Safety Risk Management Methodologies

Overview of SRM methods and analysis based on systems thinking

This document was developed by the Safety Management Panel (SMP). It is intended to support safety experts in the application of risk management methodologies. Any comments to this material should be forwarded to safetymanagement@icao.int.

Version 1.0 – April 2026

CONTENTS

1. INTRODUCTION

"Managers are not confronted with problems that are independent of each other, but with dynamic situations that consist of complex systems of changing problems that interact with each other. I call such situation messes…
Managers do not solve problems, they manage messes."

Prof. Russell Ackoff, operations theorist

1.1 Who is this for?

Systems thinking is a way of approaching and understanding systems, in particular complex systems that abound in civil aviation for decades. This document is intended to support aviation professionals interested in considering different methods to manage the risks of the system(s) they're designing, manufacturing, operating, maintaining, supporting, overseeing, or interfacing with.

Although some concepts are provided, this document is not a course on complexity or systems theory. It is divided in five parts:

- **Chapter 1** – defines systems and how they can be categorised, puts ICAO's initiative about risk management methodologies in perspective, introduces the rationale and history of systems thinking, and lays out the principles (or tenets) of systems thinking selected for the analysis that can be found in chapter 3.
- **Chapter 2** – summarizes the different risk management methods reviewed in previous ICAO publications.
- **Chapter 3** – essentially combines the preceding chapters by assessing the alignment of each risk management method (listed in chapter 2) against the tenets of systems thinking (from chapter 1), then evaluates the suitability of each method for simple, complicated or complex systems.
- **Chapter 4** – provides some definitions, abbreviations, and references for further reading.
- **Appendix** – complements chapter 1 with further information on the evolution of systems thinking, focusing on risk management in high-risk industries such as aviation.

Readers who approach systems thinking for the first time or who are interested in a chronological discovery of the topic might prefer to start with the appendices 1 and 2 before returning to this introduction and following the usual sequence of chapters. Readers more familiar with systems thinking or looking for the assessment of popular risk management methods can skip the first two chapters.

1.2 Why this document?

In 2018, ICAO's 13th Air Navigation Conference[1] underlined once again the rapid pace of innovation and increasing complexification of civil aviation. Consequently, the Safety Management Panel was tasked to provide a wider range of references related to different methodologies and tools that support safety management practices. Of all the methodologies that were considered in the following years, about half a dozen were retained for further analysis and

[1] For the report of the 13th Air Navigation Conference, see ICAO Doc 10115.

detailed in separate guidance material[2]. Although very brief summaries are provided in this document, it does not fully replicate previous guidance. Instead, it aims to contrast the various methodologies by assessing their alignment with systems thinking principles, thereby assisting aviation organizations in evaluating which method(s) would be valuable to their specific risk management needs.

1.3 What is a system?

A system is a group of interacting and interrelated entities that form a coherent whole.

Systems are composed of:

1. **Elements** that usually are well defined and easy to distinguish, whether they're physical things or intangibles (e.g., cells, organs, people, buildings, mechanical parts, materials, software, culture, etc.).
2. **Interconnections or interactions** between elements. They may be intended, lasting, predictable, linear, or the exact opposite. Over time or under certain circumstances, elements may interact or interconnect although they were not designed to do so, producing new patterns of system behaviour (which is rather typical of complex systems). Moreover, many interactions operate through the flow of information between elements, holding the system together in the process.
3. All systems have at least one **function or purpose** (e.g., a watch must give time with sufficient accuracy) but there may also be purposes within purposes, particularly in more complex systems[3].

Discussing systems can be difficult because, in contrast with sentences that must be worded in a sequential, linear order, systems happen all at once: they're not connected in one direction, but in many directions simultaneously. Using graphics and pictures can be helpful to better grasp system elements and interconnections. However, since a system is more than the sum of its parts, its behaviour cannot always be predicted by simply knowing or drawing its elements and interconnections.

Of the three basic system components listed above, functions or purposes are often the most crucial to determine how a system behaves, especially when dealing with complex systems involving human actors. A function or a purpose may not necessarily be explicit, obvious, or aligned with the intentions or goals of the people working for the system. The best way to deduce the purpose of a complex system may be to observe its behaviour and outputs rather than solely relying on company rhetoric, policies, posters, and slogans[4].

"A system is never the sum of its parts; it's the product of their interactions."

Prof. Russell Ackoff, operations theorist

[2] For further detail, see the ICAO Safety Management Implementation website at www.icao.int/smi

[3] For a deeper look into systems, refer to Meadows (2008). For the reasons why complex systems fail, refer to Cook (2021). See references in 4.3.

[4] Confusion is possible and even rather common considering the difficulty of stepping back from one's organisation and viewing it as if from outside. However, when able to do so, people sometimes realise that their organisation produces something quite different from what they had intended, if not the exact opposite (e.g., fatal accidents).

1.4 Types of systems

Like other high-risk industries that have grown in complexity at the pace of technological innovations, aviation is regarded as an entanglement of systems. They generally are categorized as follows:

Type of system	Description
Simple	Consists of a relatively small number of elements that act together according to laws that are well-defined and easy to understand and predict. Simple systems are typically the domain of 'best practices'. However, simple systems do not necessarily remain so and, under some conditions (e.g., disturbances), may behave in complex ways. *Examples: a pendulum, a clock, most mechanical systems, etc.*
Complicated	Built from a significant number of elements, with well-defined function(s) to perform, and governed by clear and understandable laws. Although the structure and interactions of the system elements are more complicated, experts can still reasonably predict their functioning using linear causal chains and by investigating several options. However, a single cause may have multiple effects, and a single effect may be the result of several possible causes. This is the domain of 'good practices' rather than 'best practices'. *Examples: a jet engine, the hydraulic system of an airliner, a steam locomotive, etc.*
Complex[5]	Built of many elements that are connected to each other and that cooperate together according to rules which may or may not be well defined, but that can also change with time. Although the behaviour of any element is unpredictable or even random to a certain degree (e.g., consider the variability of human performance, or the reliability of bolts and nuts), the sheer number of interactions and dependencies between all the elements of a complex system also creates opportunities for emergent system behaviours that are nonlinear (i.e., not happening in an expected sequence, or where outputs are not necessarily proportional to inputs) and even unpredictable. This unpredictability may manifest itself even though the system's performance is defined by strict policies and procedures. Put differently, the whole of the system is greater than the sum of its parts. Unlike simple or complicated systems, complex systems have the unique ability to learn from, and adapt to, change, challenges, and operational surprises, thanks to their human component. However, causal analyses of complex systems are generally not an effective method to improve system performance because the behaviour of the system cannot always be predicted from examining the behaviour of its separate parts, and the system cannot always be understood by only looking at one component or from one perspective. *Examples: the maintenance facility of an airline, a nuclear power plant, a hospital, a rainforest, etc.*
Chaotic	Regardless of the number of system elements, cause and effect are not discernible. A chaotic system is unpredictable, volatile, and typically unsustainable. Since any form of analysis provides little hindsight and no foresight, the basis for making decisions is often limited to trial and error in an attempt to stabilize the system.

Table 1 – Types of systems

1.5 Doesn't aviation already take a systemic perspective on safety?

One could argue that civil aviation is already 'systematically thinking' and crowded with 'systems thinkers' for several decades. Indeed, compared to worldviews that explained accidents as solely the result of a person's alleged accident proneness or inappropriate morality (with or without the intervention of 'divine wrath' or fate as the main cause), tremendous progress has been made in our understanding of causality in human affairs. However, nuances and differences in opinion persist, will likely remain, and could even be capitalized upon.

For instance, following an occurrence in their organisation, two aviation professionals may have different opinions after reading their Safety Manager's detailed internal investigation report written using Reason's popular Swiss Cheese Model of accident causation[6]. The differences, if any, can range from minor to significant. One person could

[5] Some complex systems are also labelled as sociotechnical. This adjective simply refers to the presence of human, organizational, and technical elements in the system, and to the fact that they interact. The presence or absence of humans is not a reliable criterion to consistently differentiate systems, since human involvement is unavoidable. All systems involving humans are not necessarily labelled as complex.

[6] The first documented outpourings of systems thinking applied to high-risk industries can be traced back to the 19th century. Although Dr James Reason was neither the first nor the only one to formulate a broader causality model of organizational accidents encompassing latent conditions and active failures, his model co-authored with Eng. John Wreathall in the late 1990s remains a popular risk communication tool in these industries.

perceive the report as sufficiently pertinent, practical, and helpful in identifying what happened but also which training course, company procedure, equipment, or requirement needs improvement. The other, without even discounting the findings and recommendations in the report, might think that the account is indeed valuable but perhaps a bit too straightforward or too linear. That person may also wonder whether the investigation focused too much on frontline workers. Or whether the investigators were keener on retracing only the accident sequence, rather than also understanding how normal operations vary and how the organisation adapts (or not) to these incessant, unavoidable changes. Another question could be about the scope of the investigation to fully understand daily challenges, pressures, conflicting goals, and trade-off decisions. Or about what was left out of the report.

While all the aviation professionals in this fictitious example are acutely aware of the existence of all human and non-human elements in a system and of their interactions, some will likely focus more on interventions at the level of particular system components (typically to equipment and frontline workers) whereas others will likely focus more on interventions that consider the interactions and interdependencies between all systems components. Where one person will interpret an event as a coincidence of independent failures and human errors, another will interpret it as a systematic migration (or drift) of organisational behaviours, as an effect of seeking cost-efficiency in a highly competitive environment with limited resources. Both approaches are valuable and -fortunately- are not mutually exclusive. Arguably, the greatest return on effort of using one approach or the other will depend on the unique characteristics of the event that the organisation wishes to investigate or prevent (in the case of proactive risk assessments).

Mechanics, surgeons, carpenters, engineers, and countless other professions rely on a set of different tools to get their job done and to achieve the goals of their organisation. Safety professionals are no different, be they risk managers, investigators, regulators, etc. Different perspectives, theories, models of causality, and safety management tools also coexist. Some are better suited for analysis and investigation, for proactive risk management, or for communication about risks with a diverse audience. At the moment, no single method, model, or theory is able to address all possible needs or all possible types of systems to perfection.

1.6 The need to think in systems

The fictitious example in 1.5 above introduced the contrast that can emerge between personal perspectives on risk, accidents, and safety. The first safety professional tends to lean more towards a reductionist approach, whereas the second tends to lean more towards a systems thinking approach. Rooted in the 16th century Scientific Revolution and widely considered to be successful in many societies, industries, and scientific fields, the reductionist methodology aims to break large problems into smaller ones that are easier to manage, and to explain causality by reducing processes or behaviour down to simple components or isolated parts[7]. This method can indeed be very effective but is not appropriate for *all* types of systems. More precisely, although relying entirely on a reductionist approach will likely address many issues and weaknesses in many types of systems, it will also allow -or even foster- the emergence of 'leftover', complex problems that were not fully envisaged or not considered at all.

When intricate issues eventually irrupt in daily operations, humans and technology are often ill-prepared to solve them with the time, resources, and knowledge they're typically given. Although some exceptional responses to a sudden crisis situation led to rather positive outcomes[8], many recovery attempts were unable to prevent a catastrophe[9]. In other words, civil aviation needs to complement its predominantly reductionist approach with more holistic perspectives to further improve its remarkable safety performance in a context of uninterrupted growth, complexification, and innovation.

The challenge is to take the complex entanglement of relationships and behaviours between human, technology, and their environment into due consideration. Put differently, both the creation and erosion of safety are the result of emergent behaviours that may not be straightforward, linear, controllable, or even predictable. Systems thinking

[7] Counterexamples can be found throughout the ages, for instance in holistic perspectives on health or military strategies in Ancient China, etc.

[8] Examples include the 'miracle on the Hudson', the DC-10 accident at Sioux City (UA232), or the A380 emergency landing in Singapore (QF32).

[9] Examples include the A340 loss of control over the South Atlantic (AF447), or the twin B737 MAX accidents.

improves outcomes in such complex systems. It is *"an approach to viewing systems holistically, rather than focusing on component failures and on direct causal relationships between those components. Through this approach, the components or parts of a system are viewed as integrated and interactive, rather than isolated and independent, shifting attention to the ever-changing influences and relationships among all the different parts. (…) Systems thinking is critical to recognize the extent to which the interactions within a system are unpredictable, unknowable, and of equal or even greater interest than the performance and reliability of its individual components"* (ICAO website, 2024).

Systems thinking is rooted in systems theory and in complexity sciences (see appendices 1 and 2 for a brief history). The former emerged within the physical and biological sciences[10], whereas the latter is an extensive field interested in tackling multi-dimensional, dynamic, and unpredictable problems, with a strong focus on interactions among elements within a system[11]. Therefore, systems thinking is not monolithic. Instead, it is fundamentally interdisciplinary and offers a range of approaches and modelling techniques that practitioners can choose from. Some have already been briefly presented in ICAO documents[12] but lesser-known models are also worth considering when designing or operating complex systems[13]. Since no single model is universally accepted or even universally applicable, there's value in scoping different options and matching the optimum model to the users' requirements and needs.

1.7 Systems thinking tenets

Systems thinking should be seen as a multifaceted philosophy in safety science that comprises several approaches and models. Despite some commonalities, each model has its particularities. Recent efforts to synthesise and find consensus on key principles of systems thinking have led to the publication of a handful of sets of tenets to identify important system features. In the context of systems thinking, a tenet is defined as a characteristic of a system (i.e., not just of components but through interactions of components) that creates either safe or unsafe system behaviours.

Several sets of tenets were identified and considered (see also appendix 3 for a list of the tenets in each set):

- Rasmussen (1997) – 7 tenets (summarised in Dallat, et al., 2019)
- Eurocontrol (2014) – 10 tenets
- Grant, et al. (2018) – 15 tenets
- Salmon, et al. (2023) – 10 tenets

Considering the diverse backgrounds of the users of ICAO Doc 9859 and related content, the "original" set of systems thinking tenets from Rasmussen was perceived as the most pertinent for the task. More precisely, it seemed important to introduce systems thinking tenets from the ground up, with a relatively small number of tenets that are comprehensible to the widest audience.

Mentioning the other sets appeared equally important. First, acknowledging the coexistence of several sets not only gives them visibility but also indicates both the flexibility and on-going evolution of systems thinking across multiple domains. Moreover, the set by Eurocontrol is a prime example that organisations do not necessarily have to replicate frameworks proposed by safety science scholars. Provided that an organisation doesn't denature or dilute systems thinking, it could be better served by translating and adapting those frameworks to their specific environment and organisational setting. Finally, this guidance document focuses on SRM and doesn't cover the whole spectrum of applications where systems thinking is helpful. Depending on the user's needs, another set could be more pertinent or more efficient.

[10] For further information, refer to Von Bertalanffy's seminal work and principles of open systems applied to living organisms.

[11] See also appendix 2 for an overview of the five intellectual traditions underpinning complexity sciences.

[12] Refer to the guidance documents on STPA and FRAM, available on ICAO's Safety Management Implementation website: www.icao.int/smi

[13] Examples include AcciMap, AcciNet, Net-HARMS, EAST, Agent-Based Modelling, etc. See also Salmon, Stanton, et al. (2018).

Each of the seven systems thinking tenets listed in table 2 is accompanied with a description based on accident analyses and an explanation of its relevance for SRM[14].

Tenet	Description	Translation for risk assessment methods
Multiple actors and levels	Risk is an emergent property of complex socio-technical systems. It is impacted by the decisions of all actors in the system and not just front-line workers.	The method identifies actors, decisions and actions involved with the provision of the task.
Multiple contributing factors	Risks are usually caused by multiple contributing factors across multiple levels of the organisation, not just a single catastrophic decision or action.	Multiple hazards and risks are considered within and between all levels of the system, and not solely by those at the sharp end, or solely by one 'catastrophic' or 'obvious' risk/hazard.
Vertical integration	Risks can result from a lack of vertical integration (i.e., mismatches) across levels of a complex socio-technical system, not just from deficiencies at any one level alone.	The method enables the deliberate provision of communication opportunities between actors and artefacts, in relation to hazards and risks, at all levels in the system, and not solely between those positioned at the front line.
Feedback	Lack of feedback also leads to loss of vertical integration across multiple levels. Actors are not able to see or anticipate the impact of their decisions, so risks are not obvious before an accident.	The method offers opportunity for actors in the system to verify that actions, decisions, and communications have been received and understood as intended at all appropriate levels.
External pressure	Risks are not static and tend to migrate over time under the influence of a cost gradient driven by financial pressure and an aggressive competitive environment. Work practices also migrate under an effort gradient driven by psychological pressure to follow the path of least resistance.	The method purposefully considers and evaluates potential external pressures impacting actors and artefacts across all levels of the system. The method enables new and emerging hazards and risks to be frequently considered and is not simply a repeat of past iterations; irrespective of past accident performance.
Migration of work practices within and across levels	Risks occur at multiple levels of the organisation, not just one level alone.	The method is adaptive enough to enable ongoing, dynamic risk assessment to occur.
Erosion of defences through migration of work practices	The migration of work practices over time leads to the gradual erosion of the systems defences. Risks occur as a combination of this systematic migration and a triggering event, rather than by the occurrence of an unusual action or one-off threats to safety.	The method seeks to provide context to current work practices, influences, and hazards.

Table 2 – Systems thinking tenets for SRM activities (adapted from Dallat, et al., 2019)

[14] In the interest of brevity, examples of safe and unsafe system behaviours that illustrate each tenet haven't been included. However, this is generally available in the source documents if needed (see references in 4.3).

1.8 When complementarity adds further value

The fictitious example used in 1.5 introduced the distinction between the reductionist and systems thinking approaches but also the value of considering complementary perspectives when appropriate. To illustrate this point, we'll use an actual case-study shared by an engine manufacturer whose engines performed in unexpected ways during routine airline flights many years ago. Fortunately, the events happened only twice, on the ground, and had no serious impact on safety. A thorough analysis led to systemic corrective actions and no similar occurrence has been reported since.

As one could expect in commercial air transport, the engines were designed, assessed, flight-tested, certified, manufactured, and operated in accordance with all applicable standards, regulations, and procedures. However, their protection system intended to prevent a number of unsafe situations (e.g., one engine stuck in full forward thrust while the other is in full reverse thrust during a rejected take-off) triggered an automatic, precautionary shutdown in both engines during landings. In both cases, which happened with different engines two years apart, both engines shut themselves down while the aircraft were decelerating on the runway and could not be restarted by the crew. The investigation concluded that no part or component failed, and that the pilots didn't violate any regulation or procedure published at the time. The engines performed 'as expected'.

Expanding one's perspective and 'toolbox' of risk management methods through systems thinking means - among other things - to also consider scenarios where no component fails, but where hazardous conditions can nevertheless emerge from interactions between components even though they all perform nominally or within their specifications. On the one hand, the performance of most of the equipment used in aerospace demonstrates that reductionist approaches repeatedly deliver increasing levels of reliability and efficiency. On the other, these dual engine shutdowns exemplify the limits of methods that focus heavily if not exclusively on the effects of one or more component failure(s) and on common mode failures.

In another example, an aircraft manufacturer used both reductionist and systems thinking approaches to define safety constraints while developing the smoke control system of a new aircraft type. Of all 43 constraints identified and brought into the design of the system to assure that no uncontrolled fire would ever spread through the aircraft:

- 19 safety constraints (44%) were captured by existing requirements and standard processes.
- 16 (37%) could only be captured through a systems thinking approach.
- 8 (19%) were traditionally captured during advanced stages of development, but were found earlier through a systems approach.

Although it has been simplified in the interest of brevity and clarity, the account of the engine shutdowns wouldn't be complete without also mentioning that the engine protection system had been reviewed through the lens of systems thinking shortly before entry into airline service. The analysis identified a few dozen failure scenarios that had not been considered or taken into account during development and certification. It also found a number of flawed or missing requirements, procedures, and assumptions (particularly on human performance). Corrective actions included a Service Bulletin, new system requirements, updated procedures for pilots, and software modification.

2. Overview of risk management methods

"I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail."

Prof. Abraham Maslow, psychologist

This section summarises seven of the dozens of risk management methods, models, and approaches developed in the past century. In addition to a brief description, a list of the perceived strengths and weaknesses of each method (i.e., pros and cons) is provided to assist organisations in identifying which are worth considering and could be a good fit for a specific activity, product or system.

The suitability of a method depends on a combination of factors. Some relate to the organisation (e.g., complexity, resources, experience, etc.), whereas others relate to the methodology itself. Several criteria need to be considered, such as:

- the complexity of the method or, to be more precise, its ability to adapt to the complexity of the activities, systems or products to be analysed for SRM (e.g., applying a simple method to a simple system would appear worthwhile, but would most likely be counterproductive if applied to a complex system),
- the resources needed to apply the methodology, including for training,
- the costs of any software or IT tool needed for SRM activities,
- the quality of the output and the ease to both communicate and understand those outputs,
- the availability and quality of the data to be used.

Risk management methods do not provide clear and irrefutable answers but instead help structure SRM decision-making into thoughtful and systematic processes. In the absence of a universal methodology or method, it is therefore important to identify which would be a good fit without completely shutting the door to other approaches. Readers are therefore encouraged to have more than a single tool in their SRM toolbox.

Moreover, in the interest of brevity some perceived limitations of SRM methods that appear common to all were not repeated. For instance:

- They provide comparatively more insights and value by assisting in identifying hazards and assessing risks than in building and dealing with mitigations in practice (often outside of their scope or capabilities),
- Finding reliable data to analyse or quantify risks can be challenging at best,
- Mitigating cognitive biases is difficult and can require learning new skills[15],
- Different users will inevitably reach different conclusions[16],
- While some level of simplification of complicated or complex systems is inevitable, the risk of oversimplifying analyses and creating a false sense of safety is always present to some degree.

[15] One of the possible starting points could be NASA's Practitioner Checklist for the Aerospace Sector, by Emmon, et al. (see references in 4.3).

[16] The opposite should probably raise concerns about the potential existence of groupthink.

2.1 Risk matrices

A risk matrix is a table or grid that combines two scales to rate the likelihood and severity of a particular outcome and in turn assign a level of risk once the ratings are combined. The intersection of these scales is often divided by risk tolerability (e.g., negligible, acceptable, unacceptable) to guide decision-making and follow-up actions, if needed. This simple assessment model is in use for at least 1700 years[17] and found in countless domains, helping risk owners and management to assess risk before and after taking mitigation actions.

Perceived strengths/pros	Perceived weaknesses/cons
• Effective for risk management due to simplicity, practicality, and broad applicability. • Excels in visualizing outcomes, comparing risks by severity and likelihood, and identifying worst-case scenarios, enhancing meeting engagement. • Beneficial for senior management, supporting decision-making by showing risks before and after mitigation efforts. • Streamlines risk recording and monitoring when used with risk registers. • Instrumental in determining the need for further mitigation actions, assessing residual risk acceptability, and evaluating control effectiveness (e.g., what to measure and monitor). • No need for high skills and knowledge to understand (e.g., useful when resources and budget are limited).	• Simplistic approach focusing on the rating of risks. • Not designed to consider contributing factors, human performance, external pressures, etc. • Less suitable for complex situations involving multiple stakeholders and levels (e.g., runway incursions with actions required from various entities). Does not consider the dynamic, non-linear behaviours of complex systems. • Struggles with visualizing effectiveness of mitigation measures and allocation of resources (partially mitigated by incorporating risk registers). • Subjectivity in assessing severity and likelihood, leading to differing assessments. Limited consistency among different assessments of the same risk, suggesting the need for customization, training, and monitoring. • Challenge in setting tailored risk tolerability zones, necessitating decisions at the highest management level to be consistent with the organization's safety objectives. • Potential for higher qualitative risk ratings for lower quantitative risks.

Table 3 – Perceived pros and cons of the risk matrix

[17] Although the Asipu tribe from the Tigris-Euphrates valley is known to have been the first 'risk consultants' (c. 3200 BC), the first documented risk matrix can be found in a seven-volume treatise by Arnobius the Elder to justify the sincerity of his wish to abandon pagan beliefs and practices and to convert to a monotheist religion (c. 303 AD). It was expanded by Blaise Pascal in 1657 as one of the first applications of his probability theory.

2.2 Bowtie

Bowtie is a visualisation tool to graphically organise threats, controls, mitigations, and consequences around a so-called top event (one event at a time). It is based on the principles of barrier management to help prevent, control, or mitigate undesired events. Bowties can be found in several high-risk industries. Being built on a linear and rather simple concept of causality, it can also be used as an educational tool, provided the Bowtie is not too extensive.

Perceived strengths/pros	Perceived weaknesses/cons
• Accessible to anyone with minimum expert knowledge of the component or system to be analysed. • If kept simple (trade-offs will be inevitable), can be used with a wide audience as a risk communication tool. • Can potentially provide both qualitative and quantitative results. • Draws attention to both preventative and recovery barriers, facilitating the monitoring of these controls and their effectiveness. • Can be used proactively and reactively. • Size and complexity of a Bowtie is flexible (from simple to large, compounded Bowties). • Most valuable for risk assessments of hardware or simple systems and subsystems (with little or no software or human element).	• Minimum knowledge, skills, and training needed (e.g., on Fault Tree and Event Tree Analyses). • Focuses on one top event at a time and becomes quite intricate when attempting to consider several top events simultaneously. • The graphical end-product is not an analysis method per se nor a complete SRM tool on its own. • Resource-intensive. • Due to the resource issue, users typically create a limited number of bowties that do not cover their entire operations, systems, and interfaces (e.g., mostly low-probability, high-consequence accidents). • Significant risk of oversimplification, particularly of highly automated systems. • Does not consider the dynamic, non-linear behaviours of complex systems (e.g., the failure or absence of controls may be difficult to identify).

Table 4 – Perceived pros and cons of Bowtie

2.3 ISO 31000

ISO 31000 provides a common, global guideline on the management of any type of risk faced by any organization regardless of industry or sector. Being high-level by design, the proposed risk management framework and process necessitate customization. However, it is supported by guidance material with examples of pertinent concepts and techniques. The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

Perceived strengths/pros	Perceived weaknesses/cons
• Standard high-level process that can be applied across any industry. • Globally recognized standard. • Broad international consensus on suitability of methodology. • Significant training available across all regions. • Applies to more than just aviation safety and is sometimes used as foundation for security management.	• Light on detail – a high-level document that focuses on considerations for processes and frameworks. Does not provide meaningful detail on how to implement (although IEC 31010 gives good options and examples for practical implementation). • Oriented towards enterprise management, sometimes at odds with risk science (e.g., definition of risk). • Terminology differs from ICAO Doc 9859 (terminology differences can often derail the effective implementation of process and procedure). • Integration and customization require significant stakeholder support, particularly from senior management. • Does not consider the dynamic, non-linear behaviours of complex systems.

Table 5 – Perceived pros and cons of ISO 31000

2.4 SORA – Specific Operation Risk Assessment

SORA is a harmonized risk assessment methodology for UAS operations in the 'specific' category. It is based on the principle of a holistic/total system perspective to evaluate risks related when creating, evaluating and conducting an UAS operation (from both operator and authority standpoints). The methodology provides a standardized, ten-step process to analyse the ground and air risk of the proposed Concept of Operations (ConOps) and to then establish an adequate level of confidence that the operation can be conducted with an acceptable level of risk.

Perceived strengths/pros	Perceived weaknesses/cons
• Highly detailed process considering all aspects of UAS operations. • Widely adopted practice globally. • Broad international consensus on suitability of methodology. • Increasingly available training options available across most regions. • Comprehensive but relatively straight forward process (once familiar with process). • Underpinned by quantitative modelling.	• Highly specialized risk assessment methodology only able to be applied to UAS operations. • Heavily reliant on qualitative data/inputs – limited quantitative input. • Requires an overall understanding of the process and intent – can take time to get a full understanding. • Does not consider the dynamic, non-linear behaviours of complex systems.

Table 6 – Perceived pros and cons of SORA

2.5 STPA (System-Theoretic Process Analysis)

STPA is a proactive and holistic hazard analysis and risk management tool that considers an entire system and does not focus on risks at the task level. Being deeply rooted in systems thinking and control theory, it was specifically designed to better address interactions between system components, regardless of the level of complexity of the system, rather than only addressing component failures. Experience with STPA is growing across high-risk industries and indicates that it is a valuable complement to traditional analysis techniques, if not an alternative.

Perceived strengths/pros	Perceived weaknesses/cons
• Underpinned by systems theory. • Considers the loss of control(s) across the whole sociotechnical system in a more comprehensive manner than traditional models (e.g., Fault Tree Analyses, Bow Tie, etc.) and therefore doesn't only look for risks at front-line level. • Considers hazards residing throughout the system but also their interactions. • Shown to be more effective at the identification and analysis of early warnings than conventional approaches. • Likely to be more efficient than traditional models (i.e., richer results obtained from comparatively less resources), without excluding linear causality which remains relevant for simpler systems and components/elements. • Numerous resources, including training, documentation, and IT tools, are freely available and regularly updated by the main authors and contributors from MIT.	• Requires at least an understanding of systems thinking principles. • Requires some training and practice. Needed skills/knowledge likely burdensome for small organisations not having resources to allocate. • Doesn't seek to quantify risks or losses (quantification deemed often too unreliable in complex sociotechnical systems to be useful, although it may remain valuable for purely technical, engineering aspects of the system) • While effective at analysing complex systems, it inevitably requires proportional investments to achieve its goal, which may prove problematic for the smallest organizations using STPA in isolation. • STPA being steeped in engineering, the role of front-line workers adapting to real-time conditions and operational variability may be difficult to model with precision.

Table 7 – Perceived pros and cons of STPA

2.6 ARMS ERC (Aviation Risk Management Solutions - Event Risk Classification)

ARMS was specifically designed for aviation and comprises three distinct elements: ERC for retrospective Event Risk Classification, SIRA for prospective Safety Issue Risk Assessments, and Safety Assessment to support risk assessments when managing change. ERC focuses on assessing the risk of past events but offers an enhanced version of the classical risk matrix. For instance, the assessment of probability corresponds to the assessment of the effectiveness of the remaining barriers between the event and the most credible accident scenario, and the risk scale is not linear but exponential. ERC enables different events to be scored in a standardised way, as well as the aggregation of events.

Perceived strengths/pros	Perceived weaknesses/cons
• Simple to use (commonalities with the risk matrix). • Broadly compatible with other risk assessment methodologies included in ICAO SMM. • Aviation specific – developed by aviation safety professionals for aviation. • Considers the effectiveness of barriers relevant to the operation of the organization. The barrier model can be adapted to the tenets of systems thinking. • Recognizes that the event could have led to a worst scenario (proactive approach); • Useful when the volume of events is significant, as it helps to identify the worst scenario cases and where to immediately engage actions	• Requires prior development of a barrier model adapted to the domain/organization (originally designed for operational flight safety risks). • Built on a linear model of accident causation (e.g., at odds with systems thinking). • Process has not been reviewed since 2010 and the methodology has no current custodian (i.e., ARMS Working Group is no longer meeting).

Table 8 – Perceived pros and cons of ARMS ERC

2.7 ARMS SIRA (Safety Issue Risk Assessment) and Safety Assessment

SIRA (and the complementary Safety Assessment element) can be viewed as the prospective version of the ARMS ERC methodology detailed above. It is utilized to assess the risk of emerging safety issues identified through data analysis, whereas Safety Assessment is more targeted at supporting risk assessments during a change management process (e.g., focusing on a specific part of an operation, such as the launch of a new route or activity). Both elements significantly rely on the presence of suitable safety data to inform decision-making and use concepts that are very close to the risk matrix and bowtie methodology. While both elements were specifically designed for aviation, their current adoption rate appears to remain limited.

Perceived strengths/pros	Perceived weaknesses/cons
• Broadly compatible with other risk assessment methodologies, including ICAO's. • Aviation specific - developed by aviation safety professional for aviation • Internationally recognized approach. • The methodology may be customized to specific organisational requirements and preferences. • Greater objectivity in assessing risks than the other risk assessment methods.	• High initial effort for organisations to develop criteria and process aligned with ARMS SIRA. • Process has not been reviewed since 2010 and the methodology has no current custodian (i.e., ARMS Working Group is no longer meeting). • Reliant on comprehensive organisational safety data to assess risks, therefore less useful for novel risks for which data does not exist or for activities with few sources of safety data • Difficulty in determining barrier failure rates for human performance-related controls. • Built on a linear model of accident causation (e.g., at odds with systems thinking). • Unlikely to find 'off the shelf' risk management software providers that enable SIRA approach.

Table 9 – Perceived pros and cons of ARMS SIRA

2.8 FRAM (Functional Resonance Analysis Method)

FRAM is an analytical tool not solely focused on failure cases and their causes and consequences, but also on understanding complex sociotechnical systems at all stages of their lifecycle in order to improve their resilient behaviour. This method assists in describing the functioning of a system (i.e., in everyday work or during a particular event) and to understand how the different human, technological, and organisational functions behave within a system to achieve its goals, and may be impacted by variability (i.e., variability of a single function or a combination thereof). Being more recent and having slightly less commonality with "basic" engineering principles than other methodologies, the number of publications and guidance to support FRAM implementations may not yet be as extensive but is growing, as it is nevertheless used in various settings and for various purposes in aviation.

Perceived strengths/pros	Perceived weaknesses/cons
• Holistic method underpinned by systems theory and fostering a deeper understanding of complex systems. • Core principles are relatively straightforward, but their application from simple through complicated to complex systems should be done progressively. • Can be used reactively (e.g., investigation) and proactively (e.g., system design), but is better suited and more effective with existing systems (i.e., already in operation vs. only at the concept stage). • Effective method for the assessment of performance variability and gaps between the varieties of work (e.g., particularly the gap between WAI and WAD) • Quantification (e.g., risk probability) is now provided in different extensions to the standard method. • Supported by a global community of practitioners and academics that offers and regularly updates both guidance and IT tools.	• Requires at least an understanding of systems thinking principles. • Detailed system information is needed prior to analysis. • Representations are not self-explanatory, rather they allow users to better understand the system, and enable the development of mitigation. • While effective at analysing complex systems, it inevitably requires proportional investments to achieve its goal, which may prove problematic for the smallest organizations using FRAM in isolation.

Table 10 – Perceived pros and cons of FRAM

3. Comparative analysis

3.1 Alignment with systems thinking tenets

This section evaluates to what extent the various risk management methods presented in section 2 align with the systems thinking tenets detailed in section 1 (see 1.7).

It is widely acknowledged that both successes and failures of aviation activities are systems phenomena. Consequently, accident investigators use a range of different analysis tools and methods to understand occurrences. This allows them to identify lessons to be learned and to issue recommendations to prevent a recurrence. Some of those methods (and the overarching methodology they're built on) are aligned with systems thinking, whereas others are not[18]. However, this multifaceted approach in accident investigation is not necessarily replicated in proactive SRM since many safety managers and safety departments tend to use a smaller number of methodologies, methods, models, and tools. Moreover, this also raises questions about the theoretical basis of these methods used in proactive risk assessments. For instance, does the chosen method lead its users to consider that system elements might interact and affect safety performance? Does the chosen method draw attention to feedback across the organisation?

Table 11 summarises whether each method, and by extension its methodology and their core principles, drives their users to identify system characteristics that create either safe or unsafe system behaviour. Three answers were retained to cater for the frequent absence of any form of certainty when managing risks:

Yes - by design, the systems thinking tenet is embedded into the core principle(s) of the method.
No - by design, the systems thinking tenet is not embedded into the core principle(s) of the method.
Possible - the systems thinking tenet is *not* embedded by design into the core principle(s) of the method, but highly experienced aviation professionals could slightly deviate from the method to enhance the pertinence or quality of its outputs without significantly undermining its integrity[19]. However, 'possible' doesn't mean 'likely' since adjustments to a method won't necessarily be aligned with systems thinking.

Tenet	Risk matrix	Bowtie	ISO 31000	SORA	STPA	ARMS[20]	FRAM
Multiple actors and levels	no	possible	yes	yes	yes	possible	yes
Multiple contributing factors	no	possible	possible	possible	yes	possible	yes
Vertical integration	possible	possible	yes	possible	yes	possible	yes
Feedback	no	possible	yes	possible	yes	possible	yes
External pressure	no	possible	possible	no	yes	possible	yes
Migration of work practices at multiple levels	yes	no	yes	possible	yes	no	yes
Erosion of defences through migration of work practices	no	no	possible	no	yes	no	yes

Table 11 – Alignment of SRM methodologies with systems thinking

[18] According to recent research by Bill, Costello & Cattani (2023) major AAIBs reported using at least three and sometimes well above six different accident causation models during their investigations (e.g., Swiss Cheese, AcciMap, STAMP/CAST, Bowtie, HFACS, FRAM, SHEL, etc.).

[19] This would typically happen with methods built on linear causality only. However, attempts to deviate from a method inevitably raise questions about its pertinence and validity. They usually are best answered within the organisation conducting the risk assessment or system analysis.

[20] Since no significant difference could be identified, all three elements of the ARMS method are grouped under the acronym ARMS.

3.2 Suitability of the methods

To cope with increasingly intricate systems, various risk management methods have been developed and honed over time. Inevitably, some are better suited for a particular system than others. Generally speaking, 'simple' methods are already well-known and produce positive results in simple or even some complicated systems (i.e., purely technological systems). Although it may be tempting to select what appears to be the least complex method reasonable, attention must also be paid to the level of simplification driven by a particular method. All risk management methods without exception will simplify to some extent the system that is being analysed or designed in order to make it comprehensible, manageable, or even predictable to the largest degree possible.

When selecting a method, the key is therefore to find the right balance between:

- the gaps between the actual system functioning in the real world and its model, and, on the other hand,
- the resources that are needed to achieve a level of understanding of the system that doesn't overlook important considerations for safety.

For instance, using a method that is 'too simple' for the complexity of a system may lead to missing safety-critical interactions between system elements, or to significant headaches while trying to compensate for the method's limitations when modelling a system or investigating an event. Conversely, using a method that is 'too complex' will likely create undue tensions on limited resources and generate questionable returns on investment.

While acknowledging that this guidance document is unable to provide reliable advice since organisational specificities and circumstances are both unique and ever-changing, table 12 nevertheless attempts to suggest which method(s) would likely complement current SRM approaches and operational practices in a useful manner. In other words, the different signs used in the table do not express endorsement or opposition to a particular method. Instead, they should be understood as meaning the following:

+ The method clearly appears as potentially relevant and useful for the type of system considered (i.e., worth considering and testing before a wider implementation).

+/- The relevance and usefulness of the method appears to be conditioned to a number of variables that need to be addressed by its user (i.e., although the method is worth considering and testing, close attention should be paid to both expected and unexpected/unintended outcomes).

- The method clearly appears to contain limitations that will affect its potential relevance and usefulness in the type of system considered (i.e., these limitations cannot be ignored or even underestimated).

Type of system	Risk matrix	Bowtie	ISO 31000	SORA	STPA	ARMS[21]	FRAM
Simple	+	+	+	+	+/-	+	+/-
Complicated	+/-	+/-	+	+/-	+	+	+
Complex	-	-	+/-	+/-	+	+/-	+

Table 12 – Perceived relevance of SRM methods in various types of systems

[21] Since no significant difference could be identified, all three elements of the ARMS method are grouped under the acronym ARMS.

4. Additional information

4.1 Abbreviations

Abbreviation	Meaning
AAIB	Aviation Accident Investigation Bureau/Board
ARMS	Aviation Risk Management Solutions
BANI (world)	Brittle, Anxious, Nonlinear, Incomprehensible world
CAST	Causal Analysis based on Systems Theory
ConOps	Concept of Operations
ERC	Event Risk Classification
FRAM	Functional Resonance Analysis Method
MIT	Massachusetts Institute of Technology
PANS	ICAO Procedures for Air Navigation Services
SARP	ICAO Standards and Recommended Practices
SIRA	Safety Issue Risk Assessment
SMM	Safety Management Manual
SORA	Specific Operation Risk Assessment
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
UAS	Unmanned/Uncrewed Aircraft System
VUCA (world)	Volatile, Uncertain, Complex, Ambiguous world
WAD	Work-as-done
WAI	Work-as-imagined
WW2	World War 2

Table 13 - Abbreviations

4.2 Key terms

Term	Explanation
Complicated system	Built from a significant number of elements, with well-defined function(s) to perform, and governed by clear and understandable laws. Examples: a jet engine, the hydraulic system of an airliner, a steam locomotive, etc. (Adapted from Grabowski & Strzalka, 2008) *"A complicated system is (…) mechanistic in that all the parts, components, and their interactions are knowable. However, the structure and interactions in a complicated system may be difficult to understand, and the system may have multiple functions. Experts with appropriate qualifications can understand and analyse these systems with a high degree of accuracy. An understanding of linkages and interactions of system components is developed linearly, where an understanding of one element leads to an understanding of the next element. The impact of one element on another can be reasonably predicted. The relationship between cause and effect is linear. However, a single cause may have multiple effects, and a single effect may be the result of several possible causes."* (ICAO website - Human Performance page) Despite the fact that it may consist of a huge number of components, a system is merely complicated if a complete description can be given in terms of its individual constituents. (Adapted from Cilliers, 1998)
Complex system	Built of many elements, which may or may not be identical, cooperating together according to rules which may or may not be well defined, but that can also change with time. These elements are connected in a network pattern (e.g., one-to-many and many-to-one network thinking) and can interact to create nonlinear and emergent behaviours. Example: an airliner, a nuclear reactor, etc. (Adapted from Grabowski & Strzalka, 2008; Sturmberg, et al., 2016)

(continued on next page)

Complex system *(continued)*	*"A complex system is dynamic. The whole of the system is greater than the sum of its parts and components. Interactions between parts and components are diverse and nonlinear because everything is connected to, and depending on, something else. The behaviours of these systems may change in unpredictable ways. Analysis - such as causal analysis - of complex systems is not an effective method to improve system performance because the behaviour of the system cannot be predicted from examining the behaviour of its separate parts, and the system cannot be understood by only looking at one component or from one perspective.* *Complex systems often behave unpredictably or randomly due to the diversity of interactions within the system, the unpredictable nature of system components (such as humans or weather), and/or changing influences within the system. For example, an individual may change behaviour, adapting to internal influences, such as health or personal mood, as well as to external influences, such as environment or equipment. A complex system may exhibit unpredictable behaviour even though its performance may be defined by strict policies and procedures. Unlike simple or complicated systems, complex systems have the unique ability to learn and adapt, which can be attributed to the human component of the system."* (ICAO website - Human Performance page) *"In a complex system, (…), the interaction among constituents of the system, and the interaction between the system and its environment, are of such a nature that the system as a whole cannot be fully understood simply by analysing its components. Moreover, these relationships are not fixed, but shift and change, often as a result of self-organisation. This can result in novel features, usually referred to in terms of emergent properties."* (Cilliers, 1998)
Hazard	*"A condition or an object with the potential to cause or contribute to an aircraft incident or accident."* (ICAO Annex 19)
Method	A process or procedure to reach an outcome. A method typically belongs to a wider methodology. Example: AcciMap, STAMP, and FRAM are methods of the systems thinking methodology.
Methodology	A coherent ensemble of methods that share a common perspective on one or several underlying topics. Example: systems thinking is a perspective on complex systems that contains several methods to try and uncover their workings.
Simple system	Consists of a relatively small number of elements that act together according to laws that are well-defined and easy to understand (for instance, a pendulum, a clock, most mechanical systems, etc.). However, simple systems do not necessarily remain so and, under some conditions (e.g., disturbances, chaos), may behave in complex ways. (Adapted from Grabowski & Strzalka, 2008) *"A simple system is mechanistic, comprised of a defined number of components or parts which interact to accomplish one or a small number of known goals or functions. The behaviours of the system are fully predictable and do not change over time. Therefore, when the system is degraded or fails, cause is easily identifiable. The relationship between cause and effect is linear and clear. As such, these systems are straightforward to maintain and repair to ensure that they consistently meet their pre-identified performance standards."* (ICAO website - Human Performance page)
Socio-technical system	Involves complex interactions between humans, machines (hardware and/or software), and their environment. Examples: an airline, a hospital, a powerplant.
System	*"Set of components that act together as a whole to achieve some common goal, objective, or end. A system may contain subsystems and may also be part of a larger system."* (STPA Handbook)
Tenet	Characteristic of a system (i.e., not just of components but through interactions of components) that creates either safe or unsafe system behaviours.

Table 14 - Key terms and definitions

4.3 Literature, references

Ackoff. (1979). *The future of operational research is past.* Journal of Operational Research Society 30. Issue 2.

Aven. (2026). *A history of risk science. Concepts and principles of risk analysis.* Routledge.

Bill, Costello, Cattani. (2023). *Major aviation accident investigation methodologies used by ITSA members.* Safety Science. Volume 168.

Castellani, Gerrits. (2021). *Map of the complexity sciences.* Art and Science Factory, Inc. Retrieved from: https://sacswebsite.blogspot.com/2021/09/q-for-2021-version-of-map-of-complexity.html

Cilliers. (1998). *Complexity & postmodernism: understanding complex systems.* Routledge.

Cook. (2021). *How complex systems fail.* HindSight Magazine. Issue 31. Retrieved from: www.skybrary.aero and https://how.complexsystems.fail

Dallat, Salmon, Goode. (2019). *Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation. A review of the literature.* Safety Science. Volume 119. 266-279.

Davies. (2023). *The unaccountability machine. Why big systems make terrible decisions.* Profile Books.

Dekker. (2019). *Foundations of safety science. A century of understanding accidents and disasters.* CRC Press.

Emmons, Mazzuchi, Sarkani, Larsen. (2020). Mitigating Cognitive Biases in Risk Identification: Practitioner Checklist for the aerospace Sector. NASA Public Access. doi: 10.22594/dau.16-770.25.01.

Eurocontrol. (2014). *Systems Thinking for Safety: Ten Principles. A White Paper.* Retrieved from: www.skybrary.aero

Federal Aviation Administration. (2024). *Evaluation of System-Theoretic Process Analysis for Improving Aviation Safety. Final Report.* DOT/FAA/TC-24/16.

Fletcher. (2014). *Application of system theoretic process analysis to requirements and algorithms for a thrust control malfunction protection system*. Retrieved from: https://psas.scripts.mit.edu

Flinterman. (2025). *Managing safety in complexity. Making "working safely" possible between systems that speak different codes.* Unter Soziologen.

Grabowski, Strzalka. (2008). *Simple, complicated, and complex systems – The brief introduction.* Rzeszow University of Technology. Department of Distributed Systems.

Grant, Salmon, Stevens, Goode, Read. (2018). *Back to the future: What do accident causation models tell us about accident prediction?* Safety Science. Volume 104/ 99-109.

Hollnagel. (2012). *FRAM: the Functional Resonance Analysis Method. Modelling complex socio-technical systems.* CRC Press.

Hulme, Stanton, Walker, Waterson, Salmon. (2019). *What do applications of system thinking accident analysis methods tell us about accident causation? A systematic review of applications between 1990 and 2018.* Safety Science. Volume 117. 164-183.

Hulme, Stanton, Walker, Waterson, Salmon. (2021). *Complexity theory in accident causation: using AcciMap to identify the systems thinking tenets in 11 catastrophes.* Ergonomics. Volume 64. Issue 7. 821-838.

ICAO. (2024). *Safety Risk Management Methodologies. Aviation Risk Management Solutions (ARMS) and Event Risk Classification (ERC).* Version 1. Retrieved from: http://www.icao.int/smi

ICAO. (2022). *Safety Risk Management Methodologies. Bowtie - guidelines.* Version 1. Retrieved from: http://www.icao.int/smi

ICAO. (2024). *Safety Risk Management Methodologies. FRAM - Functional Resonance Analysis Method.* Version 1.0. Retrieved from: http://www.icao.int/smi

ICAO. (2023). *Safety Risk Management Methodologies. ISO 31000 Risk management - guidelines.* Version 0.4. Retrieved from: http://www.icao.int/smi

ICAO. (2022). *Safety Risk Management Methodologies. Specific Operations Risk Assessment (SORA).* Version 0.2. Retrieved from: http://www.icao.int/smi

ICAO. (2023). *Safety Risk Management Methodologies. STPA – System-Theoretic Process Analysis.* Version 1. Retrieved from: http://www.icao.int/smi

ICAO. (2023). *Safety Risk Management Methodologies. Use of the risk matrix.* Version 3.4. Retrieved from: http://www.icao.int/smi

ICAO webpage on systems thinking. (2024). Retrieved from: https://www.icao.int/safety/OPS/OPS-Normal/Pages/Systemthinking.aspx

Jackson. (2019). *Critical Systems Thinking and the Management of Complexity. Responsible leadership for a complex world.* Wiley & Sons, Inc.

Kim. (1999). *Introduction to systems thinking.* Pegasus Communications.

Le Coze. (2015). *Reflecting on Jens Rasmussen's legacy. A strong program for a hard problem*. Safety Science. Volume 71. 123-141.

Le Coze. (2017). *Reflecting on Jens Rasmussen's legacy (2) behind and beyond, a 'constructivist turn'.* Applied Ergonomics. Issue 59. 558-569.

Meadows. (2008). *Thinking in Systems; A Primer.* Chelsea Green Publishing Company.

Patriarca. (2025). *Navigating the FRAM. Mastering the FRAM for modelling complex socio-technical systems.* CRC Press.

Rasmussen. (1997). *Risk management in a dynamic society: A modelling problem.* Safety Science. Volume 27. Issue 2/3. 183-213.

Reason. (1997). *Managing the risks of the organisational accident.* Ashgate Publishing.

Reiman. (2026). *Safety in complex organisations. A cultural approach.* CRC Press.

Ribeiro. (2016). *A systems approach to the development of an aircraft smoke control system.* Retrieved from: https://psas.scripts.mit.edu

Salmon, Read, Hulme. (2022). *Systems and systems thinking.* In The Core Body of Knowledge for Generalist OHS Professionals (2nd ed). Australian Institute of Health & Safety.

Salmon, Stanton, Walker, Hulme, Goode, Thompson, Read. (2022). *Handbook of Systems Thinking Methods.* CRC Press.

Shorrock. (2026). *Humanistic Systems. Understanding and improving work and life.* Retrieved from: https://humanisticsystems.com

Sturmberg, Martin, Katerndahl. (2016). *It is complicated! – Misunderstanding the complexities of 'complex'.* Journal of Evaluation in Clinical Practice.

Swuste, Groeneweg, et al. (2022). *From safety to safety science. The evolution of thinking and practice.* Routledge.

Thomas. (2023). *Empirical evaluations of Systems-Theoretic Process Analysis in the aviation industry.* Retrieved from: https://psas.scripts.mit.edu

Transportation Safety Board of Canada. (2019). *Raising the bar on safety: reducing the risks associated with air-taxi operations in Canada.* Air Transportation Safety Issue. Investigation Report A15H0001.

Von Bertalanffy. (1952). *Problems of Life: An Evaluation of Modern Biological Thought.* Wiley & Sons, Inc.

APPENDICES

Appendix 1 – Origins of systems thinking

Engineers may excel at designing the safest and most efficient aircraft possible; however, some are occasionally tasked to also specialize in a sudden disassembly in flight. During much darker days of humankind, significant efforts were put in the research and development of anti-aircraft artillery systems that incorporated radar and faster computing capabilities in order to not only keep an aircraft at cruising speed and cruising altitude in their crosshairs, but also to hit the aircraft where it was likely to be mere seconds after firing[22]. Beyond the complexity of building such machines, even the transcription and resolution of this 'problem' on large black boards would not have been possible without integrating feedback loops. However, as the engineers and mathematicians quickly experienced during WW2, feedback loops can easily be too weak or too strong[23]. It is said that suggestions from the medical world helped to solve that issue[24] but also marked the beginning of a new research field - cybernetics[25] - that would soon gather some of the brightest minds in science (e.g., Norbert Wiener, Margaret Mead, Ross Ashby, Alan Turing, Arturo Rosenblueth, John von Neumann, Julian Bigelow, Stafford Beer, etc.).

As it turned out, many people coming from a wide range of disciplines such as medicine, biology, social sciences, and engineering had also experienced a similar epiphany while designing radar consoles, trying to break codes, treating shell shock, etc. during the war. These realizations sparked their imagination and interest in meeting people from other fields to research how information could be quantified and theorized. With the return of peace, they could finally gather to make progress. However, it can be argued that the cybernetic revolution that quickly followed largely failed to achieve all the fundamental research it was initially set to do because it was too successful at finding practical solutions and commercial applications to widespread problems of communication and control in biological, social, and/or technological systems. Although the first half of the 20th century had already seen a significant increase in the range, quantity, quality, and speed of industrial production, it is incomparable to the second half of the century, where technological breakthroughs from WW2 and cybernetics (e.g., information theory, microprocessors, digital computers, etc.) fostered further progress, innovation, and mass production of unprecedented magnitude.

This short historical detour in the mid-1900s is only meant to provide the foundations of two axioms relevant to safety management:

1. Systems thinking emerged from attempts to solve practical and pressing problems in many domains, all related at their core to the transmission of information. This quickly provided both strong theories (on information, systems, complexity, etc.) and practical solutions, but also snowballed to the point where…
2. Technology frequently outpaced our degrees of understanding and control on these innovations.

Unfortunately, history is replete with industrial accidents illustrating the second axiom. Following decades of major disasters and erosion of public trust in government and institutions, the tipping point was achieved when a brand-new nuclear power reactor vented radioactive gases and nearly melt down at Three Mile Island (Pennsylvania) in March 1979. To a large degree, modern safety management owes a lot to the strong response of the international community that assembled and funded safety scientists and human factors specialists to identify better ways to manage high-risk industries (see figure 1). However, in the process of understanding what had happened, the various participants gradually coalesced into either one of two groups with different views on accident causation. This led to the emergence of two complementary schools of thought on 'human error' and system safety: the cognitive psychological perspective (led by Reason, et al.), and the joint cognitive systems perspective (led by Rasmussen, Woods, Hollnagel, Cook, et al.). Both worldviews claim to embrace systems thinking and have already positively

[22] The speeds and distance between the different objects involved (stationary or in motion) do not mount a simple ballistic problem. Moreover, aircrews obviously didn't consent to be shot at, and legitimately took evasive action that also had to be integrated when modelling trajectories.

[23] Since the gunsight moved to follow an aircraft, inputs changed, new information was sent to the servomotors, and the gun turret moved again. Either the gun trailed behind the aircraft (i.e., feedback loop too weak) or overcorrected and oscillated around the target (i.e., loop too strong).

[24] The suggestion was to interpret this engineering problem as equivalent to symptoms of brain injury known as ataxia and the intention tremor.

[25] Cybernet-*ics* comes from the Ancient Greek κυβερνήτης (*kubernḗtēs*), used for the person who steers a ship by giving orders to the oarsmen. For further details about the cybernetics (r)evolution but without pages full of equations, refer to Davies (2023, see reference in 4.3).

contributed to safety improvements. However, they're neither interchangeable nor mutually exclusive: both schools of thought approach systems thinking in ways that are largely compatible but also partly incompatible. Considering the prevalence of the cognitive psychological perspective in aviation and the fact that the latest risk management methods (e.g., STAMP, FRAM) are rooted in the joint cognitive systems perspective, it would seem prudent that any safety professional dealing with today's systems would be at least aware of both perspectives, and preferably conversant with the strengths and limitations of each, in order to suitably frame and positively influence safety issues by using the most appropriate analysis and management tools.

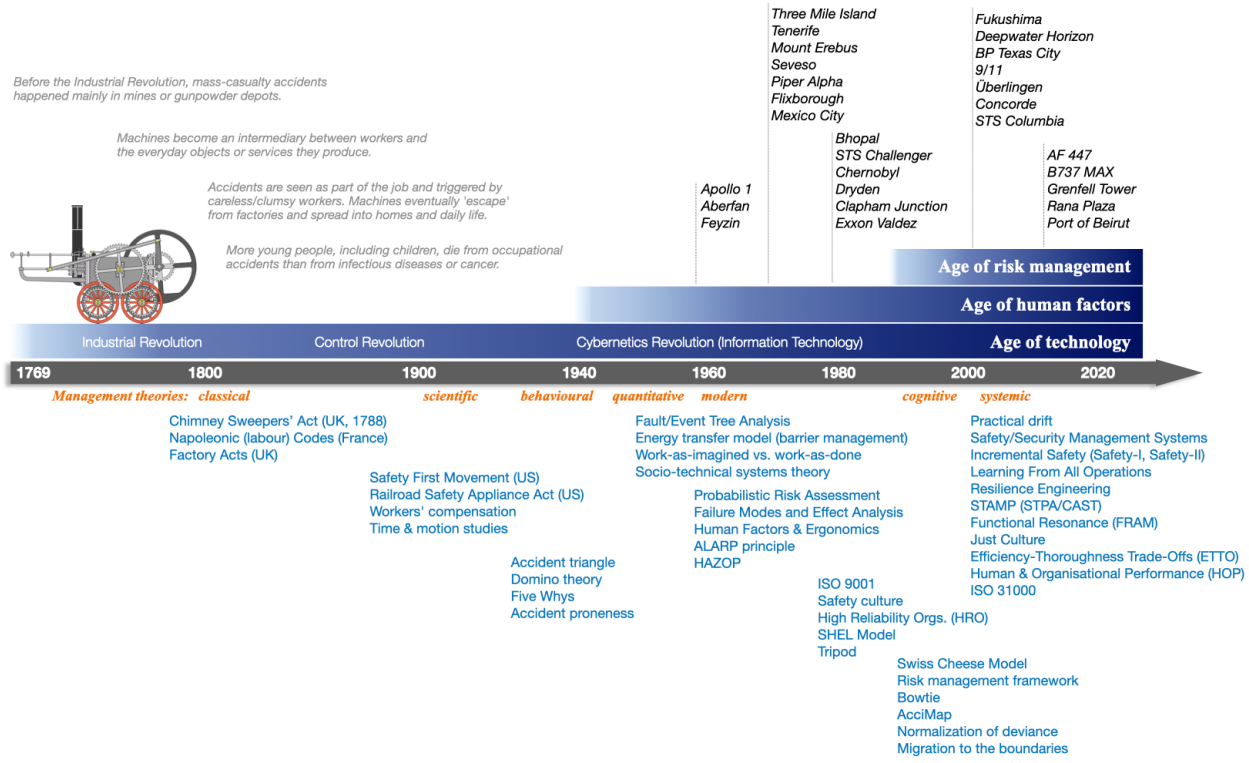

Figure 1 – Overview of significant accidents, concepts, and developments in both occupational and process safety

Systems thinking often uses notions such as vertical integration, practical drift, or migration of practices, among other seemingly cryptic concepts. Indeed, little can easily be understood without prior knowledge of research conducted on complex socio-technical systems in the second half of the 20th century.

Risk management in a dynamic society: a modelling problem

For many years, Jens Rasmussen and his colleagues (e.g., Jensen, Hollnagel, etc.) closely observed engineers conducting their daily work at the Danish nuclear research laboratory founded by Niels Bohr in Risø. Through their empirical studies on human-machine reliability, they built the view that an analytical framework encompassing a wide range of dimensions was needed to make sense of the complex socio-technical systems that had pervaded both the workplace and daily life.

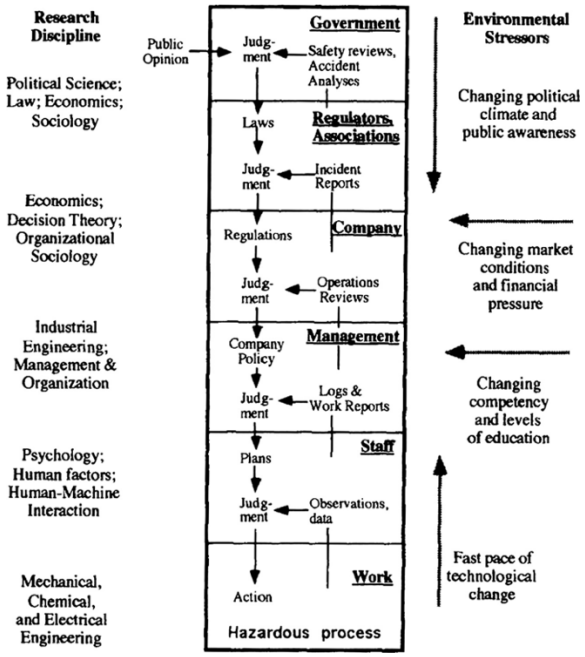

Figure 2 – Rasmussen's socio-technical perspective

Complex systems are more than the sum of their parts, they're the product of their interactions. Therefore, they cannot be understood by only analysing their components separately. Rasmussen's innovative framework combines different levels made of actors, objects, and tasks that are hierarchically stacked up, with government at the top and hazardous work processes at the bottom. All these levels are connected through feedback loops of information, scientific disciplines, and environmental dynamics. These relationships are linked to explain causal ties. They also underline the critical role of feedback control loops.

Looking vertically across the layers of a system may sound obvious today. However, the use of such holistic perspective to understand and prevent accidents was rather uncommon when Rasmussen finalized and published his models in 1997. For instance, Reason and Wreathall published the first version of what became known as the 'Swiss Cheese Model' that same year.

Rasmussen's perspective provided the foundations for different models and methods to investigate accidents (e.g., AcciMap, STAMP/CAST) and to manage risks (e.g., STAMP/STPA or FRAM). Although it helps painting the 'big picture' in a structured, holistic way, this model lacks precision on the dynamics at the workers' level. Hence, Rasmussen introduced a second model also based on years of observing daily work.

Performance variability and migration towards the boundaries

In this second model, Rasmussen zeroes in on what occurs in daily operations. Once again, the focus is on the functions and interactions rather than on the components themselves. More specifically, Rasmussen is not interested in violations or in 'human error' (that he considers the be the inevitable by-product of unsuccessful but necessary experiments to achieve system goals when confronted with daily variability). Instead, his focus is on the mechanisms that generate behaviour(s) in the actual, dynamic work context.

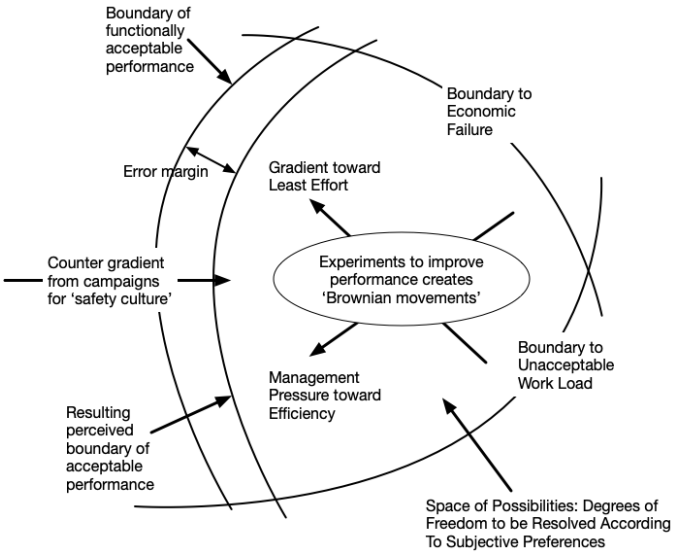

Figure 3 – Rasmussen's dynamic risk model

Starting with three outer curves, Rasmussen represents the workspace of human actors (in other words, the workers and/or their organisations) as circumscribed by three boundaries that should not be crossed:

- **Functionally acceptable performance:** crossing this boundary equates to making an error or triggering an accident. However, since there's always a margin between degraded safety and an accident, a fourth curve is drawn very close to the actual boundary to represent a space for making errors without dire consequences (the error margin).
- **Economic failure:** crossing this boundary would lead to financial distress and bankruptcy.
- **Workload:** crossing this boundary would mean that human actors find themselves without sufficient time and/or resources (at individual and/or organisational level), leading to unreasonable or even inhumane efforts while striving to achieve system goals.

The purpose of this model is not to precisely pinpoint where human actors (i.e., organisations or even an individual) are at any particular moment or how close they are from an accident. Instead, its purpose is to draw attention to, and collectively make sense of:

- the human actors' **degrees of freedom** to experiment and improve performance,
- the **space of possibilities** (or 'safe operating envelope'[26]) that is created,
- the **gradients** that will be applied based on subjective preferences (e.g., a dangerous loss of separation between two aircraft might generate a strong gradient away from the boundary of acceptable performance by launching a major campaign against runway incursions, or a worsening financial situation might force a maintenance organisation to consider reducing or selling some of its activities to remain in business), and
- the perpetual motion and necessary adaptations (called **Brownian movements**, in reference to physics) of human actors who must respect various objectives and constraints in order for work performance to be successful in a VUCA world or even in a BANI one.

[26] For further details and an example of how this model has been translated in aviation, refer to the study and investigation report A15H0001 by the Transportation Safety Board of Canada (2019, see reference in 4.3).

Appendix 2 – Map of the complexity sciences

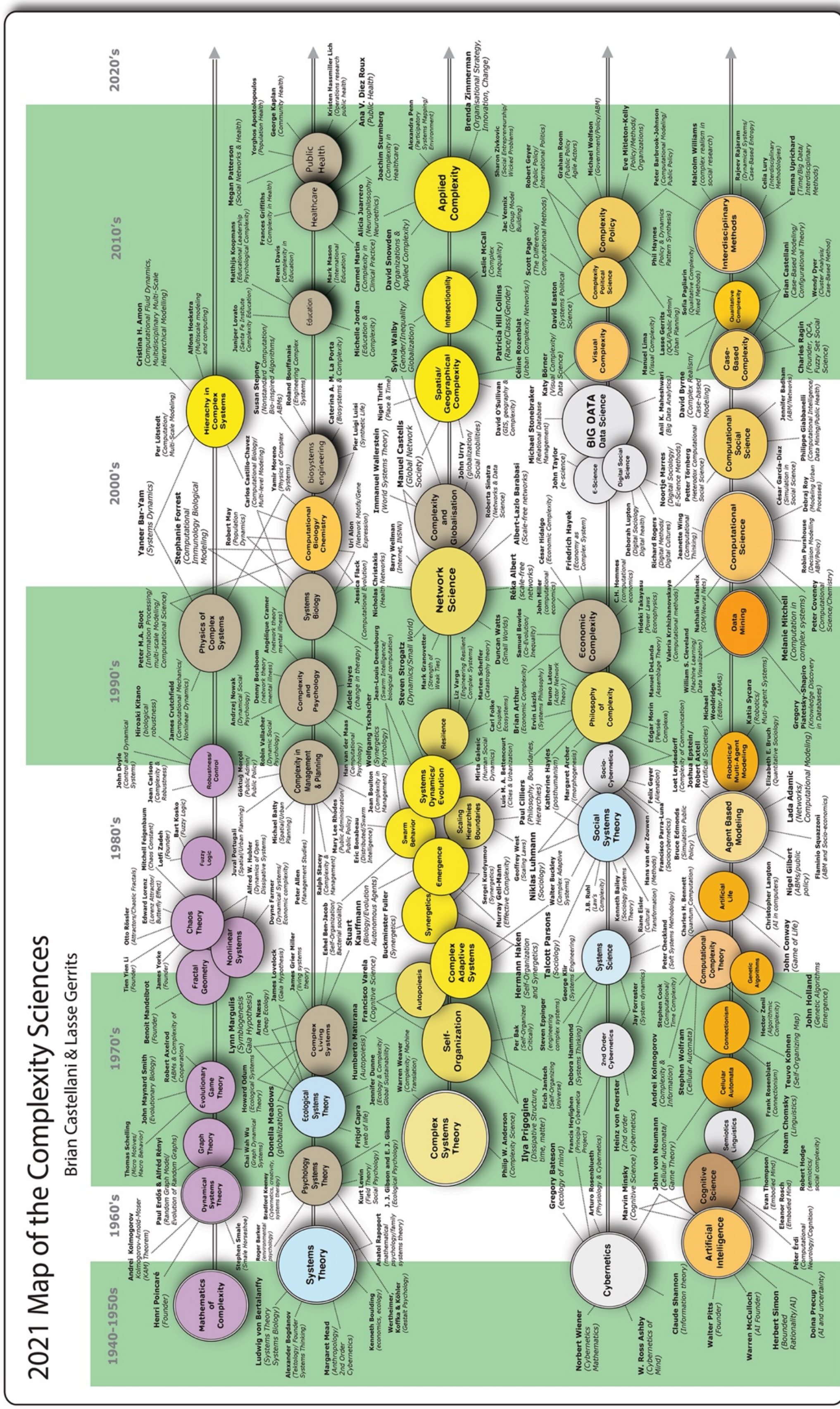

Figure 4 – Map of the complexity sciences (Castellani and Gerrits, 2021)

Appendix 3 – Existing sets of systems thinking tenets

Table 15 provides an overview of systems thinking tenets found in the literature, starting with Rasmussen's seminal work about modelling risk management in (complex) sociotechnical systems. Subsequent sets expand, refine, and build on his perspective, with the benefit of additional experience and insights.

Tenets were positioned next to each other across two or more columns whenever commonalities can be found. However, since systems thinking is not monolithic, it should not be assumed that each horizontal line necessarily represents a single specific idea or concept expressed in either identical or different words across all columns. In the interest of simplicity and brevity, the table was not designed with blank cells and arrows to graphically indicate the evolution or lineage between these sets of tenets.

For instance, although Eurocontrol's "field expert involvement" (first line) is somehow related to "vertical integration" found in the other three sets of tenets, it is different. Similarly, although Rasmussen's "multiple actors and levels" (second line) is related to the performance variability listed in the other three sets (and to Eurocontrol's "field expert involvement" as well), it is a different principle.

Rasmussen (1997)	Eurocontrol (2014)	Grant, et al. (2018)	Salmon, et al. (2023)
Vertical integration	Field expert involvement	Vertical integration	Vertical integration
Multiple actors and levels	Performance variability	Performance variability	Performance variability
Multiple contributing factors	Emergence	Emergence	Emergence
External pressure	Resources & constraints	Constraints	Constraints
Feedback	Interactions & flows	Feedback loops	Feedback loops
Migration of work practices at multiple levels	Trade-offs	Coupling	Tight and loose coupling
Erosion of defences through migration of work practices	Demand & pressure	Normal performance	Normal performance
	Local rationality	Decrementalism	Decrementalism
	Equivalence (of successes and failures)	Contributions of the protective structure	Contributions of the protective structure
	Just culture	Sensitive dependence on initial conditions	Sensitive dependence on initial conditions
		Linear interactions	
		Non-linear interactions	
		Modularity	
		Unruly technologies	
		Functional dependencies	

Table 15 – Sets of systems thinking tenets