failures, that are implied in Figure 2.

The remainder of this sub-section follows the above principles embedded in the AIM.

3.4.3 Overall Safety Function Identification

The objective here is to identify a set of Overall Safety Functions, based on the EUC hazardous events derived from the hazard and risk analysis of Phase 3. Notwithstanding the minor problem that the IEC 61508 view, of a one-to-one relationship between EUC hazards and Overall Safety Functions, does not work for ATM, the three ATM barriers (or "layers" (ICAO 2005)) fit the role of Overall Safety Functions quite nicely, and are shown in Table **3**.

Table 3 ~ Overall Safety Functions

ID	Overall Safety Function Title	Related EUC Hazards
OSF#1	Strategic Conflict Management (SCM)	Hp#1, Hp#2, Hp#3, Hp#4, Hp#5
OSF#2	Separation Provision (SP)	Hp#1, Hp#2, Hp#3, Hp#4, Hp#5
OSF#3	Collision Avoidance (CA)	Hp#1, Hp#2

3.4.4 Overall Safety Function Required Functional Properties

This step involves the determination of the required functional properties of each of the above Overall Safety Functions. The resulting Overall Safety Requirements (OSRs) are based on the *reference* operational scenario described in Sub-section 3.1.4 above and cover those items that are necessary and sufficient to ensure the safety of Point Merge operations.

In order to avoid, and / or mitigate the consequences of, the hazards shown in Table 1, the functional properties shown in Table 4 are required of the respective Overall Safety Functions. It should be noted that these requirements are objective based — i.e. they express what the OSF have to achieve rather than what they have to do.

Table 4 ~ Overall Functional Safety Requirements for Normal Operations

Reqt. ID	Requirement Description	Related EUC Hazard
OSF#1	**Strategic Conflict Management**	
OSR1.1	Arrival rates into Point Merge airspace shall not exceed the capacity of the P-RNAV routes or runway	Hp#1, Hp#5
OSR1.2	Crossing traffic and departures shall be segregated strategically from the Point Merge structure	Hp#1
OSR1.3	The Point Merge structure shall be segregated strategically from all restricted airspace	Hp#3
OSF#2	**Separation Provision**	
OSR2.1	All aircraft in Approach airspace shall be separated from each other, by either: the greater of the radar-separation minima and the wake-turbulence minima, horizontally; or by 1000ft vertically	Hp#1, Hp#5
OSR2.2	At all points along each route, from IAF to FAF, aircraft shall remain above the altitude of all close terrain/obstacles and/or be adequately separated laterally from such terrain/obstacles	Hp#2
OSR2.3	Point Merge operations shall cease in the event of severe weather posing a threat to the safety of arriving traffic flow in the Point Merge structure	Hp#4
OSF#3	**Collision Avoidance**	
OSR3.1	When the associated *separation mode* has been compromised, *mid-air* collision-avoidance action shall be taken in accordance with current operational procedures	Hp#1
OSR3.2	When the associated *separation mode* has been compromised, *terrain/obstacle* collision-avoidance action shall be taken in accordance with current operational procedures	Hp#2

3.4.5 Determine the Safety Integrity Requirements for each Overall Safety Function

This step involves the determination of the SIRs required of each of the above Overall Safety Functions, to achieve a tolerable level of risk overall. Two points are stressed in Fowler (2022):

- IEC 61508 states that the SIRs, at this level, must be specified in terms of either:
  - the risk reduction required to achieve the tolerable level of risk; or
  - the tolerable [EUC] hazardous event rate to achieve the tolerable level of risk; and
- according to IEC 61508, SIRs at this "overall" level are *not*, despite their name, properties of the OSF to which they relate — they actually specify a *target* amount of EUC risk reduction that the OSF has to meet, and could be seen to correspond to the more appropriately termed *safety criteria* in ATM.

Here, the SESAR AIM approach has two big advantages over IEC 61508 Phase 4, as follows:

- it derives SIRs that *are* properties of the OSFs themselves; and
- those properties accord directly, and fully, with the concept of Safety Integrity as defined in IEC 61508 — viz:

> *"the probability of a … safety-related system satisfactorily performing the specified safety functions under all the stated conditions, within a stated period of time"*

There is not the space in the context of this paper to provide a worked example for Point Merge but, in principle, we can see from Figure 3 above how, given sufficient relevant real-world accident data, a realistic value of EUC hazard rate and a risk tolerability level for, say, a MAC accident, the following three SIRs could be derived for each ATM barrier:

- probability of successful mitigation of the input hazard, in the absence of failure internal to the barrier;
- frequency or probability of failure internal to the barrier[18]; and
- frequency of corrupt operation of the barrier.

3.5 Overall Safety Requirements Allocation (IEC 61508-1 Phase 5)

3.5.1 Aim

The aim of this phase is to allocate to SRS(s) and/or ORRM(s), the functional safety requirements and safety integrity requirements, which were derived for the corresponding overall safety function in Phase 4.

3.5.2 Discussion

IEC 61508 gives prominence to the distinction between SRSs and ORRMs — partly, it would seem because, once identified, the latter measures fall outside the scope of the Standard.

For ATM in general, ORRMs could include non-functional, safety-related items such as airspace /route structure and runway / taxiway layout, for which specific design & development standards exist in most cases. However, given the close interaction between ATC and, say, P-RNAV route structures in the SP barrier for Point Merge, it was decided that there was little additional value in the distinction, in this case[19]. Therefore, Table 5 shows the allocation of the OSFs from Table 4 on to what might be interpreted generically as SRSs[20], within an ATM "system of systems".

Table 5 ~ Allocation of Overall Safety Functions for Point Merge

OSF/OSR ID	**Safety-related System**
OSF#1	**Strategic Conflict Management**
OSR1.1	Demand & Capacity Balancing (DCB)

[18] Depending on whether the barrier operates continuously, i.e. at a high demand rate, or at a low demand rate, respectively.

[19] We considered whether ORS1.2 should be allocated to ORRMs since the segregation of transits / overflights and departures depends on risk-reduction measures which fall mainly outside of the scope of Point Merge. Whereas this would have merit as a way of managing such measures, it would have added non-essential complexity to this paper, which we chose to avoid.

[20] These are based on what ICAO (2005) terms "*ATM operational concept components*".

OSF/OSR ID	Safety-related System
OSR1.1	Departure Synchronisation (DS)
OSR1.1	Arrival Sequencing & Spacing (ASS)
OSR1.1	Airspace Organisation & Management (AOM)
OSR1.2	
OSR1.3	
OSF#2	**Separation Provision**
OSR2.1	ATC Pre-tactical Conflict Management ~ air-to-air (ATC-PTCM-AA)
OSR2.2	ATC Pre-tactical Conflict Management ~ air-to-ground (ATC-PTCM-AG)
OSR2.1 OSR2.3	ATC Tactical Conflict Management ~ air-to-air (ATC-TCM-AA)
OSR2.2	ATC Tactical Conflict Management ~ air-to-ground (ATC-TCM-AG)
OSR2.2	Airborne Tactical Conflict Management ~ air-ground (AB-TCM-AG)
OSF#3	**Collision Avoidance**
OSR3.1	ATC mid-air collision-avoidance (ATC-MACA)
OSR3.2	Airborne mid-air collision-avoidance (AB-MACA)
OSR3.2	ATC terrain collision-avoidance (ATC-TCA)
OSR3.3	Airborne terrain collision-avoidance (AB-TCA)

The ICAO Global ATM Concept (ICAO 2005) uses the term "strategic" to mean "in advance of tactical" whilst recognising that "a continuum exists from the earliest planning of the user activity through to the latest avoidance of the hazard". In respect of the use of P-RNAV routes, with various altitude constraints, to effect separation, it is debatable whether that is strategic or tactical, or lies on the continuum somewhere between the two; we concluded that the latter was the case and coined the term "pre-tactical", within Separation Provision, to capture this in Table **5**.

Furthermore, where pre-tactical separation is provided, by the P-RNAV route structures of Point Merge, we envisage that ATC monitoring of aircraft compliance with the P-RNAV route parameters would be provided within the two (ATC-TCM) barriers, in advance of Collision Avoidance.

3.6 Safety Requirements Specification (IEC 61508-1 Phases 9 and 10)

3.6.1 Aim

In IEC 61508, the respective aims of Phases 9 and 10 is to develop safety requirements for the "SRSs" and "ORRMs" identified in Phase 5, in terms of their Functional Safety Requirements (FSRs) and the SIRs, in order to achieve the required functional safety under all *normal*, *abnormal* and *failure* conditions.

Given that, in the case of Point Merge above, we have viewed the distinction between SRSs and ORRMs as being of limited value, we have thus combined Phases 9 and 10 together in this sub-section.

3.6.2 Overview

It is important to note here that IEC 61508-1 places great emphasis on the need for a description of the workings of the SRS at this level, including:

- a description of all the safety functions, how they work together to achieve the required functional safety and whether they operate in low-demand, high-demand or continuous modes of operation;
- the required performance attributes of each safety function — e.g. timing properties and, for more data-intensive applications than possibly envisaged by IEC 61508, data accuracy, latency, refresh rate, and overload tolerance;
- all interfaces that are necessary to achieve the required functional safety;
- all relevant modes of operation of the EUC;
- response of the SRSs to abnormal conditions that might arise in the EUC or its environment;
- all required modes of behaviour of the SRSs — in particular, its failure behaviour and the required response in the event of such failure (Fowler 2022).

In the particular case of Point Merge operations, there are no new SRSs /safety functions; rather, the operational concept is based on existing Approach airspace functions / infrastructure, most of which are elements of the ATM system, i.e. what IEC 61508 terms the "EUC Control System" (see Sub-section 3.1.4 above), and which must be considered to be SRSs in their own right by virtue of their safety significance in Point Merge operations.

The questions that we need to address at this stage, therefore, are *where and when* those safety functions are deployed for Point Merge and would that be safe. To that end, this sub-section comprises four stages, as follows.

Firstly, the development of FSRs using operational scenarios, covering *normal* operations. This will be done initially at two levels (see Sub-section 3.6.3 below):

1. initially, at a relatively abstract level, without reference to explicit elements within the end-to-end ATM system, and
2. then, the lower level of a "*logical*-architecture" representation of the ATM system (i.e. the "EUC Control System")[21].

The former level is focused on *what* needs to be done and uses narrative scenarios to represent a (basic) form of behavioural model of Point Merge, which captures the initial FSRs, for the operational processes involved in a typical flight through the airspace. The latter, however, focusses on *how* this is achieved by the logical elements of the ATM system[22].

[21] Whereas IEC 61508 does not distinguish between these two levels, the approach described here has been found by the authors to be a useful approach to the safety assessment of a number of ATM applications

[22] As noted in Sub-section 3.7.2 of Fowler (2022), the IEC 61508 objective here is to "*describe, in terms not specific to the equipment, the required safety properties of the SRS(s)*". Both of these levels of requirements expression respect that objective since neither makes any assumptions about the technology involved in the realisation of the requirements.

Secondly, to show that the FSRs specified for the SRSs would be adequate to meet the risk-reduction required of the barriers / SRSs, in the absence of failure (see Sub-section 3.6.4).

Thirdly, to analyse, in a similar manner, scenarios covering *abnormal* events in order to identify any additional FSRs necessary to maintain a tolerable level of safety during such events (see Sub-section 3.6.5 below).

Fourthly, to analyse scenarios relating to potential failures of the ATM system in order to identify SIRs, and any additional FSRs, necessary to maintain a tolerable level of safety during such failure events (see Sub-section 3.6.6 below).

3.6.3 FSRs for Normal Operations

3.6.3.1 Derivation of FSRs for the "Reference" Operational Scenario

In order to derive the initial set of FSRs, the analysis first considers a typical flight through Approach airspace, as a continuum, looking in particular at transitions in the *separation mode* and in the merging of traffic, for the Point Merge structure shown in Figure 1.

For the purpose of analysis, the *subject* aircraft is assumed to be P-RNAV capable and enters the Point Merge structure, in a westerly direction, at IAF1[23]. It is termed the *reference* scenario (designated N0) since it is based on the most likely set of operational and environmental conditions[24].

For each stage in the flight at which something has to be achieved in relation to one or more of the OSRs shown in Table **4** above, the need for an FSR is identified, as shown thus "{FSR#n}" in the text below, and then the corresponding FSRs are detailed (and traced back to the related SRS(s), at Table 10 in Appendix A.

General Conditions: the following conditions apply generally throughout flight in Approach airspace:

- vertical separation at intersections of Point Merge routes with SIDs is provided achieved through aircraft conforming to appropriate published altitude restrictions {FSR#1};
- all other traffic is kept away from the Point Merge structure strategically, or by ATC tactical intervention as and when appropriate {FSR#2};
- the whole Point Merge structure is segregated spatially from Restricted Airspace {FSR#3};
- entire P-RNAV routes (i.e. from IAF to FAF) are designed in accordance with ICAO Doc 8168 Vol II (ICAO 2014) {FSR#4}.

Pre-conditions: the following conditions apply prior to aircraft entering the Point Merge structure at the designated IAF:

- required aircraft-arrival rate is derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as "metering" requirements based on runway capacity (arrivals and departures) and the limited ability of Approach airspace to absorb momentary traffic overloads {FSR#5 and FSR#6};

[23] The choice here is entirely arbitrary, and the analysis would apply equally to any P-RNAV-capable aircraft entering at the other IAF.

[24] Other scenarios will cover other *normal* conditions, e.g. the cases of aircraft that are not P-RNAV capable, as well as, later in this sub-section, *abnormal* and *failure* conditions.

- sequencing and spacing of traffic are established initially in En-route/ Terminal sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow {FSR#7, FSR#8};
- ATC monitoring of aircraft conformance with all clearances and instructions is carried out throughout each flight, including when aircraft are following the predefined P-RNAV routes that make up most of the Point Merge structure {FSR#9}.

***Flight in Approach Airspace*:** the aircraft proceeds as follows:

- entry into Approach airspace is coordinated with the adjacent upstream sector(s) according to the agreed entry conditions, including the aircraft being stable at the defined altitude prior to Sequencing Leg entry {FSR#10} — this is to reduce the chances of unnecessary ACAS / STCA alerts with opposite-direction aircraft that are approaching the end of the adjacent Sequencing Leg;
- on entry to, and along, the Sequencing Leg (SL1), the aircraft remains in level flight and is vertically separated from each eastbound aircraft on the adjacent, opposite-direction Sequencing Leg (SL2) by all aircraft complying with height restrictions published for the P-RNAV route applicable to its Sequencing Leg {FSR#11};
- spacing from preceding and succeeding aircraft on the same Sequencing Leg is provided tactically by ATC such that the 3 nautical mile longitudinal-separation minimum and wake-vortex criteria are maintained {FSR#12};
- vertical clearance from terrain/obstacles is provided by the minimum altitude specified for each Sequencing Leg's P-RNAV route section {FSR#13};
- once sufficient spacing has been established behind the aircraft immediately preceding it in the overall landing sequence, the subject aircraft is instructed by ATC to leave its Sequencing Leg, on a *Direct-to* towards the Merge Point (MP) {FSR#14} — its position in the final sequence order is thus established;

  Notes:

  1. If the spacing requirements cannot be met before the aircraft reaches the end of the Sequencing Leg, the aircraft will continue on its P-RNAV route to the Merge Point – see scenario N1 below.
  2. The handling of aircraft that are not P-RNAV-capable is discussed in scenario N2 below.

- during the Direct-to section of the flight, the following separation rules apply:
  - in this case, the subject aircraft is on the higher, i.e. inner, Sequencing Leg, and as the aircraft starts to follow the Direct-to, vertical separation from traffic on the *adjacent*, i.e. lower, Sequencing Leg is maintained by ATC instructing the subject aircraft to maintain its altitude until longitudinal separation from the aircraft still on the adjacent Sequencing Leg has been achieved {FSR#15};
  - once the subject aircraft is clear of the adjacent Sequencing Leg *and* longitudinal separation from other aircraft also heading to the MP has been established (see {FSR#15 above}), it can be cleared to descend to the MP;
  - terrain/obstacle clearance is enabled by the minimum altitude of the MP being such that there is no terrain/obstacle that is higher than the MP anywhere in the sector of the circle defined by the MP and its outermost Sequencing Leg {FSR#16};

  - unless instructed otherwise by ATC, the aircraft flight crew is responsible for maintaining safe altitude from the start of descent on the "Direct-to" leg until acquiring the ILS glidepath {FSR#17}.

- finally, from the MP to the FAF, there is now only one horizontally-merged flow; along this segment, the aircraft continues its descent, and eventually acquires the Final Approach path.

Table 10 in Appendix A specifies each of the FSRs identified above.

3.6.3.2 Derivation of Additional FSRs for other Normal Scenarios

Other scenarios describing *normal* operations, are usually variations on scenario N0, two examples of which are as follows.

Firstly, scenario N1 in which a non-P-RNAV aircraft requires to join the landing sequence. In this case, all the ATC-related FSRs for operational scenario N0 apply, with the following addition:

> *FSR#18 All non-P-RNAV aircraft shall be vectored along the Point Merge routes to emulate P-RNAV aircraft, whilst being provided with obstacle / terrain clearance by ATC.*

Secondly, scenario N2 in which an aircraft reaches the end of its Sequencing Leg before it had been possible to find a slot for it in the landing sequence[25]. The FSRs for scenario N0 apply, with the following addition:

> *FSR#19 Each Point Merge route shall include a Sequencing Leg Run-off procedure (P-RNAV segments and / or ATC manual procedure) to ensure that an aircraft will automatically continue to the Merge Point, on a predefined vertical profile, in the event that no Direct-to instruction is received before reaching the end of the Sequencing Leg.*

Other *normal* scenarios might include the following:

- planned transitions into, and out of, Point Merge operations;
- planned change of runway (same direction);
- planned change of runway direction;
- onset of strong winds.

In analysing such scenarios, any additional FSRs would need to be identified and specified.

3.6.3.3 Logical FSRs for Normal Operations

Thus far, we have specified, at a conceptual level, *individual* FSRs for the management of conflicts and avoidance of collision for Point Merge operations under normal and abnormal conditions.

What needs to be done next is to describe *how* these FSRs map on to the ATM system and how the system itself needs to behave in order to achieve the desired result.

It was decided to carry out such analyses (and the subsequent failure analysis) at the level of the system *logical* design, which describes the main human roles / tasks and machine-based functions of the system but in a manner that is entirely independent of the eventual *physical* implementation of that design — to this extent it conforms to the associated provisions of Phase 9 of the IEC 61508.

[25] Could also be a mitigation of an ATM system failure – e.g. lost comms

A typical set of elements of the Logical Model that would be appropriate to Point Merge is shown in Table 6. The list is not exhaustive in that elements not specifically affected by Point Merge, e.g. are required to simply perform their normal functions, are excluded at this stage. The type of element is also shown, and is designated as MF (machine function), HR (human role) or a set of Data.

Table 6 ~ Logical Elements

ID	Description	Type
ACAS	Airborne Collision Avoidance System	MF
AD	Airspace Design	Data
AP/FD	Autopilot/Flight Director	MF
AMAN	Arrival Manager (tools)	MF
EXEC	Executive (Tactical) Controller	HR
FCRW	Flight Crew	HR
FDP	Flight Data Processing	MF
FMS	Flight Management System	MF
MSAW	Minimum Safe Altitude Warning	MF
PLNR	Planner Controller	HR
P-RNAV	P-RNAV Procedure	Data
STCA	Short-term Conflict Alert	MF
TAWS	Terrain Awareness Warning System	MF

Examples of how FSRs then map on to the relevant Logical Elements is shown in Table 7.

Table 7 ~ Example Mapping of FSRs to Logical Model

ID	Safety Requirement	Maps to:
FSR#3	Point Merge structures shall be segregated from restricted airspace	AD
FSR#7	Sequencing and spacing of traffic shall be established initially in adjacent En-route/ Terminal airspace sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow	AMAN, PLNR
FSR#10	Vertical separation, of at least 1,000 ft, between adjacent Sequencing Legs shall be provided, by appropriate published altitude restrictions along the entire length of the Sequencing Legs	P-RNAV
FSR#11	Aircraft on the same Sequencing Leg shall be separated longitudinally, by ATC, by a 3nautical mile radar -separation minimum, or the appropriate wake-turbulence separation minimum, whichever is the greater	EXEC

ID	Safety Requirement	Maps to:
FSR#16	Except where instructed otherwise by ATC, the aircraft shall assume responsibility for maintaining safe altitude from the start of descent on the "Direct-to" leg until acquiring the ILS glidepath	FCRW, TAWS

The mapping process would then be completed by deriving appropriate (lower-level, Logical) FSRs, for each Logical Model element, in response to the higher-level FSRs assigned to it.[26]

Given then a complete Logical Model, a technique that can be used very effectively in modelling the *behaviour* of transactional system such as ATM is some form of Use Case analysis. A suitable notation for this purpose would be a sequence diagram (SD), straightforward guidance on which can be found at Sparx Systems (2022).

For many ATM applications, SDs have proved to be a very useful design-analysis technique in that they:

- provide a means of cross-checking the completeness, correctness and consistency of the lower-level FSRs which are mapped on to the SD;
- tell us more about the intended operation of the ATM system than could the FSRs individually;
- are an effective way of highlighting transitions between, inter alia, separation modes at various points in the flight;
- provide very useful, scenario-based information for real-time operational simulations and the development of operator training material; and
- provide, for the subsequent failure analysis, a valuable insight into sources of potential system failures.

Furthermore, since it also defines the required behaviour of the ATC system), it is designated as a functional safety requirement in its own right.

In a full safety assessment, other normal scenarios might also need to be similarly analysed, including scenarios N1 and N2.

3.6.4 Adequacy of the Functional Safety Requirements

In the barrier-model approach outlined in Sub-section 3.4 above, it was noted that it is the functional properties of a barrier that determines the probability of successful mitigation of the input hazard, in the absence of failure internal to the barrier. It was also noted that, in case of the SESAR AIMs, the required probability of success, and the maximum rates of occurrence of failure and corrupt operation, of each barrier is, as far possible, based on actual historic data.

In practice, establishing a *direct* relationship between the required functional properties (FSRs) of a barrier, and the required probability of its successful mitigation of input hazards, can be far from straightforward, depending on the circumstances. This is illustrated by considering two general cases, as follows:

- when ATM operations, albeit conducted in a different way from previous operations in the subject environment, remain fully compliant with established ICAO Standards and Recommended Practices (SARPs);

[26] Not done herein in order to avoid unnecessary detail…

- when ATM operations deviate from those SARPs in some way.

The first case applies to Point Merge for which, in the various normal and abnormal scenarios, the FSRs are specified so as to ensure compliance with, for example, ICAO separation minima throughout each step/portion of arrival flight in Approach airspace.

The (qualitative) safety argument would then be relative — i.e. that, given previous (ICAO complaint) arrival operations in the airspace were deemed to be tolerably safe, Point Merge operations would themselves be safe in the absence of failure. Such an argument should be reinforced by demonstrating the viability of the FSRs, as a whole, through real-time simulations, from an ATC and/or aircraft perspective, as appropriate.

The second case would apply, for example, whenever separation was applied below the associated ICAO minima and would require a more direct approach. In the specific case of reduced vertical separation minima (RVSM) in European En-route airspace, data from real-time monitoring of aircraft height-keeping accuracy was used to compute (in effect) the probability of successful vertical separation between two aircraft separated nominally by 1,000 ft, in the absence of failure. Equivalent approaches have been applied in the safety assessment of reduced wake-turbulence separation, using real-time, LIDAR measurement of wave-vortex phenomena.

3.6.5 Point Merge Operations under Abnormal Environmental Conditions

The following are examples of what were identified as abnormal conditions relevant to Point Merge operations:

- Aircraft Emergency — medical, technical, etc.
- Aircraft experiences ACAS Resolution Advisory (RA)
- Unplanned runway change, e.g. unplanned change of direction
- Unforeseen runway closure, e.g. blocked runway
- Missed Approach
- Very strong winds, e.g. > 30 knots

Table 8 contains two examples and shows, for each abnormal condition concerned, the immediate operational effect, the possible mitigations of the safety consequence of that effect and the related FSR(s).

Table 8 ~ Example Mitigation for Abnormal Operations

Ref.	Abnormal Event	Operational Effect	Mitigation of Effects	FSR
1	Aircraft Emergency	Aircraft in the landing sequence needs priority over preceding aircraft	Move the affected aircraft up the sequence order, if necessary, creating a gap by vectoring a preceding aircraft out of the sequence	FSR#20
2	Aircraft experiences an ACAS RA	Aircraft in the landing sequence needs to follow the RA	If necessary to maintain separation, and once the RA has been resolved, remove the aircraft from the landing sequence	FSR#21

It is also possible to quantify the residual risk associated with each of the abnormal events; however, this is beyond the scope of this article. What is more important at this stage is that the above analysis identified the abnormal conditions that might be encountered in the Point Merge Operational Environment and specified potential mitigations of the consequences thereof.

3.6.6 Point Merge Operations under Internal-failure Conditions

Finally, for Phases 9 and 10, is the analysis of potential failures internal to the overall Point Merge ATM system.

IEC 61508 suggests a Risk Classification Scheme (RCS) as a possible method for deriving SIRs at this level but, having already cast doubt on the validity of RCSs used traditionally in ATM, we will now outline a scheme based on that used on the SESAR Programme, which resolves most, if not all, of those doubts. The approach has one RCS dedicated to each type of accident and a hazard-severity scheme based on the success or failure of the individual stages of the Barrier Model outlined above.

The illustration shown in Table **9** is for the MAC accident type, in Terminal airspace, for which the tolerable level of risk of an accident is 1E-9 per flight hour.

Table 9 ~ Illustrative Risk Classification Scheme

Severity Class	**Hazardous Situation**	**Operational Effect**	**MTFoO**[27]
MAC-SC1	An aircraft comes into physical contact with another aircraft	Accident — Mid-air collision	1E-9
MAC-SC2a	An imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact	Near Mid-air Collision	1E-6
MAC-SC2b	Airborne collision avoidance prevents near collision	Imminent Collision	1E-5
MAC-SC3	An imminent collision was prevented by ATC Collision prevention	Imminent Infringement	1E-4
MAC-SC4a	An imminent separation infringement coming from a crew/aircraft-induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced)	1E-3
MAC-SC4b	An imminent separation infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned)	1E-2

The tolerable level of risk for each for each hazardous situation (except for the ultimate occurrence, of an accident) is expressed in terms of the Maximum Tolerable Frequency of occurrence of the Operational Effect (MTFoO), the values for which were obtained from the corresponding AIM model. In allocating the risk budget to each hazard in a given

[27] MTFoO is the Maximum Tolerable Frequency of Occurrence per flight hour.

severity class, a pre-defined number of operational hazards was assumed for each severity class, e.g. a factor of 10 for each operational effect.

The use of the scheme then follows standard ATM safety practices, in deriving SIRs for lower-level elements of the ATM system — in this case, at the *logical* level of system design as introduced in Sub-section 3.6.2 above.

In assessing such outcomes of system failures, account must be taken of:

- any mitigations of effect that might be available and FSRs specified for any new mitigating measures. For example, "*FSR#22, Aircraft shall report loss of P-RNAV capability to ATC immediately*" could be a mitigation against an onboard failure affecting P-RNAV performance;
- the existence of possible common-cause failures that could undermine the (thus far) assumed independence of barriers, OSFs, SRSs or safety functions.

Finally, in assessing the effect of Point Merge operations on overall risk, from a system-failure perspective, this could be done one of two ways:

- *absolutely*, by considering *every* failure and calculating its risk contribution from the consequences and expected failure rate; or
- *relatively*, by comparing the risk between Point Merge and existing operations but only for any new system failures or existing failures for which the consequences had changed.

The latter approach would usually be preferred whenever the risk of *existing* operations had already been shown to be tolerable but, in either case, the overriding need is to comply with, *inter alia*, the following requirement of IEC 61508, Sub-section 7.5.2.5:

> *"If, in assessing the EUC Risk, the average frequency of dangerous failures of a single EUC control system function is claimed as being lower than 1e-5 dangerous failures per hour then the EUC Control System shall [itself also] be considered to be a safety-related control system [and] subject to the requirements of this Standard".*

4 Conclusions

This paper is the second in a series of three parts, which sets out to show what functional safety assessments for transport applications might look like if they followed the safety principles and lifecycle steps set out in IEC 61508-1 and IEC 61508-4. The first part (Fowler 2022) gave an overview of those principles and lifecycle steps, together with some transport-orientated guidance, illuminated by applying them to a simple, hypothetical example of the assessment of a proposed means of enabling pedestrians to cross a busy road safely.

The scope of that exercise was limited to the seven IEC 61508 lifecycle phases relating to the specification of safety requirements. This was because most of the key principles underpinning IEC 61508 — i.e. the universal principles set out in Parts 1 and 4 of the Standard, which govern the determination of the required risk-reducing properties of safety-related systems — take effect during these earlier phases, whereas the subsequent realisation and operating phases are less specific to the Standard.

The application, herein, of those principles to the ATM example of Point Merge operations has found that applying the subject IEC 61508 lifecycle phases directly to a typical project in the ATM sector was reasonably straightforward, and the results fitted well with the

forward-looking IACO Global ATM Concept and SESAR approach to ATM safety assessment. In particular:

- treating the flow of traffic through the airspace as being the "EUC" worked very well and rightly focussed the initial stages of the safety assessment where it should always be, i.e. on the hazards that exist in the airspace, which are inherent in aviation and which the ATM system has to be shown to be able to mitigate sufficiently, in order to achieve a tolerable level of risk;
- treating the overall ATM system as the "EUC Control System" followed naturally from our interpretation of the EUC and also worked well; it provided clarity on what was, and what was not, new in relation to Point Merge, and also between safety and non-safety issues;
- above all, the early IEC 61508 lifecycle steps, followed herein, demanded that the safety functionality and performance of the ATM system in the Point Merge context be specified so as to reduce EUC risk to better than a tolerable level, when operating correctly, *before* considering what happens to EUC risk in the event of system failure.

Hence, following the principles of the specific phases of IEC 61508 provides a considerable overall benefit of ensuring a better balance in the approach to functional-safety assessment than might otherwise be the case — for which see Fowler (2015).

Acknowledgments

The authors wish to acknowledge the considerable help, support and understanding of many colleagues from EUROCONTROL and beyond, over many years, without which this paper would not have come to fruition.

The copyright holder of the quotations from published standards used for illustration in this paper is the International Electrotechnical Commission, Geneva.

References

EUROCONTROL. (2018). *Safety Assessment Methodology — Safety Case Development Manual*. EUROCONTROL, The European Organisation for the Safety of Air Navigation. Available at https://www.eurocontrol.int/tool/safety-assessment-methodology, Accessed 8th September 2022.

EUROCONTROL. (2021). *Point Merge — Improving and harmonising arrival operations*. EUROCONTROL, The European Organisation for the Safety of Air Navigation. Available at https://www.eurocontrol.int/concept/point-merge, Accessed 19th November 2022.

Fowler D, Perrin E and Pierce R. (2009). *2020 Foresight — A systems-engineering approach to assessing the safety of the SESAR Operational Concept*. Paper 446 in Proceedings of the Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM 2009), Napa, California, USA. Available at https://drive.google.com/file/d/1Tq7Qs7Reuuk9Y_4dtoV-DJNkUVPzB51t/view, Accessed 19th November 2022.

Fowler D. (2015). *Functional Safety by Design — Magic or Logic?* In Proceedings of the 23rd Safety-Critical Systems Symposium, Bristol, UK. Available at https://scsc.uk/r129/7:1. Accessed 19th June 2022.

Fowler D. (2022). *IEC 61508 Viewpoint on System Safety in the Transport Sector: Part 1 — An Overview of IEC 61508*, in Safety-Critical Systems eJournal, Vol. 1, Iss. 2. Available at https://scsc.uk/r176.3:1, Accessed 29th December 2022.

ICAO. (2005). *Global ATM Operational Concept*. The International Civil Aviation Organisation. ICAO Doc 9854, 1st edition, 2005. Available at https://www.icao.int/Meetings/anconf12/Document%20Archive/9854_cons_en[1].pdf, Accessed 19th November 2022.

ICAO. (2011). *Aviation Occurrence Categories — Definitions and Usage Notes*. ICAO, The International Civil Aviation Organization. Version 4.2, Oct 2011. Available at https://www.icao.int/APAC/Meetings/2012_APRAST/OccurrenceCategoryDefinitions.pdf, Accessed 29th December 2022.

ICAO. (2014). *Procedures for Air Navigation (Operations) — Vol II, Construction of Visual and Instrument Flight Procedures*. ICAO, The International Civil Aviation Organization. Doc 8168-2, Edition 6, 2014. Available from https://skybrary.aero/sites/default/files/bookshelf/5801.pdf, Accessed 7th September 2022.

IEC. (2010). *Functional Safety of Electrical/electronic/programmable electronic Safety-related Systems*. IEC 61508, Ed.2. International Electrotechnical Commission. Geneva.

Reason J. (2000). *Human Error: Models and Management*, British Medical Journal, BMJ 2000;320:768. Available at http://www.bmj.com/cgi/content/full/320/7237/768, Accessed 21st September 2022.

SESAR. (2018a). *Safety Reference Material*. SESAR Joint Undertaking. Edition 00.04.01, 14 Dec 2018. Available at https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR2020%20Safety%20Reference%20Material%20Ed%2000_04_01_1%20(1_0).pdf, Accessed 19th November 2022.

SESAR. (2018b). *Guidance to Apply SESAR Safety Reference Material*. SESAR Joint Undertaking. Edition 00.03.01, 14 Dec 2018. Available at https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Guidance%20to%20Apply%20the%20SESAR2020%20Safety%20Reference%20Material.pdf, Accessed 19th November 2022.

SESAR. (2021). *Delivering the Digital European Sky*. SESAR Joint Undertaking. Available at https://www.sesarju.eu/sites/default/files/documents/reports/SESAR%203%20launch%20brochure.pdf, Accessed 19th November 2022.

Sparx Systems. (2022). *UML 2 Tutorial – Sequence Diagram*. Sparx Systems Pty Ltd. Available at https://sparxsystems.com/resources/tutorials/uml2/sequence-diagram.html, Accessed 29th December 2022.

Appendix A. Point Merge Functional Safety Requirements

The following table lists all Point Merge FSRs that have been derived from the analysis at 3.6 above and shows traceability back to the SRSs in Table 5.

Table 10~ Consolidated List of FSRs for SRSs

ID	Safety Requirement	Traceability
FSR#1	Vertical separation at intersections of Point Merge routes with SIDs shall be provided by aircraft conformance to appropriate published altitude restrictions	SCM-AOM
FSR#2	Vertical separation at intersections of Point Merge routes with pre-defined routes for transit flights, overflights and other arrivals shall be provided strategically by aircraft conformance to appropriate published altitude restrictions	SCM-AOM
FSR#3	Point Merge structures shall be segregated from restricted airspace	SCM-AOM
FSR#4	All P-RNAV routes (i.e. from IAF to FAF) shall be designed in accordance with ICAO PANS-OPS, (Doc 8168) Vol II	SCM-AOM
FSR#5	The required aircraft-arrival rate shall be derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as “metering” requirements based on runway capacity (arrivals and departures) and the limited ability of Approach airspace to absorb momentary traffic overloads	SCM-DCB
FSR#6	Holding points for arrivals shall be provide in an area between the IAF and Sequencing Leg entry point for use in the event that Approach airspace becomes overloaded or that the arrival flow becomes otherwise disrupted	SCM-AOM
FSR#7	Sequencing and spacing of traffic shall be established initially in En-route/ Terminal airspace sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow	SCM-ASS
FSR#8	The required aircraft-departure flow rate shall be derived by airport ATC and fed upstream to adjacent En-route / Terminal sectors for synchronisation with the arrival flow requirements	SCM-DS
FSR#9	ATC shall monitor aircraft conformance with all clearances and instructions, throughout each flight, including when aircraft are following predefined P-RNAV routes and associated altitude constraints	ATC-TCM AA, ATC-TCM AG

ID	Safety Requirement	Traceability
FSR#10	Entry into Approach airspace is coordinated with the adjacent upstream sector(s) according to the agreed entry conditions, including the aircraft being stable at the defined altitude well before Sequencing Leg entry	ATC-PTCM-AA
FSR#11	Vertical separation, of at least 1,000 ft, between adjacent Sequencing Legs shall be provided, by aircraft conformance to appropriate published altitude restrictions along the entire length of the Sequencing Legs	ATC-PTCM-AA
FSR#12	Aircraft on the same Sequencing Leg shall be separated longitudinally, by ATC, by a 3 nautical mile radar-separation minimum, or the appropriate wake-turbulence separation minimum, whichever is the greater	ATC-TCM AA
FSR#13	The minimum altitude of each Sequencing Leg shall be sufficient to provide vertical clearance from terrain/obstacles along its entire length	ATC-PTCM-AG
FSR#14	An aircraft shall not be turned off the Sequencing Leg towards the Merge Point until it is spaced behind the previous aircraft, i.e. the aircraft immediately preceding it in the final sequence, sufficiently to ensure that at least minimum longitudinal separation / wake-vortex criteria will be established well before vertical / lateral separation minima are infringed as a consequence of flow convergence	ATC-TCM AA
FSR#15	As each aircraft turns off the Sequencing Leg towards the Merge Point, vertical separation shall be maintained between it and all aircraft on the adjacent sequencing leg until horizontal separation is established (and can be maintained) between them	ATC-TCM AA
FSR#16	The minimum altitude of the Merge Point shall be set such that there is no terrain/obstacle that is higher than the Merge Point anywhere in the sector of the circle defined by the Merge Point and its outermost Sequencing Leg	ATC-PTCM-AG
FSR#17	Except where instructed otherwise by ATC, the aircraft (flight crew) shall assume responsibility for maintaining safe altitude from the start of descent on the “Direct-to” leg until acquiring the ILS glidepath	AB-TCM AG
FSR#18	All non-P-RNAV aircraft shall be vectored along the Point Merge routes to emulate P-RNAV aircraft, while being provided with sufficient obstacle / terrain clearance by ATC	ATC-TCM
FSR#19	Each Point Merge route shall include a Run-off procedure so that aircraft will automatically continue to the Merge Point, on a predefined vertical profile, if no Direct-to instruction is received before reaching the end of the Sequencing Leg	ATC-PTCM-AG
FSR#20	In the event of an aircraft emergency, ATC shall move the subject aircraft forward in the sequence order, (by an early Direct-to or by radar vectoring, as appropriate) sufficiently to minimise the delay to its landing	ATC-TCM AA

ID	Safety Requirement	Traceability
FSR#21	Where it is necessary to resolve a conflict (or other urgent situation, e.g. an aircraft ACAS RA), ATC shall remove the affected aircraft from the landing sequence and reinsert upstream, i.e. later in the sequence, by radar vectoring.	ATC-TCM AA
FSR#22	Aircraft shall report loss of P-RNAV capability to ATC immediately	ATC-PTCM AA, ATC-PTCM AG

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

The Terminological Analysis Method SemAn and its Implementation

Peter Bernard Ladkin[1], Lou Xinxin[2], Dieter Schnäpp[3]

1. Causalis Ingenieurgesellschaft mbH, Bielefeld, Germany.
2. Causalis Ing.-GmbH. Currently at TÜV Süd, München, Germany.
3. Technische Universität Braunschweig, Institut ITL. Currently at DKE, Offenbach.

Abstract

We present the method "SemAn" for the semantic analysis of electrotechnological definitions appearing in IEC standards. SemAn is accompanied by a software tool, the SemAn Analyser, which outputs partial SemAn results in a pretty-printed and annotated format retaining the symbol-for-symbol syntax of the original definiens text. We discuss the purpose and use of this method and tool.

1 Introduction

1.1 Intellectual Background

Gottlob Frege published his *Begriffschrift* (literally, "concept-writing") in 1879 (Frege 1879); see also Wikipedia (Begriffschrift 2023). It was by no means the first attempt to render natural language into a form in which logical reasoning could be formulated and used (Aristostle's Syllogistic is perhaps the first such writing), but it has become the most successful, resulting almost immediately in what we know today as Predicate Logic, or First-Order Logic (Goldrei 2005). The use of such formal languages and logic is widespread in digital-computer science, not only in building circuits which exemplify calculations based on the "logical constants" AND, OR and NOT, but in formal languages for specifying and describing computations, as well as systems which check whether such descriptions (including high-level-language "source code") fulfil their expectations.

The ability to render natural language into formal language is taught to most university freshman philosophy students in introductory logic courses. However, rendering the semantics of most of any natural language (such as English) in a modern-logical system is far more problematic, quite apart from the doubts concerning whether such an enterprise can be at all successful (Wittgenstein 1953/1967); see also (Kripke 1982). A series of sophisticated attempts at a formal semantics for English were made by Richard Montague from 1955 to around 1970 (Montague 1974), using Higher-Order Modal Logic. Montague Semantics has subsequently been quite successfully pursued in linguistics (Janssen 2011). There are other formal semantics such as Situation Semantics (Kratzer 2007). Almost all these formal (logical) renderings refer to objects, their properties and relations between them. There is a discipline which looks at what objects the use of a natural language presumes; known as natural language ontology (Moltmann 2022). The study of ontology (rather, ontologies) is now pursued in terminological definition in computer science, and

increasingly in related engineering disciplines, e.g. the SCSC Ontology Working Group (Safety-Critical Systems Club 2023).

Ontologies speak to what objects there are. Besides objects, Fregean *Begriffschrift* and its formal-logical successors speak to properties of those objects and their relations; at time of writing, properties and relations are not as well-developed interests in computer science as objects are, although they are essential for a rendering of natural language into such formal languages.

Functional requirements specifications for digital-computer-based systems may often be rendered in formal languages specially developed for the purpose, as may, rather more easily, specifications for algorithms; see, for example Lamport (2003). The purposes of this move to formality include avoiding ambiguity, as well as enabling mathematically-rigorous checking that, say, a computer program actually fulfils its functional requirements. However, in broader engineering disciplines, it is often required that functional specifications are written in natural language — indeed, that the natural-language specification is the legally-valid specification of requirements. There are thus two main reasons why it is desirable that engineering concepts in natural language be rendered more formally:

1. It ensures that engineers are using a term to refer to one and the same concept in various working environments, in particular when they are discussing technical matters; and
2. It allows legal requirements to be formulated in such a way that enables mathematically-rigorous checking that, say, a computer program written by a supplier fulfils those requirements.

Both of these are major undertakings. The first is good practice, but only the second is (recently) recognised as an engineering discipline in its own right. The importance of the former is, however, understated. Concepts such as "risk" are formally defined in electrotechnical standards — and there are many of them, some of them very different from others. Risk is a central concept for safety engineering, and there is at time of writing an Advisory Group of the International Electrotechnical Commission (IEC) attempting to arrive at a "harmonised" definition of the concept, because of the engineering problems caused by the plethora of existing definitions (IEC 2023).

More importantly, people have been jailed in England based on arguments about the meaning of electrotechnical terminology and what this implies for software-based system behaviour. The transcript of the trial of Ms. Seema Misra for fraud in the use of the Post Office Horizon system is available (Mason 2015). There is a commentary on the use of technical terminology in this and related cases (Ladkin 2020). We are happy to report that Ms. Misra was acquitted on appeal in April 2021.

We conclude it is important to get electrotechnical terminology "right". Whatever "right" may be, considering what happened to Ms. Misra, it should reflect the reality of systems and their behaviour; other desirable properties may be clarity, and non-ambiguity (absence of homonyms).

It is not our purpose here to discuss general properties of terminology further, but rather to present a technique and a software implementation of that technique that has had some encouraging application to the analysis of electrotechnical terminology defined in standards of the International Electrotechnical Commission to enhance clarity and highlight ambiguity and point, in some cases, towards resolution.

The technique is called "SemAn", and the software tool the "SemAn Analyser". SemAn is conceptually a translation of (actual) terminology definitions into a language of Sorted

First-Order Quantifier-Free Logic. Illustrations are given below of how this helps to analyse the concepts involved. The SemAn Analyser annotates the natural-language definitions through the devices of pretty-printing and annotation with the logical constants AND and OR (quite literally, "annotates" — all symbols of the original definition are retained in the exact order in which they occur); again, examples are given below.

In contrast to philosophical or (most) linguistic purposes, the point of SemAn and the SemAn Analyser is not to render the exact meaning of a natural language phrase, but to exhibit a (*not* "the") logical structure, which will show engineers more clearly what is or seems to be meant, and highlight various possibilities for improvement. Terminology work is ongoing at the IEC and the SemAn Analyser annotations have been (cautiously, in preliminary viewing) welcomed.

SemAn and the SemAn Analyser were developed on the terminology introduced in the IEC standards and standards-like documents on functional safety and cybersecurity[1]. We can confidently state that for this specific terminology corpus, which includes over 450 terms with between 60 and 70 of them multiply/variantly defined, SemAn and the SemAn Analyser render a service known to be needed and indeed "required" by the ISO/IEC Directives but (we would suggest) often absent.

1.2 Conventions Used

In this paper, we give and discuss SemAn in two ways: as a principled method, and as the output to a tool partially implementing the method, known as the SemAn Analyser. We write manual SemAn, in Sub-sections 4.3 and 4.3, in a language of sorted predicate logic. The output of the SemAn Analyser is given pretty-printed in `Courier` font. We need to distinguish the two analyses, for example a manual SemAn introduces Meaning Postulates (MPs), and the SemAn Analyser has no facility to do this. We find that distinguishing the analyses typographically is the easiest way to do so.

2 Semantic Analysis by Means of SemAn: Preliminaries

2.1 The Scope of SemAn

The term "semantic analysis" is used here as a technical term which refers to a specific way in which definitions in technical terminology may be analysed. The SemAn method has been developed specifically for electrotechnical terminology occurring in Clause 3, "Terms and Definitions", of IEC standards. Manual examples of SemAn are given first, below, to show the method. Output of the SemAn Analyser is formatted ("pretty-printed") text with annotations illustrating logical structure.

SemAn is particularly geared towards comparative analysis, in which one has syntactically-varying definitions of the same term (homonyms), or syntactically-similar definitions of different terms (quasi-synonyms). SemAn allows the similarities and divergences between the terms to be illustrated in a canonical and intuitive way. SemAn

[1] The original list of definitions was compiled in Project Harbsafe by Sven Müller, at the time with VDE and at time of writing with DB Systel GmbH, from IEC-61508-4 2010, IEC-62443-2-1 2010, IEC-62443-2-4 2015, IEC-62443-3-1 2009, IEC-62443-3-2 2020, IEC-62443-3-3 2013, IEC-63069 2019, ISO/IEC-51 2014, and IEC-120 2018 (IEC various dates) (ISO/IEC2014).

exhibits the logico-semantic structure of individual natural-language definitions, so it also enables individual definitions to be improved to enhance understanding.

There is no one unique resulting analysis of a definition in SemAn. One may choose different primitives (unanalysed words or phrases): in one analysis, a syntactic unit may be taken to be primitive; in another analysis, a slight divergence of that syntactic unit from another item in a related definition may require the unit be further analysed (as a compound of further primitives) so that the divergence can be exactly specified[2].

The software tool SemAn Analyser gives one output per conformant definition, illustrating the logical form of the definition while taking the individual syntactic units to be primitive. It annotates the *definiens*[3] with logical constants and punctuation and pretty-prints it, as for example in Sub-section 2.4. Further examples of SemAn Analyser output are given in Section 3.

2.2 The Formal Language of SemAn

Formal semantic analysis in the linguistics of natural language, as it is practiced today, uses formal annotation into which a target definition is parsed. So does SemAn. The language used is isomorphic to the language of first-order logic (FOL). An introduction to the language of propositional logic and FOL is to be found in Goldrei (2005). Nearly a century and a half of experience with FOL has established its pre-eminence as a system in which assertions may be made with precision, and formal inferences may be precisely codified (there are other logics, often known as higher-order or non-classical logics, depending on their type, which are useful for similar purposes in domains in which FOL is limited). The language of FOL (LFOL) consists of

- predicate symbols;
- object symbols (divided into constants, which SemAn uses, and variables, which SemAn does not use);
- functional symbols (largely not used in SemAn);
- the logical constants AND, OR (used widely in SemAn and SemAn Analyser);
- the logical constant NOT (largely not used in SemAn and SemAn Analyser, because negations are often incorporated into the terms themselves); and
- quantifiers, largely incorporated into the syntactic items themselves (as negation often is).

The meaningful syntactic units of LFOL are sentences. There are no meaningful parts of sentences, such as phrases, which are not themselves sentences. This entails that translating natural language expressions into LFOL requires expanding the expressions to conform with the phraseology of LFOL.

2.3 Translating Natural Language Phrases into the Language of SemAn

As far as is yet known, there is no generally-accepted algorithm for translating natural language sentences into LFOL in a way that preserves their meaning. However, there are some more or less standard translation rules, partly illustrated below.

[2] An example is given in the manual SemAn of "harm" in Sub-section 4.2 below, in which "physical injury" and "damage to the health of a person" are discussed.

[3] In linguistics and analytical philosophy, a term being defined is known as the "*definiendum*" and the definition the "*definiens*". IEC uses the words "term" and "definition", but these have wider general use than just in Clause 3 of standards. We thus prefer to use technical terms for the linguistic items appearing in such Clauses 3.

(English) *John or Joan opened the front door*

First, the phrase in subject position, *John or Joan*, has no equivalent in LFOL. In LFOL, OR may only be used to conjoin sentences. Second, there are no syntactic elements corresponding to phrases in LFOL, only sentences and their component symbols. Third, the sentence intuitively speaks to one of two situations; one in which John opened the front door, and another in which Joan opened the front door (as well as a third in which they both did, but presumably not simultaneously). These observations may be used to convert the English sentence into one conforming to LFOL with the same intuitive meaning, namely:

(LFOL) *John opened the front door OR Joan opened the front door*

In English, phrases in subject position or object position can also be lists, with one constant (usually separating the last two list words) and separated by commas, as in

(English) *John, Joan or Jeremiah opened the front door*

Similar principles apply here as above, and we obtain the translation

(LFOL) *John opened the front door OR Joan opened the front door OR Jeremiah opened the front door*

A further step is that of constructing synonyms for predicates. In this example, three different people seem to have engaged in the same action, "*opened the front door*". In LFOL, the following action can be performed. A simpler symbol may be used to stand for the verb phrase "*opened the front door*". Second, whereas in English the subject (the person who opened the door) is typically written first and the predicate (the action) follows, with no punctuation, as in *John opened the front door*, in LFOL the assertion is expressed in a symbolic form akin to that of the elementary mathematics of functions: the argument (whoever did the opening) is expressed in parentheses after the predicate, as in *opened-the-front-door(John)* (here, hyphens are used to indicate that the predicate is denoted by a string of words rather than a single word). When symbol P is chosen to represent *opened the front door*, then this becomes syntactically easier to read.

(LFOL) Let the symbol *P* stand for the predicate "*opened the front door*". Then the assertion becomes:

P(John) OR P(Joan) OR P(Jeremiah)

SemAn uses such a natural-language version of LFOL as has been illustrated above. By experience, the illustrated translations seem to cover the routine majority of the task of translation. This language will become clearer when examples are discussed below.

3 The SemAn Analyser

3.1 *Modus Operandi*

The SemAn Analyser, in contrast to (manual) SemAn, does not use LFOL at all. It parses, annotates and pretty-prints the words and punctuation in the definition itself, in the order in which they occur. A manual translation from SemAn Analyser output into LFOL is intended to be straightforward. If a translation is not straightforward, this serves as an indication that the original definition proposed may be deficient; unclear, say. The recommended remedy is to modify the source definition so that the translation of SemAn Analyser output into LFOL becomes straightforward.

The SemAn Analyser:

- Takes all English words as primitive formal symbols
- Exhibits the logical structure of phrases by means of annotations using the logical constants (AND, OR, more rarely NOT) and marked indents

3.2 Implementation

The SemAn Analyser uses Dependency Parsing (Jurafsky and Martin 2020). It is programmed using the Dependency-Parsing suite spaCy (ExplosionAI n.d.). The programming is largely due to the second author, with help from the third author. All authors were continually involved in the evolution of the output specification.

3.3 A Simple Example

Consider the two following definitions of "signal". These are not original IEC terminology, but are "cleaned up" from existing definitions. The *definiendum* is given in bold-face font on a line by itself. The *definiens* follows on the next line, optionally prefixed by an "area of application" given in angle brackets. Here, the areas of application are "electrical", respectively "information".

signal
<electrical> electrical impulse controlled or observed by a test resource

signal
<information> visual, audible, or other indication used to convey information

The annotated versions would ideally be[4]:

```
signal:
<electrical> electrical impulse controlled or observed by a test
resource
\\
electrical impulse
                      > [OR] controlled
                      > [OR] or observed
                                > by a test resource
signal:
<information> visual, audible, or other indication used to convey
information
\\
     > [OR] visual
     > [OR] , audible
     > [OR] , or other indication
                           > used to convey information
```

SemAn Analyser thus exhibits the first as a sort, *electrical impulse*, with one of two relations to a *test resource*, that of being *controlled* or that of being *observed*. The second definition is a disjunction: the qualifier of all three disjuncts is that they are *used to convey information*, and the information conveyer may be *visual* or *audible* or an *other indication*.

[4] It has been suggested that there might be an alternative reading. This may well be. One of the purposes of SemAn Analyser output is to make clear such possibilities. SemAn Analyser output is dependent upon a non-deterministic parser, so such possibilities can be expected to arise simply from the parsing operation itself.

In this case, with simple and short definitions which have no key terms in common, a comparison of the two *definiens* shows that they are clearly distinct concepts.

Note: the above SemAn renderings are manual. The current implementation of the SemAn Analyser does not in fact output these annotations, although we wish it did — it renders both definitions without the annotations shown here. However, the examples of *application*, *harm* and *asset*, following, are indeed output by the current implementation of SemAn Analyser.

3.4 "Application"

An example which intuitively illustrates the benefits of logical annotation in more complex definitions is that of *application*, defined as

```
software program that performs specific functions initiated
by a user command or a process event and that can be
executed without access to system control, monitoring, or
administrative privileges
```

Parsed, this becomes:

```
\\
     software program
          > [AND] that performs specific functions
                       > initiated by a | [OR] user command
                                        | [OR] or a process event
          > [AND] and that can be executed without access
                       > to | [OR] system control
                            | [OR] , monitoring
                            | [OR] , or administrative privileges
```

This shows the clear logical structure that:

- this is a software program (defines the *sort*, the type of object which is being talked about);
- that this program has two properties:
  - of performing specific functions …
  - of executing without access to …
- and that these properties have further logical details.

3.5 "Harm"

The annotated/pretty-printed output of the SemAn Analyser invoked on the term *harm* is as follows::

```
67.
harm:
physical injury or damage to the health of people or damage to
property or the environment
\\
     [OR] physical injury
     [OR] or damage
               > [OR] to the health
                            > of people
               > [OR] to property
               > [OR] or the environment
[Source: IEC 61508-4:2010]
```

It can be seen that the SemAn Analyser takes the definiens as syntactically given and marks it up. It treats *physical injury* as a primitive. Below (Sub-section 4.2), a manual SemAn does not take this phrase as primitive, but invokes *Meaning Postulates*, which allow *physical injury* to be compared with *damage to the health of people* in order to determine if the definition can be expressed more succinctly and clearly (answer: yes).

It follows that the output of the SemAn Analyser is not a full SemAn, but a preliminary processing of the definition that exhibits certain formal features of the definition, enabling improvements to be made where they are appropriate, and which enables a human analyst to continue the SemAn if desired; for example by considering the meaning of *physical injury* and relating it to *damage to the health of people*. It is also clear from the example of *signal* that the current implementation of the SemAn Analyser does not quite yet do all we wish to expect of it.

4 Examples of SemAn Analyser Output and of SemAn

4.1 Output of SemAn Analyser on *asset*

There are two non-identical definitions of *asset* in the IEC 62443 series of standards. Both are considered below, in order to illustrate the harmonisation task, and to show how much easier it is made by using the SemAn Analyser.

SemAn Analyser output on the two definitions of asset is:

```
10.
asset:
physical or logical object owned by or under the custodial duties
of an organization, having either a perceived or actual value to
the organization
\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]

11.
asset:
physical or logical object having either a perceived or actual
value to the IACS
\\
     physical or logical object
          > having either a perceived or actual value
                 > to the IACS
[Source: IEC 62443-3-3:2013]
```

This annotated parsing/pretty-printing immediately shows a number of similarities and differences in the two definitions. First, an *asset* is a *physical or logical object*[5]. Second, it *[has] a perceived or actual value*. To whom the value accrues is different in the two cases (some implicit *organisation* in the first, presumably a human organisation such as a company; in the second, a system, namely the *IACS* (Industrial Automation and Control System)). Similarly, the first definition mentions custodial duties associated with the asset; the second mentions no such duties.

This comparison gives clear indications of difference, and therefore the scope of discussion, to domain experts attempted to harmonise the two definitions. The harmonisation task here is twofold:

- To whom/what does the *value* of the *asset* accrue?
- Is the ownership/custody of the asset a key property? Is it implicit, or does it need to be explicit?

4.2 Example: A Manual SemAn of *harm*

1. harm IEC 61508-4 subclause 3.2.1 and IEC Guide 120 subclause 3.7 :

physical injury or damage to the health of people or damage to property or the environment

SemAn goes further than the SemAn Analyser, using domain knowledge about the concepts (words and phrases) occurring in the definition (recall that the SemAn Analyser takes these as primitive). Invoking domain knowledge results in a meaning postulate. Because the result analysis has used the meaning postulates, they are restated along with the result of the SemAn.

First is to fill this definition out by "expanding conflations", as follows.

- Expand syntactic conflation: "OR" is used to conjoin two noun phrases. The SemAn Analyser has identified two "levels" of conjoined phrase:
  - associated with *physical injury*
  - associated with *damage*

  A first step is thus to expand. The *damage* is associated with the same qualifying phrase, namely

  to the health of people OR to property OR to the environment

  There are two ways this qualifying phrase can be treated:
  - Parentheses can be used to make a unit out of this phrase:
    (to the health of people OR to property OR to the environment)
  - An auxiliary definition can be used:
    Let *P* stand for *to the health of people OR to property OR to the environment*

- The resulting phrase is:

  physical injury (to the health of people OR to property OR to the environment)
  OR
  damage (to the health of people OR to property OR to the environment)

[5] An "or" occurring in an input phrase, as here, is simply a syntactic token. The "OR" outputted as annotation by the SemAn Analyser is intended to be the logical constant OR. The SemAn Analyser at present has no mechanism for recognising syntactic tokens representing logical constants in the input and manipulating its output accordingly.

Alternatively

P(physical injury) OR P(damage)

The second alternative is obviously of no help whatever in further analysis. The first alternative is used to proceed.

- Consider next the first conjunct:

  physical injury (to the health of people OR to property OR to the environment)

  The ORs can be expanded further:

  physical injury to the health of people
  OR
  physical injury to property
  OR
  physical injury to the environment

  Semantic domain knowledge is invoked: (Meaning Postulate MP1) only people or sentient beings can be physically injured, not property or the environment. According to (MP1), then, this may be further reduced:

  physical injury to the health of people

  Using further domain knowledge, we note that physical injury to the health is redundant:

  physical injury to people

- Consider the second conjunct:

  damage (to the health of people OR to property OR to the environment)

  Again, this expands to:

  damage to the health of people
  OR
  damage to property
  OR
  damage to the environment

- Conjoining the two expanded/reduced phrases gives

  physical injury to people
  OR
  (damage to the health of people
  OR
  damage to property
  OR
  damage to the environment)

  Note that logical OR is associative: *A OR (B OR C)* is the same as *(A OR B) OR C*, and thus either may be written unambiguously without parentheses: *A OR B OR C* (Goldrei 2005). So this can be written:

  physical injury to people
  OR
  damage to the health of people
  OR
  damage to property

OR
damage to the environment

- *Physical injury* is a term which contains *injury*, and (Meaning Postulate MP2, obviously related to MP1) injury can only occur to sentient beings. The term *people* is used; (domain knowledge) *people* is a plural of *person*, as is *persons*. The question arises if *harm* can be caused to one *person*, or must it always be more than one (plural)? Singular or plural? (Meaning Postulate from domain knowledge MP3) Harm to one person is still harm. The issue could be clarified by rewriting *people* as *one or more persons*

  physical injury to one or more persons
  OR
  damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

- The first two conjoined clauses have as part *one or more persons*. Furthermore, they are semantically related: (MP4) *Physical injury* is *damage to the health* of (a person or persons). But is all *damage to the health* also *physical injury*? No, there can be damage to health that is predominantly psychiatric: post-traumatic stress syndrome for example. So (MP5) *damage to the health* includes *physical injury* but not vice versa. Put in terms of logic,

  physical injury to one or more persons
  IMPLIES
  damage to the health of one or more persons

  but not vice versa. It follows that the first clause can be omitted without semantic loss. However, an analyst might wish to retain it as a means of emphasis[6].

- Result:

  damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

  Alternatively,

  physical injury to one or more persons
  OR
  other damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

[6] There are circumstances in which additional words are logically unnecessary, but help to ensure understanding, and that it is ideally part of an analyst's skillset to recognise such cases.

- Finally, these could be consolidated, by regrouping according to English conventions, for example:

  physical injury or other damage to the health of one or more persons
  OR
  damage to property or to the environment

  Alternatively,

  damage to the health of one or more persons, or to property, or to the environment

- The second definition can now be considered.

  2. harm IEC Guide 51 subclause 3.1:

  injury or damage to the health of people, or damage to property or the environment

- Comparing with the analysis of IEC 61508-4 subclause 3.2.1 above, it is clear that
  - the analysis can proceed largely as before;
  - (MP6) *damage to the health* can be considered equivalent to *injury*

- Result:

  damage to the health of people, or damage to property or the environment

  Equivalently

  injury to people, or damage to property or the environment

Given that people and one or more persons are synonyms, as are injury to and damage to the health of, it follows that, under MP1 … MP6, the two definitions are synonymous. The results may be expressed as follows:

- Under meaning postulates[7]

  (MP1) only people or sentient beings can be *physically injured*, not property or the environment;

  (MP2) *injury* can only occur to sentient beings;

  (MP3) *harm* to one *person* is still *harm*;

  (MP4) *Physical injury* is *damage to the health* of (a person or persons);

  (MP5) *damage to the health* includes *physical injury* but not vice versa; and

  (MP6) *damage to the health* can be considered equivalent to *injury*,

  the two definitions are synonymous and equivalent to:
  physical injury or other damage to the health of one or more persons, or
  damage to property or to the environment
  damage to the health of one or more persons, or to property, or to the environment
  injury to people, or damage to property or the environment

- It follows that there is a harmonisation task, but one which is in this case purely syntactic: an analyst must choose between the three example definitions above (or ones

[7] Note these MPs are specific to the SemAn of "*harm*". This article does not address the appropriate formulation of MPs across multiple definitions and resolution of possible conflicts. We are not so far along.

in which synonymic phrases are used, such as *people* instead of *one or more persons* or vice versa).

This analysis is laborious, and the result relatively easily foreseeable from the start, but the purpose is to illustrate the principles and steps involved in a manual SemAn, including the formulation of MPs and this is shown more easily on such straightforward examples[8].

4.3 SemAn Example: *asset*

1. asset, IEC 62443-1-1 subclause 3.2.6 and IEC 62443-2-1 subclause 3.1.3

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

The SemAn proceeds with similar steps to that of *harm* in Sub-section 4.2. The steps are not elaborated here in as much detail. However, the SemAn itself is more complex.

- Expand: An *asset* is a *physical object OR a logical object <with additional properties>*. The adjectives here are (Meaning Postulate MP1) applicative, so an *asset* is an object. It is left unexplained exactly what a logical object is. (One might speculate that a *metaphysical object* is meant, but most engineers do not use that term.) Introduce the primitive *Ob* to denote the thing of sort Obj which is being talked about. The mathematics-type notation typical of formal logic is used: *P(Ob)* says *Ob is physical*, whereas *L(Ob)* says *Ob is logical*. For objecthood, then, the term *Ob* of sort Obj has been introduced and yields the assertion *P(Ob) OR L(Ob)*.
- Fill out *<additional properties>*: another OR syntactic conflation is expanded.

  owned by an organisation OR under the custodial duties of an organisation.

  There is another sort here, *organisation*. Whereas for *Ob*, a specific *asset* is meant, the organisation is unspecified: (MP2) *some organisation* is meant. The term *some* is a quantifier and in logic, one would be tempted to quantify: "*there is an organisation Org such that …*". But, for a given *asset*, it can be assumed that (Meaning Postulate MP3) there is just one organisation that owns it or just one organisation that has custody of it. Note that this meaning postulate is not like the ones involved in the analysis of *harm*; it involves rather an assumption about the way of the world; that if there are multiple owners or custodians, just one can be singled out to be *Org* for the purposes of the definition. So, for *Ob*, there is a single *Org* of sort *Organisation* (let us say *Orgn*) which either *Owns* it or *HasCustody* of it:

  Owns(Ob,Org) OR HasCustody(Ob,Org).

- Fill out ",": there is a list of properties here, starting with *owned by … OR under the custodial duties of …* and then *having … .* It is clear that *AND* is meant by the comma.
- Fill out further. Result: *(Ob has a perceived value to Org) OR (Ob has an actual value to Org)*. Choose primitives *PV* and *AV* for the predicates *has a perceived value to* and *has an actual value to*. The result is *PV(Ob,Org) OR AV (Ob,Org).*
- Result: it seems the analysis has arrived at the following, in formal form:

  P(Ob) OR L(Ob) AND Owns(Ob,Org) OR HasCustody(Ob,Org) AND PV(Ob,Org) OR AV (Ob,Org)

[8] There might be disputes concerning the MPs, and such disputes could be problematic in, say, courts of law. The result given here follows from the MPs given. We construe the SemAn task here as identifying the need for, and formulating, MPs. The validity of MPs so formulated may indeed be doubted, but resolution of such doubts we see as a task more appropriate for the accompanying, more philosophic-analytic, technique ConcAn (Ladkin 2022).

However, there is an AND..OR ambiguity which needs to be disambiguated. AND..OR ambiguities arise because *A AND (B OR C)* does not have the same meaning *as (A AND B) OR C* and when there are no parentheses, as in *A AND B OR C*, one cannot tell which is meant. To disambiguate, parentheses are used:

(P(Ob) OR L(Ob)) AND (Owns(Ob,Org) OR HasCustody(Ob,Org)) AND (PV(Ob,Org) OR AV (Ob,Org))

- Rewriting the result: This formula looks "formal" and is typical for the indication of the logical structure of phrases and sentences/assertions. But it is hard to read. There are some ways to make such formulas easier to read, for example the vertical stacking of clauses, as in TLA$^+$ (Lamport 2003)[9]. In the TLA$^+$ "pretty-printing" style, all clauses in a conjunction are preceded by the conjunction sign and stacked vertically, *mutatis mutandi*s for disjunction. Indentation allows the elimination of the parentheses used for disambiguation:

  && P(Ob) OR L(Ob)
  && Owns(Ob,Org) OR HasCustody(Ob,Org)
  && PV(Ob,Org) OR AV (Ob,Org)

  The OR clauses within the conjuncts can be similarly formatted if so wished (the symbol ⋁ is used to denote OR), to yield:

  && ⋁ P(Ob)
  ⋁ L(Ob)
  && ⋁ Owns(Ob,Org)
  ⋁ HasCustody(Ob,Org)
  && ⋁ PV(Ob,Org)
  ⋁ AV (Ob,Org)

  but there seems to be little point to doing so here. It is up to the analyst to decide which is most helpful. The sorts of *O*b and *Org* have been so far left implicit, but there might be circumstances in which one needs to reason with them taken into account (see below). When introduced, the formal sentence in the language of sorted logic looks like:

  && Obj(Ob)
  && Orgn(Org)
  && P(Ob) OR L(Ob)
  && Owns(Ob,Org) OR HasCustody(Ob,Org)
  && PV(Ob,Org) OR AV(Ob,Org)

Consider now the second definition of asset.

2. asset IEC 62443-3-3 subclause 3.1.1
physical or logical object having either a perceived or actual value to the IACS

- Fill it out: The first observation is that too much was done with the first definition. The predicate *physical* need not have been separated from the predicate *logical*: instead of *P(Ob) OR L(Ob)* we could have used one predicate *PorL(Ob)*. But no matter; it was done, and will be left so.
- Fill it out: again, *perceived value OR actual value*, but the subject of the valuation has changed. Now, it is not an *organisation* (a group of people) but is an engineering object, a system, namely the Industrial Automation and Control System — IACS — to

[9] TLA = Temporal Logic of Actions

which the IEC 62443 series is specifically targeted. Here, (Meaning Postulate MP3) there is no possible ambiguity as to which IACS is meant: it is the one to which this standard is currently being applied. A sort *IACS* is introduced along with a primitive *theIACS* for an object of this sort.

- Result:

  && Obj(Ob)
  && IACS(theIACS)
  && P(Ob) OR L(Ob)
  && PV(Ob,theIACS) OR AV(Ob,theIACS)

There are now two analysed definitions of *asset*, which are not identical. The term *asset* is thus a homonym. The task of harmonisation is to select one of these as the primary definition. There are most often two ways in which this may be done. First, definitions may be specialised to domains of application, as illustrated in Sub-section 3.3. So, for example, *signal* means one thing in railway control, and another thing in wire-transmitted telecommunications, leading to two definitions, one for *signal (railways)* and a different one for *signal (telecommunications)*. The specialisations in electrotechnical terminology usually follow the designations of the IEC Technical Committees (TC 9 is Electrical equipment and systems for railways); there are many Technical Committees which could (and do) use a telecommunications notion (in fact, signal has many definitions; see Sub-section 3.3). The second way is by reconciling the two different definitions into one. Considerations towards the second path are illustrated here.

- Much of both definitions is the same, but some of it is definitively different. The IACS in question is uniquely determined: it is whichever system the IEC 62443 series of standard is applied to in the instance of its application. The organisation involved (according to the first definition) might also be unique, but it could be that many organisations are involved in the joint ownership or custodianship of an asset. Is an IACS, as a nonsentient physical object, an object of which it might make any sense at all to speak of as having values? Or is the valuer an implicit organisation which is considering *Ob* and *theIACS* together, to determine whether there is a perceived or actual "value" (causal influence?) of the one on the other? Say, *PV(Ob,theIACS,Org) OR AV(Ob,theIACS,Org)*. The SemAn analyst cannot decide such matters; the domain specialists writing the standard must do so.

4.4 Output of SemAn Analyser on *asset*

There are two non-identical definitions of asset in the IEC 62443 series of standards. Here is the output of the SemAn Analyser on both:

```
10.
asset:

physical or logical object owned by or under the custodial duties of
an organization, having either a perceived or actual value to the
organization

\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
```

```
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]

11.
asset:

physical or logical object having either a perceived or actual value
to the IACS

\\
     physical or logical object
          > having either a perceived or actual value
                > to the IACS
[Source: IEC 62443-3-3:2013]
```

This annotated parsing/pretty-printing shows immediately and clearly the similarities and differences immediately which we have recognised in the more laborious manual SemAn. Namely, first, an *asset* is a *physical or logical object*; and, second, this object *[has] a perceived or actual value*. To whom the value accrues is clearly different in the two cases. Further, one definition mentions custodial duties associated with the asset; the other does not. This comparison gives clear indications of the differences seen during the manual SemAn, and leads to the same scope of discussion for domain experts attempting to harmonise the two definitions as did the manual analysis.

5 Conclusions

We have argued, briefly, that getting electrotechnical terminology "right" is an important task, for many reasons (not least, that using it properly may help keep some innocent people out of jail!). Logical annotation seems to us to be a helpful method of doing so, and we have explicated here a method of logical analysis, SemAn, and an annotator, the SemAn Analyser, which annotates according to SemAn but without (as yet) using Meaning Postulates.

We have endeavoured to show by example that such analyses are useful in identifying similarities and distinctions in definitions which are ripe for clarification. Meaning Postulates can help, but skill is involved in the formulation of the Meaning Postulates and we don't see at present how this process may be automated.

Experience has shown that use of the SemAn Analyser eases the task of performing a SemAn, as it clearly did in the case of *asse*t in Sub-sections 4.3 and 4.4. In the case of *harm*, Sub-section 4.2 showed that there were many Meaning Postulates that played a role in eliminating/reducing some of the terms occurring in the definition, which the SemAn Analyser treats as primitive. So here the manual SemAn achieved results which the SemAn Analyser could not obtain. (Also, we observed in Sub-section 3.3 that the current implementation of the SemAn Analyser does not quite do all we wish it to do.) Third parties involved in terminology work have indicated to us that they find it helpful.

Correspondence Address

The Corresponding Author is Peter Bernard Ladkin, Causalis Ing.-GmbH, Bielefeld, Germany; e-mail: Ladkin@causalis.com.

Acknowledgments

The SemAn method was developed by the first author in the project Harbsafe, financed by (as it then was) the German Federal Ministry for Economic Affairs and Energy, No. 03TNG006A-B in the Wipano programme, awarded to the Technical University of Braunschweig (TU-BS), Institut IVA, and DKE (the Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE), which is a German electrotechnical standardisation organisation, in 2017—2019.

The SemAn Analyser was developed by Causalis Ingenieurgesellschaft mbH as subcontractor to TU-BS, Institut IVA (then to become Institut IITL) in the project Harbsafe II, Nos. 03TN0018A-C, granted to TU-BS, DKE and INOSOFT AG, financed by the German Federal Ministry for Economic Affairs and Climate Action, in 2020—2022, also in the Wipano programme.

References

Begriffschrift. (2023). In *Wikipedia*. https://en.wikipedia.org/wiki/Begriffsschrift. Accessed 13th January 2023.

ExplosionAI. (n.d.). spaCy DependencyParser. https://spacy.io/api/dependencyparser. Accessed 13th January 2023.

Frege G. (1879). *Begriffsschrift: eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. Halle an der Saale: Verlag von Louis Nebert.

Goldrei D. (2005). *Proposition and Predicate Calculus: A Model of Argument*. Springer-Verlag, London.

IEC. (2023). *Standards Management Board – Joint Task Force on the Concept of Risk and Associated Terms*. International Electrotechnical Commission. Overview available from https://www.iec.ch/dyn/www/f?p=103:85:702664603091386::::FSP_ORG_ID,FSP_LANG_ID:28611,25. Accessed 13th January 2023.

IEC 61508-4:2010. *Functional Safety of Electrical/electronic/programmable electronic Safety-related Systems– Part 4: Definitions and abbreviations*. IEC 61508-4, Edition 2. International Electrotechnical Commission. Geneva. 2010.

IEC TS 62443-1-1:2009. *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. IEC TS 62443-1-1, Edition 1. International Electrotechnical Commission. Geneva. 2009.

IEC 62443-2-1:2010. *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*. IEC 62443-2-1, Edition 1. International Electrotechnical Commission. Geneva. 2010

IEC 62443-2-4:2015+AMD1:2017. *Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*. IEC 62443-2-4, Edition 1.1. International Electrotechnical Commission. Geneva. 2017.

IEC 62443-3-1:2009. *Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*. IEC 62443-3-1, Edition 1. International Electrotechnical Commission. Geneva. 2009.

IEC 62443-3-2:2020. *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*. IEC 62443-3-2, Edition 1. International Electrotechnical Commission. Geneva. 2020.

IEC 62443-3-3:2013. *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*. IEC 62443-3-3, Edition 1.0. International Electrotechnical Commission. Geneva. 2013.

IEC TR 63069:2019. *Industrial-process measurement, control and automation - Framework for functional safety and security*. IEC TR 63069, Edition 1. International Electrotechnical Commission. Geneva. 2019.

IEC Guide 120. *Security aspects - Guidelines for their inclusion in publications*. IEC Guide 120, Edition 1. International Electrotechnical Commission. Geneva. 2018

ISO/IEC Guide 51. *Safety aspects – Guidelines for their inclusion in standards*. ISO/IEC Guide 51, Edition 3. International Organization for Standardization and International Electrotechnical Commission. Geneva. 2014.

Janssen T. M. V. (2011). *Montague Semantics*. In Stanford Encyclopedia of Philosophy. 2011, revised 2021. Available from https://plato.stanford.edu/entries/montague-semantics/. Accessed 13th January 2023.

Jurafsky D, and Martin J. H. (2023). *Speech and Natural Language Processing, Chapter 14: Dependency Parsing*. Preprint draft of January 7, 2023. Available from https://web.stanford.edu/~jurafsky/slp3/14.pdf. Accessed 13th January 2023.

Ladkin P. B. (2020). *Robustness of Software*. In Digital Evidence and Electronic Signature Law Review, Vol. 17. Available from https://journals.sas.ac.uk/deeslr/article/view/5171. Accessed 13th January 2023.

Ladkin P. B. (2022). *Some Principles of Conceptual Analysis for Electrotechnical Terminology (ConcAn)*. Submitted for publication, 2022. {**Editor's Note:** It is hoped that this paper can be published in Volume 2, Issue 2, of this Journal}

Lamport L. (2003). *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*. Addison-Wesley

Kratzer A. (2007). *Situations in Natural Language Semantics*. In Stanford Encyclopedia of Philosophy. 2007, revised 2021. Available from https://plato.stanford.edu/entries/situations-semantics/. Accessed 13th January 2023.

Kripke S. A. (1982). *Wittgenstein on Rules and Private Language: An Elementary Exposition*. Wiley Blackwell

Mason S. (2015). *Case Transcript: England & Wales - Regina v Seema Misra, T20090070 - Commentary and Index to the transcript by Stephen Mason*. In Digital Evidence and Electronic Signature Law Review, Vol. 12. Available from https://journals.sas.ac.uk/deeslr/issue/view/328. . Accessed 13th January 2023.

Moltmann F. (2022). *Natural Language Ontology*. In Stanford Encyclopedia of Philosophy. Available from https://plato.stanford.edu/entries/natural-language-ontology/. Accessed 13th January 2023.

Montague R. (1974). *Formal Philosophy: Selected Papers of Richard Montague* (Ed. H. Richmond H. Thomason). Yale University Press 1974.

Safety-Critical Systems Club. (2023). *SCSC — Group: Ontology Working Group*. https://scsc.uk/go. Accessed 13th January 2023.

Wittgenstein L. (1967). *Philosophical Investigations* (G. E. M. Anscombe, Trans.). Basil Blackwell, Third Edition. (Original work written 1953).

This collation page left blank intentionally.

Appendix A. Multiply-Defined Concepts: Diff. Notes

A.1 Introduction

This document presents a list of concepts in the IEC functional safety and cybersecurity standards listed in the main body of the paper. Amongst the 450+ concepts defined in those documents; these are the concepts which have multiple definitions.

The list of multiply-defined concepts was developed in 2018 in Project Harbsafe (see the Acknowledgments section above), and has been reformatted for this paper.

A.2 Summary

Identical definitions	22
Minor difference (including syntactic)	11
Moderate difference	7
Substantial difference	21
Unknown (one is reference)	2
Total	63

Notes to Summary

- where there are different classes of difference within the definitions of one term, the highest difference category is assigned to the term
- "*availability*" occurs in two syntactic variants, counted here as one
- "*authenticate/authentication*" occurs as verb and noun, counted as one
- "*configuration baseline*" only occurs once — an error in the MultDefConcepts list
- there are five different versions of "*integrity*", counted as one
- "*non-repudiation*" is spelled multiple ways, counted as one
- "*risk tolerance*" and "*risk tolerance level*" are counted as one…

A.3 List of Multiply-defined Concepts

Table 1 ~ List of Multiply-defined Concepts

Concept	Sources	Remarks
access control	IEC 62443-1-1 IEC 62443-3-1	minor difference labelled enumeration (-3-1), or not

Concept	Sources	Remarks
accountability	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1	identical
application	IEC 61508-4 IEC 62443-1-1	substantial difference IEC 61508-4: referring to system: EUC IEC 62443-1-1: specialist meaning for SW
asset	IEC 62443-1-1 IEC 62443-2-1 IEC 62443-3-3	Identical includes ownership/custody and subject (organisation) moderate difference no ownership; subject IACS
asset owner	IEC 62443-2-4+AMD IEC 62443-3-3	moderate difference IEC 62443-2-4+AMD: subject: organization IEC 62443-3-3: subject: company
attack	IEC 62443-1-1 IEC Guide 120 IEC 62443-3-3	identical definition + paraphrase (in “i.e.” clause) minor difference definition only, no paraphrase
authenticate	IEC 62443-1-1	difference from noun verb: concrete action: verify
authentication	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1 IEC 62443-3-3	identical noun: measure designed to verify (different objects) substantial difference noun: abstractly formulated action: assurance
authorization	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1	identical
availability availability (performance)	IEC Guide 120 IEC62443-3-3 IEC 62443-3-1 IEC 62443-1-1	moderate difference no subject of property substantial difference probability, circumscribed in time, qualified substantial difference that of which the probability (above) is assessed

Concept	Sources	Remarks
channel	IEC 61508-4 IEC 62443-1-1	substantial difference IEC 61508-4: independent implementation of safety function IEC 62443-1-1: link in a conduit
ciphertext	IEC 62443-1-1 IEC 62443-3-1	minor (syntactic) difference
client	IEC 62443-1-1 IEC 62443-3-1	identical
conduit	IEC 62443-1-1 IEC 62443-3-3	moderate difference IEC 62443-1-1: for channels, common secreqs IEC 62443-3-3: for assets, protection
confidentiality	IEC 62443-1-1 IEC 62443-3-1 IEC Guide 120 IEC 62443-3-3	identical moderate difference essentially semantically equivalent, negative formulation substantial difference positive formulation as restrictions
configuration baseline	IEC 61508-4	only defined once
consequence	IEC 62443-2-1 IEC 62443-3-3	substantial difference IEC 62443-2-1: abstract, subject “incident” IEC 62443-3-3: condition or state, subject “event”
control system	IEC 62443-2-4+AMD IEC 62443-3-3	substantial difference IEC 62443-2-4+AMD: also that “used in design” IEC 62443-3-3: HW & SW of an IACS
countermeasure	IEC 62443-1-1 IEC 62443-3-3	identical
decryption	IEC 62443-1-1 IEC 62443-3-1	identical
defence in depth	IEC 62443-1-1 IEC 62443-3-1	substantial difference IEC 62443-1-1: usual: layers IEC 62443-3-1: architecture, abstract

Concept	Sources	Remarks
demilitarized zone	IEC 62443-1-1 IEC 62443-3-3	substantial difference IEC 62443-1-1: usual internal vs. external IEC 62433-3-3: generalised: between zones (ambiguity “zone”)
denial of service	IEC 62443-1-1 IEC 62443-3-1	identical
digital signature	IEC 62443-1-1 IEC 62443-3-1	identical
encryption	IEC 62443-1-1 IEC 62443-3-1	identical
environment	IEC 61508-4 IEC 62443-3-3	substantial difference IEC 61508-4: abstract: parameters IEC 62443-3-3: surrounding entities & circumstances
equipment under control	IEC 61508-4 IEC 62443-1-1	identical
harm	IEC Guide 120 ISO/IEC Guide 51 IEC 61508-4	identical minor difference
hazard	IEC 61508-4 ISO/IEC Guide 51	identical
hazardous event	IEC 61508-4 ISO/IEC Guide 51	minor difference semantically equivalent
hazardous situation	IEC 61508-4 ISO/IEC Guide 51	identical
incident	IEC 62443-2-1 IEC 62443-3-3	minor difference punctuation
industrial automation and control system	IEC 62443-1-1 IEC 62443-2-4+AMD IEC 62443-3-3	moderate differences all collections … that … IEC62443-1-1: of personnel, HW, SW IEC 62443-3-3: of personnel, HW, SW, policies IEC 62443-2-4+AMD: of personnel, HW, SW, policies, procedures

Concept	Sources	Remarks
integrity	IEC 62443-1-1 IEC 62443-3-1	identical
	IEC 62443-3-3 IEC Guide 120	moderate differences (changed to substantial) various concepts of “integrity” dealt with elsewhere
– software safety integrity	IEC 61508-4	substantial differences
– software safety integrity level	IEC 61508-4	substantial differences
– safety integrity	IEC 61508-4	substantial differences
– safety integrity level	IEC 61508-4 IEC 62443-1-1	moderate differences, also different from above
interception	IEC 62443-1-1 IEC 62443-3-1	minor difference IEC 62443-1-1: synonym also given — otherwise identical
interface	IEC 62443-1-1 IEC 62443-3-1	identical
local area network	IEC 62443-1-1 IEC 62443-3-1	identical
non-repudiation	IEC 62443-3-3 IEC Guide 120	identical
	IEC 62443-1-1 IEC 62443-3-1	identical, but substantially different from above heterographs IEC 62443-3-3/Guide 120: positive formulation: prove IEC 62443-1-1/3-1: service providing protection against...
plaintext	IEC 62443-1-1 IEC 62443-3-1	identical
product supplier	IEC 62443-2-4+AMD IEC 62443-3-3	identical
reasonably foreseeable misuse	IEC 61508-4 ISO/IEC Guide 51	identical

Concept	Sources	Remarks
remote access	IEC 62443-1-1 IEC 62443-2-1 IEC 62443-2-4+AMD IEC 62443-3-3	substantial differences IEC 62443-1-1: zone + “different geog. location” + rights IEC 62443-2-1: “perimeter” rather than “zone” IEC 62443-2-4+AMD: access through external interface (usual) IEC 62443-3-3: zone + “perimeter”
repudiation	IEC 62443-1-1 IEC 62443-3-1	identical
residual risk	IEC 61508-4 ISO/IEC /Guide 51 IEC 62443-1-1	minor differences IEC 61508-4: “protective measures” Guide 51: “risk reduction measures (protective measures)” IEC 62443-1-1: “security controls or countermeasures: specific to sec. risk
risk	IEC 61508-4 ISO/IEC Guide 51 IEC Guide 120 IEC 62443-1-1/3-1	identical identical, but substantial difference from above IEC 61508-4, etc.: combination of probability with severity IEC 62443-1-1, etc: expectation of loss, restricted to “vulnerability”
risk assessment	ISO/IEC Guide 51 IEC 62443-1-1 IEC 62443-2-1	substantial differences IEC Guide 51: risk analysis + risk evaluation IEC 62443-1-1: description of process, restricted to “vulnerabilities” IEC 62443-2-1: description of process, no restriction
risk tolerance /level	IEC 62443-1-1 IEC 62443-2-1	substantial difference (change 2018-12-27: minor difference) IEC 62443-1-1: term “level”, else semantically equivalent

Concept	Sources	Remarks
safety	IEC 61508-4 IEC 62443-1-1 ISO/IEC Guide 51 IEC Guide 120	identical identical but minor difference from above semantically equivalent if "unacceptable" = "not tolerable
safety instrumented system	IEC 62443-2-4+AMD IEC 62443-3-3	substantial difference IEC 62443-2-4+AMD: system used to implement FS IEC 62443-3-3: system used to implement SFs
security	IEC Guide 120 IEC 62443-1-1	substantial difference IEC Guide 120: protection ensuring inviolability IEC 62443-1-1: enumerated listing of features
security incident	IEC 62443-1-1 IEC 62443-2-4+AMD	substantial difference IEC 62443-1-1: "adverse" event or a threat of occurrence IEC 62443-2-4+AMD: compromise or attempt of significance to asset owner
security level	IEC 62443-1-1 IEC 62443-3-3	substantial difference IEC 62443-1-1: required effectiveness of countermeasures and properties IEC 62443-3-3: measure of confidence of vulnerability-freeness
security program	IEC 62443-1-1 IEC 62443-2-4+AMD	substantial difference IEC 62443-1-1: combination of all aspects of secmanagement IEC 62443-2-4+AMD: portfolio of secservices applicable to IACS
security services	IEC 62443-1-1 IEC 62443-3-1 IEC Guide 120	identical
server	IEC 62443-1-1 IEC 62443-3-1	identical
service provider	IEC 62443-2-4+AMD IEC 62443-3-3	moderate difference IEC 62443-2-4+AMD: organisation that has agreed to provide service IEC 62443-3-3: individual or organisation providing support

Concept	Sources	Remarks
sniffing	IEC 62443-1-1 IEC 62443-3-1	minor difference IEC 62443-1-1: a reference to another entry
spoof	IEC 62443-1-1 IEC 62443-3-1	identical
system	IEC 62443-1-1 IEC 62443-2-4+AMD	identical
system software	IEC 62443-1-1 IEC 62443-3-1 IEC 61508-4	Identical SW to facilitate ops and maintenance moderate difference from above SW relates to functioning of device itself or its services
threat	IEC 62443-1-1 IEC Guide 120 IEC 62443-3-1 IEC 62443-3-3	identical potential for violation of security moderate difference, also to above IEC 62443-3-1: potentially damaging action or capability IEC 62443-3-3: potentially circumstance/event adversely affecting operations
tolerable risk	IEC 61508-4 ISO/IEC Guide 51	minor difference IEC Guide 51: “level of ...”
vulnerability	IEC 62443-1-1 IEC 62443-2-4+AMD IEC 62443-3-1 IEC Guide 120	identical
wide area network	IEC 62443-1-1 IEC 62443-3-1	minor differences IEC 62443-1-1: “to connect computers, networks or other devices...” IEC 62443-3-1: “to connect computers...”
zone	IEC 62443-1-1 IEC 62443-3-3	minor difference? IEC 62443-1-1: a reference to another subclause

Appendix B. SemAn Analyser Output on Multiply-Defined Concepts

B.1 Introduction

The SemAn Analyser results below were developed in 2021-2 by TU-BS and Causalis Ing.-GmbH in Project Harbsafe II (see the Acknowledgments section above).

B.2 SemAn Analyser Results

```
1. (no definition)

2.
access control(a):

a) protection of system resources against unauthorized access

\\
     a) protection
          > of system resources
                 > against unauthorized access
[Source: IEC TR 62443-3-1:2009]

3.
access control(b):

b) process by which use of system resources is regulated according to a security
policy and is permitted only by authorized entities according to that policy

\\
     b) process
          > by which use
                 > of system resources
                 > [AND] is regulated according to a security policy
                 > [AND] and is permitted only by authorized entities
                           > according to that policy
[Source: IEC TR 62443-3-1:2009]

4.
access control:

protection of system resources against unauthorized access;

a process by which use of system resources is regulated according to a security
policy and is permitted by only authorized entities according to that policy

\\
     protection
          > of system resources
                > against unauthorized access
     ;

     a process
          > by which use
                 > of system resources
```

```
                > [AND] is regulated according to a security policy
                > [AND] and is permitted only by authorized entities
                                    > according to that policy
[Source: IEC TS 62443-1-1:2009]

5.
accountability:

property of a system that ensures that the actions of a system entity may be
traced uniquely to that entity, which can be held responsible for its actions

\\
     property
          > [AND] of a system
          > [AND] that ensures that the actions
                       > [AND] of a system entity
                       > [AND] may be traced uniquely to that entity
                                    > , which can be held responsible for its
actions
[Source: IEC Draft Guide 120]
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

8.
application:

task related to the EUC rather than to the E/E/PE system

\\
     task
          > [AND] related to the EUC
          > [AND] rather than to the E/E/PE system
[Source: IEC 61508-4:2010]

9.
application:

software program that performs specific functions initiated by a user command or
a process event and that can be executed without access to system control,
monitoring, or administrative privileges

\\
      software program
          > [AND] that performs specific functions
                       > initiated by a |[OR] user command
                                       |[OR] or a process event

          > [AND] and that can be executed without access
                       > to | [OR] system control
                            | [OR] , monitoring
                            | [OR] , or administrative privileges
[Source: IEC TS 62443-1-1:2009]

10.
asset:

physical or logical object owned by or under the custodial duties of an
organization, having either a perceived or actual value to the organization

\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]
```

```
11.
asset:

physical or logical object having either a perceived or actual value to the IACS

\\
     physical or logical object
          > having either a perceived or actual value
                > to the IACS
[Source: IEC 62443-3-3:2013]

13.
asset owner:

individual or company responsible for one or more IACS

\\
     [OR] individual
     [OR] or company
               > responsible for
                     > one or more IACS
[Source: IEC 62443-3-3:2013]

14.
asset owner:

individual or organization responsible for one or more IACSs

\\
     [OR] individual
     [OR] or organization
               > responsible for
                     > one or more IACS
[Source: IEC 62443-2-4:2015+AMD1:2017]

15.
attack:

assault on a system that derives from an intelligent threat

\\
     assault
          > [AND] on a system
          > [AND] that derives from an intelligent threat
[Source: IEC 62443-3-3:2013]

16.
attack:

assault on a system that derives from an intelligent threat – i.e., an
intelligent act that is a deliberate attempt (especially in the sense of a method
or technique) to evade security services and violate the security policy of a
system

\\
     assault
          > [AND] on a system
          > [AND] that derives from an intelligent threat
     – i.e.
     , an intelligent act
          > that is a deliberate attempt
                > [AND] to evade security services
                > [AND] and violate the security policy
                           > of a system
[Source: IEC Draft Guide 120]
[Source: IEC TS 62443-1-1:2009]
```

```
18.
Authenticate

verify the identity of a user, user device, or other entity, or the integrity of
data stored, transmitted, or otherwise exposed to unauthorized modification in an
information system, or to establish the validity of a transmission

\\
     [OR] verify the identity
               > of | [OR] a user
                    | [OR] , user device
                    | [OR] , or other entity
     [OR] , or the integrity
               > of data
                     > stored, transmitted, or otherwise exposed to unauthorized
modification
                               > in an information system
     [OR] , or to establish the validity
               > of a transmission
[Source: IEC TS 62443-1-1:2009]

19.
authentication:

security measure designed to establish the validity of a transmission, message or
originator or a means of verifying an individual’s authorization to receive
specific categories of information

\\
     security measure
          > designed to establish the | [OR] validity
                                      |           > of a | [OR] transmission
                                      |                  | [OR] , message
                                      |                  | [OR] , or originator
                                      | [OR] or a means
                                      |           > of verifying an individual’s
authorization
                                      |                  > to receive specific
categories
                                      |                        > of information
[Source: IEC 62443-2-1:2010]

20.
authentication:

provision of assurance that a claimed characteristic of an identity is correct

\\
     provision
          > of assurance
                 > that a claimed characteristic
                        > [AND] of an identity
                        > [AND] is correct

[Source: IEC 62443-3-3:2013]

21.
authentication:

security measure designed to establish the validity of a transmission, message,
or originator, or a means of verifying an individual's authorization to receive
specific categories of information

\\
     security measure
          > designed to establish the | [OR] validity
                                      |           > of a | [OR] transmission
                                      |                  | [OR] , message
```

```
                                        |                  | [OR] , or originator
                                        | [OR] , or a means
                                        |           > of verifying an individuals
authorization
                                        |                  > to receive specific
categories
                                        |                        > of information
[Source: IEC Draft Guide 120]
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

24.
authorization:

right or permission that is granted to a system entity to access a system
resource

\\
      [OR] right
      [OR] or permission
                > [AND] that is granted to a system entity
                > [AND] to access a system resource
[Source: IEC Draft Guide 120]
[Source: IEC TS 62443-1-1:2009]

25.
authorization:

right or a permission that is granted to a system entity to access a system
resource

\\
      [OR] right
      [OR] or a permission
                > [AND] that is granted to a system entity
                > [AND] to access a system resource
[Source: IEC TR 62443-3-1:2009]

27.
availability:

property of ensuring timely and reliable access to and use of control system
information and functionality

\\
     property
          > of ensuring timely and reliable | [AND] access to
                                            | [AND] and use
                                            |            > of control system |
[AND] information
                                            |                               |
[AND] and functionality
[Source: IEC 62443-3-3:2013]

28.
availability:

property of being accessible and usable upon demand by an authorized entity

\\
     property
          > of being accessible and usable upon demand
                 > by an authorized entity
[Source: IEC Draft Guide 120]

29.
availability:
```

```
probability that an asset, under the combined influence of its reliability,
maintainability and security will be able to fulfil its required function over a
stated period of time or at a given point in time

\\
     probability
          > that an asset
                 > [AND] , under the combined influence
                             > of its | [AND] reliability
                                      | [AND] , maintainability
                                      | [AND] and security
                 > [AND] will be able to fulfil its required function
                             > [OR] over a stated period
                                         > of time
                             > [OR] or at a given point
                                         > in time
[Source: IEC TR 62443-3-1:2009]

30.
availability:

ability of an item to be in a state to perform a required function under given
conditions at a given instant or over a given time interval, assuming that the
required external resources are provided

\\
     ability
          > [AND] of an item
                        > to be in a state
          > [AND] to perform a required function
                        > under given conditions
                               > [OR] at a given instant
                               > [OR] or over a given time interval
                               > [AND] , assuming that the required external
resources
                                                  > are provided
[Source: IEC TS 62443-1-1:2009]

31.
channel:

element or group of elements that independently implement an element safety
function

\\
     [OR] element
     [OR] or group
               > [AND] of elements
               > [AND] that independently implement
                           > an element safety function
[Source: IEC 61508-4:2010]

32.
channel:

specific communication link established within a communication conduit

\\
     specific communication link
          > established within a communication conduit
[Source: IEC TS 62443-1-1:2009]

33.
ciphertext:

data that have been transformed by encryption so that the semantic information
content is no longer intelligible or directly available
\\
```

```
     data
          > that have been transformed by encryption
                 > so that the semantic information content
                        > [OR] is no longer intelligible
                        > [OR] or directly available
[Source: IEC TR 62443-3-1:2009]

34.

ciphertext:

data that has been transformed by encryption so that its semantic information
content (i.e., its meaning) is no longer intelligible or directly available

\\
     data
          > that has been transformed by encryption
                 > so that the semantic information content
                        > [OR] is no longer intelligible
                        > [OR] or directly available

[Source: IEC TS 62443-1-1:2009]

35.
client:

device or application receiving or requesting services or information from a
server application

\\
     [OR] device
     [OR] or application
               > [OR] receiving or requesting services
               > [OR] or information
                           > from a server application
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

37.
conduit:

logical grouping of communication channels, connecting two or more zones, that
share common security requirements

\\
     logical grouping
          > of communication channels
                 > , connecting | [OR] two
                                | [OR] or more zones
                                |           > , that share common security
requirements
[Source: IEC 62443-3-3:2013]

38.
conduit:

logical grouping of communication assets that protects the security of the
channels it contains

\\
     logical grouping
          > [AND] of communication assets
          > [AND] that protects the security
                        > of the channels
                              > it contains
[Source: IEC TS 62443-1-1:2009]
```

```
39.
confidentiality:

preserving authorized restrictions on information access and disclosure,
including means for protecting personal privacy and proprietary information

\\
     preserving authorized restrictions
          > on | [AND] information access
               | [AND] and disclosure
               |            > , including means
               |                  > for protecting | [AND] personal privacy
               |                                  | [AND] and proprietary
information
[Source: IEC 62443-3-3:2013]

40.
confidentiality:

property that information is not made available or disclosed to unauthorized
individuals, entities, or processes

\\
     property
          > [AND] that information
          > [AND] is not | [OR] made available
                         | [OR] or disclosed to unauthorized | [OR] individuals
                         |                                   | [OR] , entities
                         |                                   | [OR] , or
processes
[Source: IEC Draft Guide 120]

41.
confidentiality:

assurance that information is not disclosed to unauthorized individuals,
processes or devices
\\
     assurance
          > that information
                 > is not disclosed to unauthorized | [OR] individuals
                                                    | [OR] , processes
                                                    | [OR] or devices
[Source: IEC TR 62443-3-1:2009]

42.
confidentiality:

assurance that information is not disclosed to unauthorized individuals,
processes or devices
\\
     assurance
          > that information
                 > is not disclosed to unauthorized | [OR] individuals
                                                    | [OR] , processes
                                                    | [OR] ,or devices
[Source: IEC TS 62443-1-1:2009]

43.

configuration baseline:

information that allows the software release to be recreated in an auditable and
systematic way, including: all source code, data, run time files, documentation,
configuration files, and installation scripts that comprise a software release;

information about compilers, operating systems, and development tools used to
create the software release
```

```
\\
     information
          > that allows the software release
                 > [AND] to be recreated in an auditable and systematic way
                 > [AND] , including: all | [AND] source code
                                          | [AND] data
                                          | [AND] run time files
                                          | [AND] , documentation
                                          | [AND] , configuration files
                                          | [AND] , and installation scripts
                                          |           > that comprise a software
release
; information about compilers
     > [AND], operating systems
     > [AND], and development tools
                    > used to create the software release
[Source: IEC 61508-4:2010]

44.
consequence:

result that occurs from a particular incident

\\
     result
          > that occurs from a particular incident
[Source: IEC 62443-2-1:2010]

45.
consequence:

condition or state that logically or naturally follows from an event

\\
     [OR] condition
     [OR] or state
               > that logically or naturally follows from an event
[Source: IEC 62443-3-3:2013]

46.
control system:

hardware and software components of an IACS

\\
     hardware and software components
          > of an IACS
[Source: IEC 62443-3-3:2013]

47.
control system:

hardware and software components used in the design and implementation of an IACS

\\
     hardware and software components
          > used in the | [AND] design
                        | [AND] and implementation
                        |            > of an IACS
[Source: IEC 62443-2-4:2015 + AMD1:2017]

48.
countermeasure:

action, device, procedure, or technique that reduces a threat, a vulnerability,
or an attack by eliminating or preventing it, by minimizing the harm it can
cause, or by discovering and reporting it so that corrective action can be taken
```

```
\\
     [OR] action
     [OR] , device
     [OR] , procedure
     [OR] , or technique
               > [AND] that reduces | [OR] a threat
                                    | [OR] , a vulnerability
                                    | [OR] , or an attack
                                > [OR] by eliminating
                                > [OR] or preventing it
                                > [OR] , by minimizing the harm
                                                > it can cause,
                                > [OR] or by | [AND] discovering
                                             | [AND] and reporting it
               > [AND] so that corrective action
                                > can be taken
[Source: IEC 62443-3-3:2013]
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TS 62443-1-1:2009]
```

```
51.
decryption:

process of changing ciphertext into plaintext using a cryptographic algorithm and
key (see 3.1.24 “encryption”)

\\
     process
          > of changing ciphertext
                 > [AND] into plaintext
                 > [AND] using a | [AND] cryptographic algorithm
                                 | [AND] and key
[Source: IEC TR 62443-3-1:2009]
```

```
52.
decryption:

process of changing cipher text into plaintext using a cryptographic algorithm
and key

\\
     process
          > of changing cipher text
                 > [AND] into plaintext
                 > [AND] using a | [AND] cryptographic algorithm
                                 | [AND] and key
[Source: IEC TS 62443-1-1:2009]
```

```
53.
defense in depth:

security architecture based on the idea that any one point of protection may, and
probably will, be defeated

\\
     security architecture
          > based on the idea
                 > that any one point
                        > of protection
                              > may, and probably will, be defeated
[Source: IEC TR 62443-3-1:2009]
```

```
54.
defense in depth:

provision of multiple security protections, especially in layers, with the intent
to delay if not prevent an attack

\\
     provision
          > [AND] of multiple security protections
                    > ,especially in layers
          > [AND] , with the intent
                              > to delay if not prevent an attack
[Source: IEC TS 62443-1-1:2009]

55.
demilitarized zone:

common, limited network of servers joining two or more zones for the purpose of
controlling data flow between zones

\\
     common, limited network
          > [AND] of servers
          > [AND] joining two or more zones
                       > for the purpose
                              > of controlling data flow
                                     > between zones
[Source: IEC 62443-3-3:2013]

56.
demilitarized zone:

perimeter network segment that is logically inserted between internal and
external networks

\\
     perimeter network segment
          > that is logically inserted
                 > between | [AND] internal
                           | [AND] and external networks
[Source: IEC TS 62443-1-1:2009]

57.
denial of service:

prevention or interruption of authorized access to a system resource or the
delaying of system operations and functions

\\
     [OR] prevention
     [OR] or interruption
               > of authorized access
                      > to a system resource
     [OR] or the delaying
               > of system | [AND] operations
                           | [AND] and functions
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TR 62443-3-1:2009]

59.
digital signature:

result of a cryptographic transformation of data which, when properly
implemented, provides the services of origin authentication, data integrity, and
signer non-repudiation

\\
     result
```

```
          > of a cryptographic transformation
                > [AND] of data
                > [AND] which, when properly implemented, provides the services
                              > of | [AND] origin authentication
                                   | [AND] , data integrity
                                   | [AND] and signer non-repudiation
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

61.
encryption:

cryptographic transformation of plaintext into ciphertext that conceals the
data’s original meaning to prevent it from being known or used

\\
     cryptographic transformation
          > [AND] of plaintext
          > [AND] into ciphertext
          > [AND] that conceals the data’s original meaning
                        > to prevent it
                              > from being known or used
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

63.
environment:

all relevant parameters that can affect the achievement of functional safety in
the specific application under consideration and in any safety lifecycle phase

\\
     all relevant parameters
          > that can affect the achievement
                > of functional safety
                      > in the specific | [AND] application
                                        |            > under consideration
                                        | [AND] and in any safety lifecycle
phase
[Source: IEC 61508-4:2010]

64.
environment:

surrounding objects, region or circumstances which may influence the behavior of
the IACS and/or may be influenced by the IACS

\\
     surrounding | [OR] objects
                 | [OR] , region
                 | [OR] or circumstances
          > [OR] which may influence the behavior
                     > of the IACS
          > [OR] and/or may be influenced by the IACS
[Source: IEC 62443-3-3:2013]

65.
equipment under control:

equipment, machinery, apparatus or plant used for manufacturing, process,
transportation, medical or other activities

\\
     [OR] equipment
     [OR] , machinery
     [OR] , apparatus
     [OR] or plant
               > used for | [OR] manufacturing
```

```
                          | [OR] , process
                          | [OR] , transportation
                          | [OR] , medical or other activities
[Source: IEC TS 62443-1-1:2009]
[Source: IEC 61508-4:2010]

67.
harm:

physical injury or damage to the health of people or damage to property or the
environment

\\
     [OR] physical injury
     [OR] or damage
               > [OR] to the health
                           > of people
     [OR] or damage
               > [OR] to property
               > [OR] or the environment
[Source: IEC 61508-4:2010]

68.
harm:

injury or damage to the health of people, or damage to property or the
environment

\\
     [OR] injury
     [OR] or damage
               > to the health
                      > of people
     [OR] , or damage
               > to | [OR] property
                    | [OR] or the environment
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]



70.
hazard:

potential source of harm

\\
     potential source
          > of harm
[Source: IEC 61508-4:2010]
[Source: IEC Guide 51:2014]

72.
hazardous event:

event that may result in harm

\\
     event
          > that may result in harm
[Source: IEC 61508-4:2010]

73.
hazardous event

event that can cause harm

\\
```

```
     event
          > that can cause harm
```

[Source: IEC Guide 51:2014]

74.
hazardous situation:

circumstance in which people, property or the environment are exposed to one or more hazards

```
\\
     circumstance
          > in which | [OR] people
                     | [OR] , property
                     | [OR] or the environment
                     |           > are exposed to one or more hazards
```

[Source: IEC 61508-4:2010]
[Source: IEC Guide 51:2014]

76.
incident: correct except for the splitting

event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

```
\\
     event
          > [AND] that is not part
                       > of the expected operation
                              > of a | [OR] system
                                     | [OR] or service
          > [AND] that causes or may cause,
                       > [OR] an interruption to,
                       > [OR] or a reduction in,
                                   > the quality
                                          > of the service
                                                 > provided by the system
```

[Source: IEC 62443-2-1:2010]

77.
incident:

event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

```
\\
     event
          > [AND] that is not part
                       > of the expected operation
                              > of a | [OR] system
                                     | [OR] or service
          > [AND] that causes, or may cause,
                       > [OR] an interruption to,
                       > [OR] or a reduction in,
                                   > the quality
                                          > of the service
                                                 > provided by the control system
```

[Source: IEC 62443-3-3:2013]

78.
industrial automation and control system:

collection of personnel, hardware, software and policies involved in the

```
operation of the industrial process and that can affect or influence its safe,
secure and reliable operation

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , software
                     | [AND] and policies
          > [AND] involved in the operation
                       > of the industrial process
          > [AND] and that can | [OR] affect
                               | [OR] or influence its | [AND] safe,
                               |                       | [AND] secure
                               |                       | [AND] and reliable
operation
[Source: IEC 62443-3-3:2013]

79.
industrial automation and control system:

collection of personnel, hardware, software, procedures and policies involved in
the operation of the industrial process and that can affect or influence its
safe, secure and reliable operation

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , software
                     | [AND] , procedures
                     | [AND] and policies
          > [AND] involved in the operation
                       > of the industrial process
          > [AND] and that can | [OR] affect
                               | [OR] or influence its | [AND] safe,
                               |                       | [AND] secure
                               |                       | [AND] and reliable
operation
[Source: IEC 62443-2-4:2015 + AMD1:2017]

80.
industrial automation and control system:

collection of personnel, hardware, and software that can affect or influence the
safe, secure, and reliable operation of an industrial process

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , and software
          > [AND] that can | [OR] affect
                           | [OR] or influence the | [AND] safe,
                           |                       | [AND] secure,
                           |                       | [AND] and reliable operation
                           |                       |           > of an
industrial process
[Source: IEC TS 62443-1-1:2009]


81.
integrity:

property of protecting the accuracy and completeness of assets

\\
     property
```

```
          > of protecting the | [AND] accuracy
                              | [AND] and completeness
                              |           > of assets
```

[Source: IEC 62443-3-3:2013]

82.
integrity:

property of accuracy and completeness

```
\\
     property
          > of | [AND] accuracy
               | [AND] and completeness
```

[Source: IEC Draft Guide 120]

83.
integrity:

quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

```
\\
     quality
          > [AND] of a system
          > [AND] reflecting the | [AND] logical correctness
                                 | [AND] and reliability
                                 |            > of the operating system
                                 | [AND] , the logical completeness
                                 |              > of the | [AND] hardware
                                 |                       | [AND] and software
                                 |                       |           >
implementing the protection mechanisms
                                 | [AND] , and the consistency
                                 |            > of the | [AND] data structures
                                 |                     | [AND] and occurrence
                                 |                     |            > of the
stored data
```

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

85.
interception:

capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission and other communication attributes

```
\\
     [OR] [AND] capture
          [AND] and disclosure
                     > of message contents
     [OR] or use
               > of traffic analysis
                     > [AND] to compromise the confidentiality
                                  > of a communication system
                     > [AND] based on | [OR] message destination
                                      | [OR] or origin
                                      | [OR] , frequency
                                      | [OR] or length
                                      |           > of transmission
                                      | [OR] and other communication attributes
```

[Source: IEC TR 62443-3-1:2009]

86.

interception:

sniffing, capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes

\\
[AND] sniffing
[AND] capture
[AND] and disclosure
> of message contents
[OR] or use
> of traffic analysis
> [AND] to compromise the confidentiality
> of a communication system
> [AND] based on | [OR] message destination
| [OR] or origin
| [OR] , frequency
| [OR] , and other communication attributes
| [OR] or length
| > of transmission
[Source: IEC TS 62443-1-1:2009]

87.
interface:

logical entry or exit point that provides access to the module for logical information flows

\\
[OR] logical entry
[OR] or exit point
> that provides access
> [AND] to the module
> [AND] for logical information flows
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

89.
local area network:

communications network designed to connect computers and other intelligent devices in a limited geographic area

\\
communications network
> designed to connect | [AND] computers
| [AND] and other intelligent devices
> in a limited geographic area
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TR 62443-3-1:2009]

91.
non repudiation:

ability to prove the occurrence of a claimed event or action and its originating entities

\\
ability
> to prove the | [AND] occurrence
| > of a claimed | [OR] event
| | [OR] or action
| [AND] and its originating entities
[Source: IEC Draft Guide 120]

```
[Source: IEC 62443-3-3:2013]


93.
non repudiation:

security service that provides protection against false denial of involvement in
a communication

\\
     security service
          > that provides protection
                 > against false denial
                        > of involvement
                               > in a communication
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

95.
plaintext:

unencoded data that is input to and transformed by an encryption process or that
is output by a decryption process

\\
     unencoded data
          > [OR] that is input to and transformed
                        > by an encryption process
          > [OR] or that is output
                        > by a decryption process
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

97.
product supplier:

manufacturer of hardware and/or software product

\\
     manufacturer
          > of | [OR] hardware
               | [OR] and/or software product

[Source: IEC 62443-3-3:2013]
[Source: IEC 62443-2-4:2015 + AMD1:2017]

99.
reasonably foreseeable misuse:

use of a product, process or service in a way not intended by the supplier, but
which may result from readily predictable human behaviour

\\
     use
          > [AND] of a | [OR] product
                       | [OR] , process
                       | [OR] or service
          > [AND] in a way
                       > [AND] not intended by the supplier
                       > [AND] , but which may result from readily predictable
human behaviour
[Source: IEC 61508-4:2010]


100.
reasonably foreseeable misuse:

use of a product or system in a way not intended by the supplier, but which can
```

```
result from readily predictable human behaviour

\\
     use
          > [AND] of a | [OR] product
                       | [OR] or service
          > [AND] in a way
                       > [AND] not intended by the supplier
                       > [AND] , but which may result from readily predictable
human behaviour
[Source: IEC Guide 51:2014]

101.
remote access:

communication with, or use of, assets or systems within a defined perimeter from
any location outside that perimeter

\\
     [OR] communication with,
     [OR] or use of, | [OR] assets
                     | [OR] or systems
                     |           > [AND] within a defined perimeter
                     |           > [AND] from any location
                     |                       > outside that perimeter
[Source: IEC 62443-2-1:2010]

102.
remote access:

access to a control system by any user communicating from outside the perimeter
of the zone being addressed

\\
     access
          > to a control system
                 > by any user
                        > communicating from
                               > outside the perimeter
                                      > of the zone
                                             > being addressed
[Source: IEC 62443-3-3:2013]

103.
remote access:

access to a control system through an external interface of the control system

\\
     access
          > to a control system
                 > through an external interface
                        > of the control system
[Source: IEC 62443-2-4:2015 + AMD1:2017]

104.
remote access:

use of systems that are inside the perimeter of the security zone being addressed
from a different geographical location with the same rights as when physically
present at the location

\\
     use
          > of systems
                 > [AND] that are inside the perimeter
                              > of the security zone
                 > [AND] being addressed from a different geographical location
```

```
                              > with the same rights
                                    > as when physically present at the location
[Source: IEC TS 62443-1-1:2009]

105.
repudiation:

denial by one of the entities involved in a communication of having participated
in all or part of the communication

\\
     denial
          > [AND] by one of the entities
                       > involved in a communication
          > [AND] of having participated in | [OR] all
                                           | [OR] or part
                                           |           > of the communication
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

107.
residual risk:

risk remaining after protective measures have been taken

\\
     risk
          > remaining after protective measures
                 > have been taken
[Source: IEC 61508-4:2010]

108.
residual risk:

risk remaining after risk reduction measures have been implemented

\\
     risk
          > remaining after risk reduction measures
                 > have been implemented
[Source: IEC Guide 51:2014]

109.
residual risk

remaining risk after the security controls or countermeasures have been applied

\\
     remaining risk
          > after the | [OR] security controls
                      | [OR] or countermeasures
                      |           > have been applied
[Source: IEC TS 62443-1-1:2009]


110.
risk:

combination of the probability of occurrence of harm and the severity of that
harm

\\
     combination
          > of the | [AND] probability
                   |            > of occurrence
                   |                   > of harm
                   | [AND] and the severity
                   |            > of that harm
```

```
[Source: IEC 61508-4:2010]
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]


113.
risk:

expectation of loss expressed as the probability that a particular threat will
exploit a particular vulnerability with a particular consequence

\\
     expectation
          > of loss
                 > expressed as the probability
                        > that a particular threat
                               > will exploit a particular vulnerability
                                      > with a particular consequence
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

115.
risk assessment:

process of identifying and evaluating risks to the organization’s operations, the
organization’s assets or individuals by determining the likelihood of occurrence,
the resulting impact, and additional countermeasures that would mitigate this
impact

\\
     process
          > of identifying and evaluating risks
                 > [AND] to the | [OR] organization’s operations
                                | [OR] , the organization’s assets
                                | [OR] or individuals
                 > [AND] by determining | [AND] the likelihood
                                        |            > of occurrence
                                        | [AND] , the resulting impact
                                        | [AND] , and additional countermeasures
                                        |            > that would mitigate this
impact
[Source: IEC 62443-2-1:2010]

116.
risk assessment:

overall process comprising a risk analysis and a risk evaluation

\\
     overall process
          > comprising a | [AND] risk analysis
                         | [AND] and a risk evaluation
[Source: IEC Guide 51:2014]

117.
risk assessment:

process that systematically identifies potential vulnerabilities to valuable
system resources and threats to those resources, quantifies loss exposures and
consequences based on probability of occurrence, and recommends how to allocate
resources to countermeasures to minimize total exposure

\\
     process
          > that systematically identifies potential | [AND] vulnerabilities
                                                     |            > to valuable
system resources
                                                     | [AND] and threats
```

```
                                                        |            > to those
resources
                                                        | [AND] , quantifies loss
exposures
                                                        | [AND] and consequences
                                                                   > based on
probability
                                                                        > of
occurrence
                                                        | [AND] , and recommends how
to allocate resources
                                                        |            > to
countermeasures
                                                        |            > to minimize
total exposure
[Source: IEC TS 62443-1-1:2009]


118.
risk tolerance:

risk the organization is willing to accept

\\
     risk
          > the organization
                > is willing to accept
[Source: IEC 62443-2-1:2010]



119.
risk tolerance level:

level of residual risk that is acceptable to an organization

\\
     level
          > of residual risk
                > that is acceptable to an organization
[Source: IEC TS 62443-1-1:2009]

120.
safety:

freedom from unacceptable risk

\\
     freedom
          > from unacceptable risk
[Source: IEC 61508-4:2010]
[Source: IEC TS 62443-1-1:2009]

121.
safety:

freedom from risk which is not tolerable

\\
     freedom
          > from risk
                > which is not tolerable
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]

124.
safety instrumented system:
```

system used to implement one or more safety-related functions

\\
     system
          > used to implement one or more safety-related functions
[Source: IEC 62443-3-3:2013]

125.
safety instrumented system:

system used to implement functional safety

\\
     system
          > used to implement functional safety
[Source: IEC 62443-2-4:2015 + AMD1:2017]

126.
safety integrity:

probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

\\
     probability of
          > an E/E/PE safety-related system
                 > satisfactorily performing the specified safety functions
                        > [AND] under all the stated conditions
                        > [AND] within a stated period
                                    > of time
[Source: IEC 61508-4:2010]

127.
safety integrity level:

discrete level for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems

\\
     discrete level
          > for specifying the safety integrity requirements
                 > of the safety-instrumented functions
                        > to be allocated to the safety-instrumented systems
[Source: IEC TS 62443-1-1:2009]

128.
safety integrity level:

discrete level, corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

\\
     discrete level
          > corresponding to a range
                 > of safety integrity values
                        > , where | [AND] safety integrity level 4
                                  | > has the highest level
                                  | > of safety integrity
                                  | [AND] and safety integrity level 1
                                  | > has the lowest
[Source: IEC 61508-4:2010]

129.
security:

a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

\\
     a condition
          > that results from the | [AND] establishment
                                  | [AND] and maintenance
                                  | > of protective measures
                                  | > that ensure a state
                                  | > of inviolability
                                  | > from | [OR] hostile acts
                                  | | [OR] or influences
[Source: IEC Draft Guide 120]

130.
security:

a) measures taken to protect a system

\\
     a) measures
          > taken to protect a system
[Source: IEC TS 62443-1-1:2009]

131.
security:

b) condition of a system that results from the establishment and maintenance of measures to protect the system

\\
     b) condition
          > [AND] of a system
          > [AND] that results from the | [AND] establishment
                                        | [AND] and maintenance
                                        | > of measures
                                        | > to protect the system
[Source: IEC TS 62443-1-1:2009]

132.
security:

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

\\
     c) condition
          > of system resources
                > being free from | [AND] unauthorized access
                                  | [AND] and from | [OR] unauthorized
                                  | | [OR] or accidental change
                                  | | [OR] , destruction
                                  | | [OR] , or loss
[Source: IEC TS 62443-1-1:2009]

133.
security:

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

\\
d) capability
> of a computer-based system
> [AND] to provide adequate confidence
> that unauthorized | [AND] persons
| [AND] and systems
| > can neither | [OR] modify the software
| | [OR] nor gain access
| | > to the | [AND] system functions
| | | [AND] and its data
> [AND] , and yet to ensure that this is not denied to authorized persons
[Source: IEC TS 62443-1-1:2009]

134.
security:

prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

\\
prevention
> [OR] of illegal or unwanted penetration of
> [OR] , or interference
> with the | [AND] proper
| [AND] and intended operation
| > of an industrial automation and control system
[Source: IEC TS 62443-1-1:2009]

135.
security incident:

security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

\\
[OR] security compromise
> that is of some significance
> to the asset owner
[OR] or failed attempt
> [AND] to compromise the system
> [AND] whose result
> could have been of some significance
> to the asset owner
[Source: IEC 62443-2-4:2015 + AMD1:2017]

136.
security incident:

adverse event in a system or network, or the threat of the occurrence of such an event

\\
[OR] adverse event
> in a | [OR] system
| [OR] or network

```
     [OR] , or the threat
               > of the occurrence
                     > of such an event
[Source: IEC TS 62443-1-1:2009]
```

```
137.
security level:

measure of confidence that the IACS is free from vulnerabilities and functions in
the intended manner

\\
     measure
          > of confidence
                 > that the IACS
                       > [AND] is free from vulnerabilities
                       > [AND] and functions in the intended manner
[Source: IEC 62443-3-3:2013]
```

```
138.
security level:

level corresponding to the required effectiveness of countermeasures and inherent
security properties of devices and systems for a zone or conduit based on
assessment of risk for the zone or conduit

\\
     level
          > [AND] corresponding to the | [AND] required effectiveness
                                       |            > of countermeasures
                                       | [AND] and inherent security properties
                                       |            > [AND] of devices
                                       |            > [AND] and systems
                                       |                        > for a | [OR]
zone
                                       |                                | [OR] or
conduit
          > [AND] based on assessment
                      > of risk
                           > for the zone
[Source: IEC TS 62443-1-1:2009]

139.
security program:

portfolio of security services, including integration services and maintenance
services, and their associated policies, procedures, and products that are
applicable to the IACS

\\
     portfolio
          > [AND] of security services
          > [AND], including | [AND] integration services
                             | [AND] and maintenance services
                             | [AND] , and their associated | [AND] policies
                             |                              | [AND] , procedures
                             |                              | [AND] , and
products
                             |                              |           > that
are applicable to the IACS
[Source: IEC 62443-2-4:2015 + AMD1:2017]


140.
security program:
```

```
combination of all aspects of managing security, ranging from the definition and
communication of policies through implementation of best industry practices,
ongoing operation and auditing

\\
     combination
          > of all aspects
                 > [AND] of managing security
                 > [AND], ranging from the | [AND] definition
                                           | [AND] and communication
                                           |           > of policies
                 > [AND] through | [AND] implementation
                                 |           > of best industry practices
                                 | [AND] , ongoing operation
                                 | [AND] and auditing
[Source: IEC TS 62443-1-1:2009]

141.
security services:

mechanisms used to provide confidentiality, data integrity, authentication, or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] , or no repudiation
                            |           > of information
[Source: IEC Draft Guide 120]



142.
security services:

mechanisms used to provide confidentiality, data integrity, authentication or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] or no repudiation
                            |           > of information
[Source: IEC TR 62443-3-1:2009]

143.
security services:

mechanisms used to provide confidentiality, data integrity, authentication or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] , or no repudiation
                            |             > of information
[Source: IEC TS 62443-1-1:2009]

144.
server:
```

```
device or application that provides information or services to client
applications and devices

\\
     [OR] device
     [OR] or application
               > that provides | [OR] information
                               | [OR] or services
                               |           > to | [OR] client applications
                               |                | [OR] and devices
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

146.
service provider:

organization that has agreed to undertake responsibility for providing a given
support service and obtaining, when specified, supplies in accordance with an
agreement

\\
     organization
          > that has agreed to undertake responsibility
                 | [AND] for providing a given support service
                 | [AND] and obtaining, when specified, supplies
                 |            > in accordance
                 |                  > with an agreement
[Source: IEC 62443-3-3:2013]


147.
service provider:

individual or organization that provides a specific support service and
associated supplies in accordance with an agreement with the asset owner

\\
     [OR] individual
     [OR] or organization
               > that provides a | [AND] specific support service
                                 | [AND] and associated supplies
                                 |            > in accordance
                                 |                  > with an agreement
                                 |                        > with the asset
owner
[Source: IEC 62443-2-4:2015 + AMD1:2017]


148.(omitted since it has only one word)
149.(omitted since it has only one word)

150.
software safety integrity:

part of the safety integrity of a safety-related system relating to systematic
failures in a dangerous mode of failure that are attributable to software

\\
     part
          > of the safety integrity
                 > [AND] of a safety-related system
                 > [AND] relating to systematic failures
                            > [AND] in a dangerous mode
                                      > of failure
                            > [AND] that are attributable to software
[Source: IEC 61508-4:2010]
```

```
151.
software safety integrity level:

systematic capability of a software element that forms part of a subsystem of a
safety-related system

\\
     systematic capability
          > of a software element
                 > that forms part
                        > of a subsystem
                               > of a safety-related system
[Source: IEC 61508-4:2010]

152.
spoof:

pretending to be an authorized user and performing an unauthorized action

\\
      [AND] pretending to be authorized user
      [AND] and performing an unauthorized action
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

154.
system:

interacting, interrelated, or interdependent elements forming a complex whole

\\
     [OR] interacting,
     [OR] interrelated,
     [OR] or interdependent elements
               > forming a complex whole
[Source: IEC 62443-2-4:2015 + AMD1:2017]
[Source: IEC TS 62443-1-1:2009]

156.
system software:

part of the software of a PE system that relates to the functioning of, and
services provided by, the programmable device itself, as opposed to the
application software that specifies the functions that perform a task related to
the safety of the EUC

\\
     part
          > [AND] of the software
                        > of a PE system
          > [AND] that relates to the | [AND] functioning of, and services
                                      |            > provided by, the
programmable device itself
                                      | [AND] , as opposed to the application
software
                                      |            > that specifies the functions
                                      |                   > that perform a task
                                      |                          > related to the
safety
                                      |                                 > of the
EUC
[Source: IEC 61508-4:2010]

157.
system software:

special software designed for a specific computer system or family of computer
```

systems to facilitate the operation and maintenance of the computer system and associated programs and data

\\
special software
| [AND] designed for a specific | [OR] computer system
| | [OR] or family
| | > of computer systems
| [AND] to facilitate the operation
| [AND] and maintenance
| > of the | [AND] computer system
| | [AND] and associated | [AND] programs
| | | [AND] and data

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

159.
threat:

circumstance or event with the potential to adversely affect operations, assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

\\
[OR] circumstance
[OR] or event
> with the potential
> to adversely affect | [OR] operations
| [OR] , assets
| [OR] , control systems
| [OR] or individuals
> via | [OR] unauthorized access
| [OR] , destruction
| [OR] , disclosure
| [OR] , modification
| > of data
| [OR] and/or denial
| > of service

[Source: IEC 62443-3-3:2013]

160.
threat:

potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

\\
potential
> [AND] for violation
> of security
> [AND], which exists when there is a | [OR] circumstance
| [OR] , capability
| [OR] , action
| [OR] , or event
| > that could | [AND] breach security
| | [AND] and cause harm

[Source: IEC Draft Guide 120]

161.
threat:

potentially damaging action or capability to adversely impact through a vulnerability

\\
potentially | [OR] damaging action
| [OR] or capability
| > to adversely impact
| > through a vulnerability
[Source: IEC TR 62443-3-1:2009]

162.
threat:
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

\\
potential
> [AND] for violation
> of security
> [AND] , which exists when there is a | [OR] circumstance
| [OR] , capability
| [OR] , action
| [OR] , or event
| > that could | [AND] breach security
| | [AND] and cause harm
[Source: IEC TS 62443-1-1:2009]

163.
tolerable risk:

risk which is accepted in a given context based on the current values of society

\\
risk
> which is accepted in a given context
> based on the current values
> of society
[Source: IEC 61508-4:2010]

164.
tolerable risk:

level of risk which is accepted in a given context based on the current values of society

\\
level
> of risk
> which is accepted in a given context
> based on the current values
> of society
[Source: IEC Guide 51:2014]

165.
vulnerability:

flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise

\\
[OR] flaw
[OR] or weakness
> [AND] in the | [OR] design
| [OR] , implementation

```
                                | [OR] , or operation
                                | [OR] and management
                                |           > of a component
                > [AND] that can be exploited to cause a security compromise
[Source: IEC 62443-2-4:2015 + AMD1:2017]


166.
vulnerability:


flaw or weakness in a system’s design, implementation, or operation and
management that could be exploited to violate the system’s security policy

\\
     [OR] flaw
     [OR] or weakness
               > [AND] in a system’s | [OR] design
                                     | [OR] , implementation
                                     | [OR] , or operation
                                     | [OR] and management
               > [AND] that could be exploited to violate the system’s security
policy
[Source: IEC Draft Guide 120]

167.
vulnerability:

flaw or weakness in a system's design, implementation, or operation and
management that could be exploited to violate the system's integrity or security
policy

\\
     [OR] flaw
     [OR] or weakness
               > [AND] in a system’s | [OR] design
                                     | [OR] , implementation
                                     | [OR] , or operation
                                     | [OR] and management
               > [AND] that could be exploited to violate the system’s | [OR]
integrity
                                                                       | [OR] or
security policy

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

169.
wide area network:

communications network designed to connect computers, networks and other devices
over a large distance, such as across a country or the world

\\
     communications network
          > designed to connect | [AND] computers
                                | [AND] , networks
                                | [AND] and other devices
                                |            > over a large distance
                                |                  > , such as across a | [OR]
country
                                |                                       | [OR]
or the world
[Source: IEC TS 62443-1-1:2009]

170.
wide area network:
```

communications network designed to connect computers over a large distance, such as across a country or the world

\\
     communications network
          > designed to connect computers
                 > over a large distance
                        >, such as across a | [OR] country
                                            | [OR] or the world
[Source: IEC TR 62443-3-1:2009]

171.
zone:

grouping of logical or physical assets that share common security requirements

\\
     grouping
          > of logical or physical assets
                 > that share common security requirements

[Source: IEC 62443-3-3:201

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

About the Safety-Critical Systems eJournal

Purpose and Scope

This is the Journal of the Safety-Critical Systems Club CIC (SCSC), ISSN 2754-1118 (Online), ISSN 2753-6599 (Print). Its mission is to publish high-quality, peer-reviewed articles on the subject of systems safety.

When we talk of systems, we mean not only the platforms, but also the people and their procedures that make up the whole. Systems Safety addresses those systems, their components, and the services they are used to provide. This is not a narrow view of system safety, our scope is wide and also includes safety-related topics such as resilience, security, public health and environmental impact.

Background

When the Safety-Critical Systems Club (SCSC) was set up thirty years ago, its objectives were to raise awareness of safety issues and to facilitate safety technology transfer. To achieve these objectives, the club organised events, such as Seminars and an annual Symposium, and published a newsletter, Safety Systems, three times a year.

The Newsletter has, in addition to news, opinion, correspondence, book reviews, and the like, also carried articles discussing current and emerging practices and standards. The length of such articles is limited to about two and a half thousand words, which does not allow an in-depth treatment. It was therefore been decided to add a third string to our bow and supplement the events and newsletter with this journal containing longer papers. The journal will be published here, as the Safety-Critical Systems eJournal, and is to comprise two issues a year.

Content Sources

Sources include the outputs of SCSC working groups; solicited technical articles and topic reviews; submitted articles on new analysis techniques, discussion of standards, and industrial practice; and guidelines and lessons learned. If you wish to contribute, please see, "Information for Authors".

Types of paper include, but are not limited to:

Technical Articles: Written by practitioners and describing practical safety assurance techniques and their industrial applications.

Integration Studies: Written by practitioners reporting upon successful (or otherwise) synergies achieved in practice with other assurance domains, e.g. security, environment, and resilience.

Position Papers: Written by, or on behalf of, Regulators, Standardisation Organisations, or other official bodies, setting out their position on a topic, e.g. the interpretation of a particular standard or regulation.

Review Articles: Papers highlighting recent developments and trends in some aspect of safety-critical systems or of their use in a particular industrial sector.

Historical Articles: Papers describing the development of safety assurance in an industrial sector; how we got to where we are today.

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

Perspectives: The authors' personal opinions on a subject, e.g. whether to use statistical methods in particular scenarios.

Reports: The lessons learned from incidents or the outcomes of trials with a description of scenarios, or methods, and a discussion of the results obtained.

Working Group Outputs: Written by Safety-Critical Systems Club Working Groups to include discussions, underpinning theory, or guidelines.

Copyright and Disclaimer