# White Paper: Safety in the Air begins with Quality on the Ground

## A New View for Safety in ATM


**Authors:** Huw Ross

Roger Dillon



**Version:** Issue 1.0

June 2021

# Executive Summary

## Setting the Scene

The aviation industry is considered ultra-safe; however, accidents still occur that result in the loss of life. The total numbers of fatalities are considered low compared to other industries, but numbers alone do not help us understand the actual level of safety and what that means for tomorrow with any confidence. We should not become complacent and should continue to seek out new opportunities to understand and improve Flight Safety.

The ATM sector has an opportunity to identify and realise the benefits of the digital era within the delivery of traffic management services. The aviation system of tomorrow will look very different to today. New aircraft types using new alternative fuels, flying in urban and rural environments require us to transform how we understand safety in the air and on the ground. Traffic management services should extend to these new vehicles but at a scale unseen in the current ATM environment. The ATM sector will need to innovate. The fundamental purpose of an ANSP does not need to change. However, we have the opportunity to reimagine the services we provide and how we provide them to airspace users of today and tomorrow to help protect all those in the air and on the ground from harm.

## Safety in ATM

Right now, there are two important questions that continue to be debated:

**Question 1: Is our approach to safety in ATM fit for purpose to manage our future challenges?**

**Question 2: Can we clearly define what value our safety efforts provide to ATM service delivery or to flight operations?**

In this white paper we explain why we think **the answer is No** to both questions. We layout our vision for the future to address the shortcomings in our current approach. We start by reminding ourselves of the basic principle of safety – **protecting humans from harm**. This is usually managed in organisations by Occupational Health and Safety (OHS) practices. In ATM, safety has a different focus. The core purpose[1] of an ATC service is **to prevent collisions while expediting and maintaining an orderly flow of air traffic**. As such, our understanding of safety has evolved **to align with the needs of a service industry one step removed from the purpose of protecting people from harm.** We have adopted Systems Safety techniques to help us in ATM by addressing perceived limitations in OHS techniques.

We discuss how the **adoption of Systems Safety practices has not achieved the outcome the ATM sector desired.** The approach is applied without context of how to best prevent collisions or how to appropriately consider the role of the human within the system. As a consequence, our safety efforts appear to have lost some of their impact within air traffic service operations.

Looking to the future, we discuss **how the ATM industry is transforming to achieve scalability and resilience goals,** and the recent ATM regulation changes that facilitate that process. We examine recent initiatives and good practice from within the industry and from safety thought-leaders. For instance: analysing the widely held view that safety is measured by the absence of safety; how techniques from resilience engineering provide opportunity for change; and finally, that safety is an emergent property of delivering quality services.

## *Blueprint for Aviation Safety*

Reflecting on our learnings from this discussion we set out eight principles that should be considered in the development of new practices within the ATM sector to address safety. The principles provide a new view of safety in ATM that will help us remain relevant as our industry **welcomes new entrants** and to **realise the benefits of digitalisation in delivery of new services**.

| Title | Principle |
|---|---|
| **01 - Flight Safety** | Flight Safety should only be evaluated (safety risk) and measured (safety performance) at the level where the harm can occur. |
| **02 - Total System Safety Approach** | A total system safety risk picture should be available to all service providers to inform their service delivery activities in support of Flight Safety. |
| **03 - Safety Support Assessments in ATM** | Safety support assessments should be used to document service effectiveness by outlining a service providers' contribution to Flight Safety. |
| **04 - Assurance Levels** | Assurance level methods should be used to design a resilient system as a platform for delivering ATM/ANS services. |
| **05 - System Analysis Techniques** | System analysis techniques should be used to help match the capabilities of the machine and the human in the design of the ATM system, with emphasis on how the human adapts to handle variability within the system. |
| **06 - Service Effectiveness Criteria** | Service effectiveness should be defined in terms of service risk and service performance and follow the same criteria. |
| **07 - Quality Management Practices** | Integrated management systems based on a service lifecycle process approach should be used to define and manage the working practices that support service delivery. |
| **08 - Culture as a pillar of management systems** | Service providers should continue to promote a culture that supports trust, learning, open reporting and sharing of information across the entire aviation industry to aid the continuous improvement of Flight Safety. |

## *Looking to the future*

The 'number one' principle in our blueprint is that Safety should only be evaluated and measured at the level where harm can occur. It recognises that safety cannot be credibly evaluated by the ATM service provider; it is only those that use the services provided that can evaluate safety risk. Airspace users understand the effectiveness of the services they use and focussing on effectiveness of ATM services is what the ANSP community should do to remain relevant. To achieve this, we should prioritise our efforts on the design and operation of resilient services using a quality management approach supporting traditional safety management methods. **We highlight that safety is not something we do but rather an outcome of doing many different things well.** Improving safety requires us to improve the quality of how we deliver our services. This approach has been used to great success in other process and manufacturing industries and should be followed in ATM. This will require adoption of integrated management systems within ANSPs that serve as the vehicle for everyone in the organisations to collaborate on service delivery.

# Evolution of Safety in ATM

***The purpose of ATM is to prevent collisions while expediting and maintaining an orderly flow of air traffic. However, it was not until the 1990s that formal safety methods began to be introduced to manage the safety of the ATM services. Since then, our safety methods have evolved to match the needs of the system; but there is still a long way to go. The process of learning should continue.***

## *Freedom from Harm*

It has been a priority, and a legal[1] requirement in some countries, for every organisation to protect its employees from harm and to ensure that they can carry out their work with the confidence that they are unlikely to get hurt. In other words, **the freedom to perform their job safely**.

In every industry, Occupational Health and Safety (OHS) is afforded the highest priority. Naturally, the type of industry that people work in, and the tasks that they perform expose them to have varying levels of risk of injury. Therefore, **different techniques are available to OHS practitioners to help them ensure safety**.

It became apparent to ANSPs in the early 1990s that the safety of ATM services they provided should be considered explicitly. **These services are essential to airspace users and provide mitigation against the risk of aircraft accidents**. Safety still provides 'freedom' but in this case, not just to the employees of the organisation. The definition of Safety is now extended to cover the travelling public, flight crew, airport operators and the general public; referred to in this paper as Flight Safety.

**ATM followed other high-hazard industries** (e.g. nuclear and rail) and looked to *System Safety*[2] rather than to OHS as the source of appropriate techniques. Primarily because *System Safety* supports assessment of complex process-based systems with multiple stakeholder interfaces.

The decision to separate OHS and *System Safety* practices within the ANSP community seemed appropriate, partly as OHS was thought to dilute the focus on Systems Safety. However, **the separation resulted in lack of attention on the people that we are trying to protect from harm**. Additionally, we struggled to understand the role of the people delivering the air traffic services. Together, this contributed to the ATM safety community's ability to gain relevance within air traffic operations.

***Learning Point 01***
***Returning our focus to protecting humans from harm will provide valuable input into defining our future approach to safety in ATM.***

## *Introduction of System Safety*

The first attempts to introduce *System Safety* methods into the ATM community **concentrated on the equipment** – as change programmes were dominated by the introduction of new equipment and software tools to support ATC service delivery. Hazards were identified **for failure modes of the equipment without context of how it was used, and safety assurance focused on the contribution of the equipment to those hazards**.

[1] The UK Health and Safety at Work act introduced in 1974.

[2] Nancy Leveson - Safeware: System Safety and Computers (1995) and Engineering a Safer World; Systems thinking applied to Safety (2011).

The issue was the **scope of the 'system'**; in effect it **was limited to the 'machine' elements only** and **little effort was invested in the 'human'**. Furthermore, the scope of the system **rarely extended to those elements outside the organisation's boundary** of responsibility, not properly considering the contribution that other stakeholders played in the delivery of safe air traffic services.

***Learning Point 02***
***The scope of the system should be addressed; ensuring all actors the contribute to Flight Safety are included is critical to understanding safety in ATM.***

## The Evolution of Safety Assessments

Over time the approach to safety assessments evolved to consider hazards defined at the interface between the machine and the human i.e., the display of information at the controller working station to air traffic control staff. Workload or the impact on the inability to provide air traffic services started to be used to describe the outcome of a failure of information display. **Including the human in this context was a significant step forward and is still the benchmark for safety assessments in most ANSPs**. Increasingly, **human factors assessments** are now regarded as essential in the most mature organisations. Ergonomic assessments of the working environment and task analysis of operating practices has helped us improve how we introduce changes into the operation. Whilst significant progress has been made, it is noted that these are often standalone assessments and not integrated with the safety assessment activities.

Safety assessments **primarily followed a numerical approach to setting safety targets on equipment**. This meant that safety assessments were more like reliability assessments. The **confusion between reliability and safety still continues today** in that we believe understanding the failure rate of equipment has a relationship to a level of safety in the operation. The focus on reliability meant that the functional requirements for the equipment were rarely considered. **Functional requirements provide an important opportunity to influence what the system does** and, notably, to influence the design of the machine to support the human in operations.

The reliability of the equipment, or lack thereof, increasingly became recognised as the driver of service 'delay' performance, rather than safety, as major equipment outages occurred causing disruption to airspace users. What are considered low safety consequence outcomes relating to loss of ATM equipment functionality are often noted as having high consequence service outcomes. As a result, **'Safety Cases' at the equipment level turned into general assurance cases** covering service outcomes such as delay in addition to safety. However, risk classification schemes struggled to identify appropriate service outcomes for the business within the severity scheme.

More recently, barrier model techniques for safety assessment **have turned from theoretical studies into applied techniques** within a small number of ANSPs. These provide a new opportunity to understand safety from a system perspective by analysing the different barriers that are in place to prevent accidents. Work on barrier models continues to develop in ATM, constrained by the limitations that linear models have on representing complex socio-technical interactions where (1) many functions work in parallel, and, (2) how functions are used is dependent on the specific scenario. Whilst the practical application of *System Safety* in ANSPs' change management programmes continues to evolve, the defined SMS processes have not advanced with the same thinking, often remaining linked to regulatory requirements rather than aligning with the needs of the business.

***Learning Point 03***
***Safety and assurance methods should be appropriate for the service context and the service outcomes the organisation aims to achieve.***

## Use of Assurance Levels

The use of assurance level methods are common in ATM. This is where a set of 'design' requirements are defined for different levels of criticality of function. For high - criticality functions the design requirements are stringent and 'highly recommended' by the standards. For low criticality functions there are fewer and less stringent requirements to implement. Fulfilment of the requirements is focused on expertise and judgement supported where appropriate by numerical analysis. The most effective example of this is **the use of software assurance level (SWALS)** in software assurance standards. **Similar approaches for procedures (PALS) and humans (HALS)** were proposed by Eurocontrol in the early 2000s **but did not progress into common usage**.

The most recognised approach to assurance levels, outside software assurance, is within the international standard IEC61508 [3] which sets 'integrity levels' for functions within systems and provides guidance on architectural features that should be considered.

***Learning Point 04***
***Assurance level methods provide practical qualitative techniques to assess the effectiveness of the system and should be considered further in place of quantitative safety assessment techniques.***

## Safety Performance Measurement

Our understanding of safety performance in ATM is based on measuring proxies for an aircraft accident. The most commonly used proxy is the 'loss of separation' based on aircraft infringing into the airspace of other aircraft or a 'runway incursion' within an aerodrome. It is frequently observed that safety performance is primarily measured by the absence of safety – counting things that go wrong rather than what goes right.

More recently, ANSPs have started **analysing information from mandatory and voluntary reporting schemes and using other available data sources such as flight track data**. In these situations, causal factors have been identified and analysed **to help understand current performance at a more granular level to proxies** and **to allow us to target new mitigation to address vulnerabilities within the system**. This causal factor approach is a form of leading indicator analysis but the predictive validity, i.e., the strength of the relationship between the causal factor and the worst consequence, is in most cases low. **Identifying 'weak signals' in our operation to lead our performance improvement activities remains challenging and still in its infancy**.

Furthermore, the way we evaluate safety risk as a result of changes to the design of the system uses a different set of criteria to those by which we measure safety performance. Inevitably, **this leads to difficulties in showing that investments in safety lead to a reduction in safety risk**. Indeed, the business case for any investment in safety is very difficult to make in financial cost benefit terms.

Lastly, **the events that we monitor to determine safety performance nearly always occur when the equipment and procedures are *working-as-designed***. Similarly, it is common to see NO safety events (as described by the current proxies) following failures of the equipment. For instance, a total loss of controller-pilot communications often does not result in a loss of separation owing to the resilient design of the system and the flexibility provided by the human.

***Learning Point 05***
***New methods are required to understand safety performance using indicators that reflect the presence of safety. Any new method should use the same criteria to evaluate safety risk.***

[3] IEC61508 - Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems

## *Safety Management Systems*

Application of Safety Management Systems (SMS) in ANSPs came into regular usage in the late 1990s. This initiative was industry driven in response to a number of high-profile accidents in aviation and other safety related industries. The initial SMS was the vehicle for formal establishment of organisational working practices and was the basis for the topics discussed above.

It is **now a regulatory requirement for service providers to have an SMS** and the majority of ANSPs have implemented one and are actively improving its maturity. The **SMS Manual is the most common document used to describe safety management practice**. However, one recognised weakness to implementation is that the **practices are not well understood by the organisation** and in some cases only considered applicable to those in the safety department.

The challenge organisations face is to **take the SMS Manual off the 'dusty' shelf and promote its objectives across different community groups**.

Successful implementation of an SMS remains closely linked to management commitment to safety. Our understanding of safety accountability has improved significantly and senior managers in operational, technical and support functions (including human resources and finance) are actively shaping their departments activities to contribute to safe operations. Our leaders are also becoming more visible in the organisation and exhibiting safety leadership behaviours in formal and informal situations. Leadership remains a key enabler for fostering a positive culture that promotes sharing, knowledge and trust at all levels of the organisation.

Just Culture principles empower all staff to engage in safety management activities and to raise attention to safety concerns without fear of repercussions. However, the principles are not consistently and universally applied. Organisations are seeking new methods to communicate Just Culture with input from systems-thinking principles and specifically better understanding the role the human plays in the system. This is discussed further in Section 4. Psychological safety is the term used in other industries to describe an equivalent concept to Just Culture. Learning from other industries may provide useful insight into our continued promotion of Just Culture in aviation.

The scope of the SMS is today based on the regulatory framework defined by ICAO. A brief background to evolution of SMS regulation is explained in the next section. **The most important observation we make today is that the activities that we perform in our organisations to contribute to safe operations are not reflected within the regulatory framework**.

Integrated management systems are promoted in our industry as the next step in organisational maturity. This will help us better understand the scope of activities that contribute to safety. This also helps us understand the relationship with other business drivers such as information security and human performance that also play a role in delivering effective services.

***Learning Point 06***

***The safety management system should reflect the activities that the organisation performs to contribute to safety and the relationships to other business drivers (e.g., information security and human performance).***

# Role of Regulation in ATM

***Regulation, and compliance to it, has a major influence on our approach to safety and the activities we allocate our resources to. The equipment focus discussed above, and the requirements for quantified risk assessments have been largely driven by regulation. The absence of a systems approach[4] to safety has hindered progress in improving safety maturity in favour of regulatory compliance.***

## Background to SMS in Regulation

Eurocontrol Safety and Regulatory Requirements [ESARR] 3 formalised need for an SMS for Eurocontrol Member States in 2000. ESARR 3, Use of Safety Management Systems by ATM Service Providers, was transposed into European Community law by Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services, and subsequently by (EU) No 1035/2011 of 17 October 2011 and (EU) No 2017/373 of 1 March 2017, the last of which entered into force on 2 January 2020.

The ICAO Annexes contained guidance for safety management prior to the introduction of Annex 19 in 2013 which brought together the guidance from other Annexes into a standalone Safety Management annex and raised the focus on SMS to a standard.

There is strong alignment between the requirements for Safety Management Systems in ICAO Annex 19 and the European Rules presented in (EU) 2017/373. The ATM sector also continues to drive best practice in the industry by the publication of the CANSO / EUROCONTROL Standard of Excellence in Safety Management Systems.

## Quantification of Safety Risk

The ESARRs and more recently the ATM/ANS Common Requirements regulation, **require the quantification of safety risk, where practicable**. *Where practicable* has been interpreted as a non-negotiable requirement and safety assessments are usually driven by numerical safety targets. While numerical assessments are valid for random failures of equipment (e.g., loss failures), they are not credible for software or human performance. This means that quantified analysis of safety risk is not credible in complex socio-technical systems.

## Safety Risk at Accident Level

Recent developments in Regulation (EU) 2017/373 set a requirement to conduct a safety risk assessment in the context of the accident outcomes within aviation. At a conceptual level this requirement aligns with the views of the authors that safety should be expressed in the context of harm to humans. On a practical level, **Regulation (EU) 2017/373 does not recognise the complex stakeholder relationships within the total aviation system**.

Similarly, defining meaningful proxies for assessing the ATM/ANS contribution to an accident sequence are difficult, if not impossible, to justify. As discussed above, proxies are generally connected to the absence of safety events.

***Learning Point 07***
***Performance indicators used in ATM should be related to the delivery of the operational service rather than in the context of an accident sequence.***

[4] A systems theory approach treats safety as an emergent property. Such property can be controlled by a set of constraints related to the behaviour of the components of the system. According to the systems approach accidents occur when the components interact and those interactions violate the constraints (Leveson, 2002)

**The regulation continues to require quantified risk assessments where possible, however, it remains debatable whether the requirements of the regulation can be achieved in a qualitative way let alone quantitative**. The complexity of the system and the cooperation between actors required to perform such an assessment inhibits the opportunity to assess safety risk in this way. In our experience, **organisations are inconsistently interpreting the requirement of the regulation, and the value it brings to the safety community is limited**.

***Learning Point 08***
***ANSPs cannot credibly evaluate safety risk at the point where harm occurs without input from other service providers in the total aviation system.***

***Learning Point 09***
***Regulation should provide clarity that qualitative judgement-based approaches are the most credible while quantitative safety risk assessments are not appropriate at the system level.***

## Software 'Safety' Assurance

A prime example of where regulation did not achieve the objectives it intended is highlighted in the rules for software safety e.g., those documented in European Regulation (EU) 483/2008 which in 2020 was re-badged as an Acceptable Means of Compliance (AMC) to Regulation (EU) 2017/373. The rules requiring the development of a software safety assurance system are not helpful in organisations that often do not develop their own code. Furthermore, the rules compound a view that focuses too much effort on the equipment rather than how it is used to provide a service.

Whilst the development of robust software should remain a critical focus area for any industry using software intensive systems, our observation is that the focus on software safety by the software community has taken safety resources away from other critical tasks when application of engineering resource would be more appropriate. **The role of the human in the context of the system function should be the priority for any safety activity**.

***Learning Point 10***
***Regulation should ensure that all system elements and the assurance activities to analyse them are conducted at the system level in the context of service delivery.***

# New Service Delivery Models

***The future of ATM service delivery has progressed rapidly in recent years as ANSPs re-think their operating models and seek opportunities to provide new services to the aviation community and create a flexible technical architecture to enable the faster adoption of new information sources.***

## *Service Orientation in ATM*

Goals for transformation of the ATM sector are being set through the ICAO Global Air Navigation Plan (GANP) and through regional transformation programmes such as Next Generation Air Transportation System in the United States and the Single European Sky in Europe. **Service orientation is now the target for global and regional transformation programmes** and is recognised as a key enabler to create scalable and resilient ATS services within the ATM network.

Service orientation principles **have already been adopted by some ANSPs** in the design of their future system architecture. There is recognition that there are opportunities to buy in capabilities from external parties rather than developing and maintaining the capability internally. The opportunity now being explored is the commoditisation of the entire service stack (i.e., all the capabilities that an ANSP needs to function). The belief is that scalability can be achieved through creating common or centralised services (e.g., surveillance-as-a-service) that simplifies the sharing of data across sovereign borders such that the ATS provider in one country could provide ATS services in another. Whilst there is yet no credible path for this to be achieved at any scale, **we expect to see national service providers taking the benefit of new IT tools and practices to achieve flexibility within their own borders**. Understanding the service delivery chain is essential to understand what it means in terms of safety – as organisations that contribute technology will be further separated from the organisations that ultimately use the information for ATS provision.

***Learning Point 11***
***The approach to safety in ATM should align with the air navigation service orientation strategy.***

***Learning Point 12***
***New approaches are required to mitigate the effect of the fragmentation on the service delivery chain (aka the safety chain) including approaches to maintain the organisational culture required to create trust and the open sharing of information.***

## *Quality Management; Safety as an Emergent Property*

The role of an organisation's quality management system in supporting service delivery provides a significant foundation to our work on safety. The focus on Quality, in effect, represents the integration of all the management systems functions that the service providers have chosen to implement (e.g., OHS, Flight Safety, Environment, Security, Information Security, Systems Engineering). **The role of Quality is to setup the management system such that the working practices in the organisation required to achieve the desired service outcomes are documented and effective**.

ANSPs are preparing for a service orientated strategy by adopting good practice for service management within their Quality Management Systems.

The service management principles within ISO20000 and the guidance from ITIL[5] provides an appropriate starting point. ITIL provides practical guidance on service delivery using a simple service lifecycle. The stages are:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement (a transversal stage).

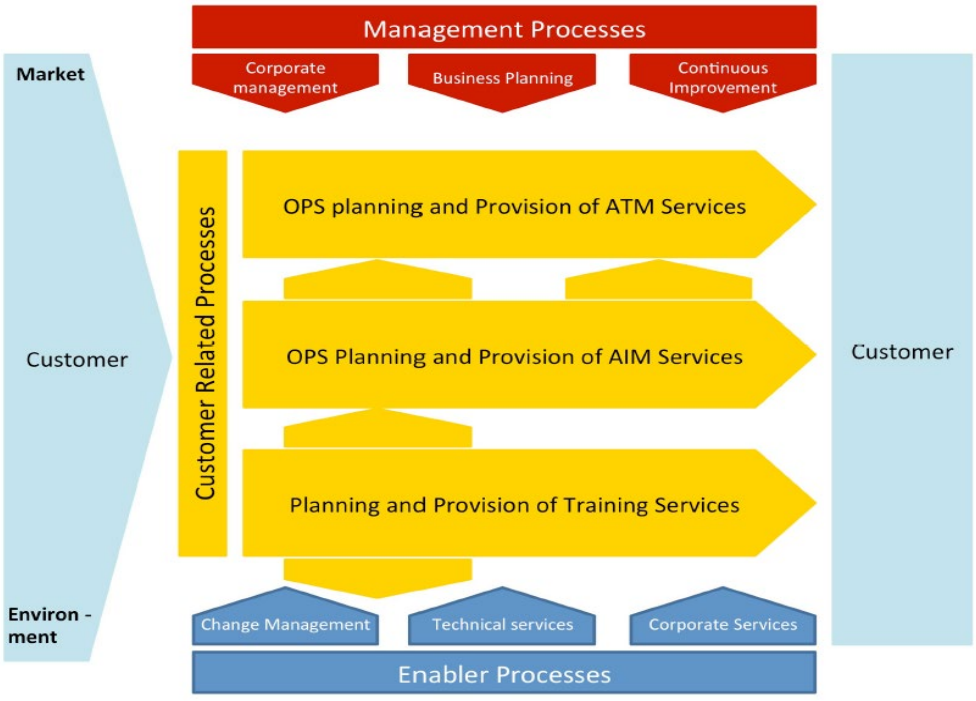
The CANSO Framework for ANSP Management Systems[6] shown in the figure below provides a Management System framework that allows you to host your value chain as 'customer related processes.' **The ITIL lifecycle is an ideal structure for an organisation's customer related processes.**

For **the safety community to make progress it should take an active part in the development of Quality Management practices** and the design of integrated management systems. An outcome of this approach is to recognise the many existing practices that contribute to safety that are omitted from a regulatory based Safety Management System construct. **In summary, safety is not something we do but rather an outcome of doing many different things well**.

***Learning Point 13***

***Integrated management systems using a service lifecycle process approach should be considered to ensure all the organisations activities, and the relationship between them, are understood in the context of delivering effective services.***

*Figure 1– CANSO Management System Framework*




[5] https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[6] CANSO Framework for ANSP Management Systems (2014)

## *Regulation Enabling the Future*

As a positive step, service orientation is recognised in the ATM/ANS regulations in Europe to a certain extent. Regulation (EU) 2017/373 introduces the concept of 'Safety Support Assessment' for service providers that do not deliver an Air Traffic Service [7] . This is **a really positive move and creates a foundation for further progression**. As the implementation of a service orientation approach matures the regulation will deliver benefit for ATS providers. This will also enable the introduction of **ATM Data Service Providers**, a concept introduced in Europe through the SESAR Airspace Architecture Study report [8] and further developed in studies by the European Commission [9] . The general trend to un-bundle traditional ANSPs services into discrete elements will require further development in regulation and SMS practices to ensure the benefits and impacts are managed.

***Learning Point 14***

***The Safety Support Assessment approach provides important context to differentiate between those organisations that are providing ATS services and those organisations that provide services in support of ATS delivery.***

[7] Refer to Annex III Subpart C. in Regulation (EU) No. 2017/373.

[8] https://www.sesarju.eu/node/3253

[9] ttps://ec.europa.eu/transport/modes/air/news/2020-09-22-ses-more-sustainable-and-resilient-air-traffic-management_en

# New Systems-Thinking Practices

***The conversation on the future of ATM service delivery and the approach to safety is progressing rapidly. New Systems-Thinking practices based on Safety-II and Resilience Engineering and their benefit to aviation safety and the methods we use in ATM should be explored.***

## *Introduction to Safety-II*

Our understanding of Systems-Thinking practices in aviation has progressed significantly in recent times. As discussed earlier, the definition of the 'system' requires clarity to recognise the complex relationship between humans and machines within it. In particular, it should recognise the positive contribution of the human as the only flexible component able to make decisions in normal and abnormal situations. This flexibility provides the adaptability needed within the system to balance safety and efficiency; the two key service outcomes. The concept is explained by David Provan et al.[10] using the term 'guided adaptability' and is a synonym for Safety II.

In summary, Provan et al. explain that traditional safety management theories have been challenged by theories from high reliability organisations, resilience engineering and now Safety-II. These theories focus on the "capacity of organisations to 'guide adaptability' of workers and systems, through understanding and supporting how complex systems usually succeed, but sometimes fail." This is strengthened by explaining that "Organizational systems succeed despite the basic limits of predetermined plans, in a complex, interdependent and changing environment, because responsible people adapt to make the system work."

The concept provides further clarity on the relationship between safety and efficiency and how they are balanced in reality as "Safety-II enables people to dynamically align the pursuit of both safety and effectiveness because there are always multiple conflicting goals, limited resources, and pressures to achieve more (i.e., industry's 'Faster, Better, Cheaper' imperative)."

A focus on guided adaptability will improve our understanding of safety in ATM by improving how we understand the system and implement changes. The challenge is guiding how people adapt to handle variability, and "when to 'trade-off' and re-prioritize across multiple risks and goals when operating in the midst of uncertainties, changing tempos and pressures."

**Learning Point 15**

***New techniques and methods should be introduced into organisations such that they can better facilitate how people adapt to handle variability within the system. This will provide insight in how we balance interdependent and conflicting goals in service delivery.***

## *Safety-II and Performance*

*"To safety, love is just zero hate - makes it easy to measure, meaningless but easy."*

There is a growing consensus in ANSPs that you cannot understand safety by analysing and reporting on the absence of safety. Thanks to the focus of Prof Erik Hollnagel the ATM/ANS industry now sees a potential opportunity to respond to the imbalance by analysing the day-to-day work of our operations[11].

[10] Safety II professionals: How resilience engineering can transform safety practice, David Provan et al, March 2020.

[11] https://erikhollnagel.com/books/safety-i-safety-ii-2014

Prof Hollnagel states that **you can identify performance metrics that allow organisations to understand safety based on day-to-day events**. Identifying what those events are and how you use them to understand safety is the target for many ANSPs.

***Learning Point 16***
***New methods to understand the presence of safety (noted in LP05) should be based on the activities that are performed within the system to deliver ATM services.***

## *Safety-II and System Safety*

There are differences of opinion between Prof Nancy Leveson (a thought leader in Software and Systems Safety) and Prof Hollnagel. Prof Leveson recently released a paper [12] that was critical of the Safety II approach with statements such as **"Safety-II is a giant step backward" and "Goals such as resilience, flexibility, and adaptability are important, but they are much more likely to be achieved using approaches other than Safety-II."** Though the arguments presented are compelling it is clear that System Safety practices have not been applied appropriately in ATM/ANS and that intervention is required. Prof Hollnagel has achieved that. Put simply, he has put the human back into our understanding of system performance in ATM.

***Learning Point 17***
***Concepts of Systems Safety and Safety-II should be considered together to help understand the complex stakeholder relationships and the role of all humans in the system who contribute to Flight Safety.***

[12] Safety III: A Systems Approach to Safety and Resilience, Prof. Nancy Leveson, Aeronautics and Astronautics Dept., MIT, 7/1/2020 http://sunnyday.mit.edu/safety-3.pdf

# Blueprint for ATM

## *Conclusion*

The aviation industry is considered ultra-safe; however, accidents still occur that result in the loss of life. The total numbers of fatalities are considered low compared to other industries, but numbers alone do not help us understand the actual level of safety and what that means for tomorrow with any confidence. We should not become complacent and should continue to seek out new opportunities to understand and improve Flight Safety.

The Air Traffic Management industry is currently undergoing a significant transformation. The Air Navigation Service Provider (ANSP) community and the supporting supply chain partners are seeking out opportunity to realise the benefits of digital innovation. One thing is clear: The aviation system of tomorrow will look very different to today. The transition to a new era of traffic management services is critical to the success of our industry. However, right now, there are two important questions that continue to be debated:

**Question 1: Is our approach to safety in ATM fit for purpose to manage our future challenges?**

**We believe the answer is no. Our approach to safety focusses too much on the machine and our understanding of the overall socio-technical system and its role in service delivery is limited. This bias is compounded by regulation. New theoretical techniques are being discussed that will help us progress on the digitalisation and automation journey. We do not yet know how to apply them. The pressure on the small amount of resource available constrains our progress and the safety community struggles to be relevant in a way the operational staff understand.**

**Question 2: Can we clearly define what value our safety efforts provide to ATM service delivery or to flight operations?**

**Again, we believe the answer is no. The operational benefits realised by the safety activities in our ANSPs cannot be explicitly demonstrated - leaving regulatory compliance as the main benefit. It is observed that the majority of benefit originates from the implementation of technical and operational strategies. Looking more broadly, effective and efficient ATM is vital to a safe aviation industry. Preventing accidents is the key focus of ATM, and we need to change the mindset of the industry to see that it is not a burden but an enabler. Increasing service effectiveness in our contribution to safety enables more effective air traffic operations.**

## *Principles for Aviation Safety*

Reflecting on our learnings from this discussion we set out eight principles that should be considered in the development of new practices in the industry and within ATM sector to address safety. The principles provide a new view of safety in ATM that will help us remain relevant as our industry welcomes new entrants and the realisation of the digitalisation strategy to deliver new services. A summary of the Learning Points is provided in Annex A and each Principle is further explained and explored in Annex B.

| Title | Principle | Learning Point |
|---|---|---|
| **01 - Flight Safety** | Flight Safety should only be evaluated (safety risk) and measured (safety performance) at the level where the harm can occur. | LP01, LP05, LP08 |
| **02 - Total System Safety Approach** | A total system safety risk picture should be available to all service providers to inform their service delivery activities in support Flight Safety. | LP02, LP03, LP08, LP10, LP17 |
| **03 - Safety Support Assessments in ATM** | Safety support assessments should be used to document service effectiveness by outlining the service providers contribution to Flight Safety. | LP03, LP07, LP11, LP14 |
| **04 - Assurance Levels** | Assurance level methods should be used to design a resilient system as a platform for delivering ATM/ANS services. | LP04, LP09 |
| **05 - System Analysis Techniques** | System analysis techniques should be used to help match the capabilities of the machine and the human in the design of the ATM system with emphasis on how the human adapts to handle variability within the system. | LP02, LP15 |
| **06 - Service Effectiveness Criteria** | Service effectiveness should be defined in terms of service risk and service performance and follow the same criteria. | LP07, LP11, LP16 |
| **07 - Quality Management Practices** | Integrated management systems based on a service lifecycle process approach should be used to define and manage the working practices that support service delivery. | LP06, LP11, LP13, |
| **08 - Culture as a pillar of management systems** | Service providers should continue to promote a culture that supports trust, learning, open reporting and sharing of information across the entire aviation industry to aid the continuous improvement of Flight Safety. | LP12 |

## *Looking to the future*

The 'number one' principle in our blueprint is that safety should only be evaluated at the level where the harm can occur. It recognises that safety cannot be credibly evaluated by the ATM service provider; it is only those that use the services provided that can evaluate safety risk. Airspace users understand the effectiveness of the services they use and focussing on effectiveness of ATM services is what the ANSP community should do to remain relevant. To achieve this we should prioritise our efforts on the design and operation of resilient services using a quality management approach in place of traditional safety management methods. **We highlight that safety is not something we do but rather an outcome of doing many different things well.** Improving safety in aviation requires us to improve the quality of how we deliver our services. This approach has been used to great success in other process and manufacturing industries and should be followed in ATM. This will require adoption of integrated management systems within ANSPs that serve as the vehicle for everyone in the organisations to collaborate on service delivery.

# Annex A – Summary of Learning Points

| # | Learning Point | Section |
|---|---|---|
| **01** | Returning our focus to protecting humans from harm will provide valuable input into defining our future approach to safety in ATM. | 2.1 |
| **02** | The scope of the *system* should be addressed; ensuring all actors the contribute to Flight Safety are included is critical to understanding safety in ATM. | 2.2 |
| **03** | Safety and assurance methods should be appropriate for the service context and the business outcomes the organisation aims to achieve. | 2.3 |
| **04** | Assurance level methods provide practical qualitative techniques to assess the effectiveness of the system and should be considered further in place of quantitative safety assessment techniques. | 2.4 |
| **05** | New methods are required to understand safety performance using indicators that reflect the presence of safety. Any new method should use the same criteria to evaluate safety risk. | 2.5 |
| **06** | The safety management system should reflect the activities that the organisation performs to contribute to safety and the relationships to other business drivers (e.g., information security and human performance). | 2.6 |
| **07** | Performance indicators used in ATM should be related to the delivery of the operational service rather than in the context of an accident sequence. | 3.4 |
| **08** | ANSPs cannot credibly evaluate safety risk at the point where harm occurs without input from other service providers in the total aviation system. | 3.4 |
| **09** | Regulation should provide clarity that qualitative judgement-based approaches are the most credible while quantitative safety risk assessments are not appropriate at the system level. | 3.4 |
| **10** | Regulation should ensure that all system elements and the assurance activities to analyse them are conducted at the system level in the context of service delivery. | 3.5 |
| **11** | The approach to safety in ATM should align with the air navigation service orientation strategy. | 4.1 |
| **12** | New approaches are required to mitigate the effect of the fragmentation on the service delivery chain (aka the safety chain) including approaches to maintain the organisational culture required to create trust and the open sharing of information. | 4.1 |
| **13** | Integrated management systems using a service lifecycle process approach should be considered to ensure all the organisations activities, and the relationship between them, are understood in the context of delivering effective services. | 4.2 |
| **14** | The Safety Support Assessment approach provides important context to differentiate between those organisations that are providing ATS services and those organisations that provide services in support of ATS delivery. | 4.3 |
| **15** | New techniques and methods should be introduced into organisations such that they can better facilitate how people adapt to handle variability within the system. This will provide insight in how we balance interdependent and conflicting goals in service delivery. | 5.1 |
| **16** | New methods to understand the presence of safety (noted in LP05) should be based on the activities that are performed within the system to deliver ATM services. | 5.2 |
| **17** | Concepts of *Systems Safety* and Safety-II should be considered together to help understand the complex stakeholder relationships and the role of all humans in the system who contribute to Flight Safety. | 5.3 |

# Annex B – A conversation for possibility

## *Principle 1 – Flight Safety*

The definition of Flight Safety should be standardised across aviation. This will ensure the consistent evaluation of safety risk to flight operations. It is observed that risk is a term often used interchangeably with hazard. The difference between risk and performance is also misused. Safety performance is measured based on yesterday's historical performance. Risk cannot be measured it can only be evaluated through judgement. It is a judgement of the amount of uncertainty we face tomorrow. According to Risk Management standard ISO31000, risk is the "effect of uncertainty on objectives" and refers to the positive consequences of uncertainty as well as negative ones. This perspective on risk is considered to provide a more useful framework for balancing competing business drivers with safety.

To ensure consistent evaluation of safety risk there should be a single aviation safety risk classification scheme, addressing the following:

1. A definition of risk based on ISO31000.
2. The aviation sectors where safety risk can be evaluated i.e. at the point at which harm occurs.
3. The consequences to be assessed within the scheme aligned to the ICAO accident categories but broadened to cover all aviation scenarios for manned and unmanned operations.
4. Severity categories that represent the potential impact on people: covering fatalities, serious injury and minor injury.
5. Likelihood categories that represent frequency of events corresponding to the societal acceptability of risk for all aircraft types in all airspace classes including emerging airspace definition for unmanned aircraft systems.
6. Appreciation for airborne risk and ground risk in all airspace classes.
7. **The means for support service providers to declare service effectiveness for the actions that contribute to Flight Safety.**

For ANSPs, the outcome of this principle is that 'safety risk' should not be evaluated for ATM/ANS services. The concept that replaces 'safety risk' in an ANSP is 'service effectiveness' which should be assessed and documented in a safety support assessment. Service effectiveness can be evaluated using risk assessment techniques, however, the intent of this principle is to only evaluate safety risk at flight operations level based on the necessary stakeholder contributions for each scenario.

## *Principle 2 – Total System Safety Approach*

A total system safety approach, as described in ICAO SMM (Doc9859), should be used as the basis of the development of an industry wide safety risk picture(s). They should be based on Safety-II and System Safety principles that allow us to construct stakeholder interface relationships which help understand how all stakeholders contribute to Flight Safety.

The safety risk picture should be made available to all support service providers, including the ATM Sector, to inform their service delivery activities and optimise the value they provide in improving Flight Safety at the appropriate interfaces. This would be achieved by analysing the human, machine, environment, infrastructure and organisational interfaces within the ANSP to all highlighted stakeholders.

The safety risk picture should be developed based on both success and failure themes. This can be achieved by identifying intermediate success states that should be achieved through each phase of flight to ensure safe outcomes. All stakeholders can then have a common point of reference for collaborative discussions. A second dimension related to preventing bad outcomes is also required. This will follow traditional methods for identifying vulnerabilities in the system. The overall outcome that we seek to achieve is better recognition of the day-to-day activities of the aviation stakeholder community that support Flight Safety and maximising the effectiveness of these activities through analysis and collaboration between stakeholders.

Approaches to risk modelling should be collaborative which requires commitment to the total system safety approach. Working across organisational and sector lines within aviation is difficult and how it is achieved requires careful consideration. Is it the role of the state or regional regulatory authorities to create and manage the collaboration? The best practice in State Safety Program (SSP) Implementation already recognises the sector risk profiles. Can this extend to the dynamic co-ordination of all industry stakeholders to create a safety risk picture? And does this create conflict with the role regulators already play in the setting of regulation? These issues need to be explored.

## *Principle 3 – Support Safety Assessments in ATM*

ANSPs will document their contribution to Flight Safety in Safety Support Assessments that record the assessment of service effectiveness based on the declared contribution to the safety risk picture as discussed in Principle 2.

It will always be difficult to relate air traffic service operations to Flight Safety. We should invest effort in understanding what we can do to ensure safe outcomes and, where appropriate, help to resolve or prevent bad outcomes. The ATM sector should tailor services to the needs of the airspace user, both manned and unmanned and in all airspace classes we operate to maximise the value ATM services contribute to Flight Safety.

Each function ATM services provide that contributes to Flight Safety will have a different level of importance or criticality. The criticality level for any function would be determined by the impact of failure on the ability of the function to achieve its purpose i.e., how could a vulnerability in the system degrade the function, and what impact does this have on the ability to provide an effective service. The reason for determining the criticality level of each control is to provide guidance on the levels of assurance required to be demonstrated in the design and operation of that system element. This is discussed under Principle 4.

Efficient and effective ATM is vital to make aviation function. ATM is an enabler and not a burden. We should emphasise that improving service effectiveness in ATM will help improve Flight Safety and efficiency of air traffic operations. Understanding the relationship between preventing collisions and expediting an orderly flow of traffic is the key factor in facilitating this change in mindset. This is discussed under Principle 5.

## *Principle 4 – Assurance Levels*

Assurance levels are a better way to achieve a resilient design than quantified assessments as they help service providers and suppliers to develop a common understanding of what the 'system' is required to do and the level of resources / effort required for implementation. Assurance level criteria should be developed, adopted and/or adapted for all system element types, including as a minimum:

1. Equipment architecture
2. Human-related factors including procedure design
3. Airspace design
4. Software assurance.

The Assurance Level scheme should be linked to the approach for Safety Support Assessments which involves understanding the criticality of functions (i.e., mitigations) provided by ATM services.

There is already significant experience available in this field. Software assurance standards have already been mentioned. The CANSO Standard of Excellence in Human Performance Management [13] also provides a strong platform for the development of assurance levels for Human Performance.

With specific reference to the role of the human, the Assurance Level scheme should include criteria as to the level of investigation required into working practices within the operation to help understand, as far as possible, the realities of work-as-done. The techniques required to conduct that investigation need to be developed and this is explored further in Principle 5.

## *Principle 5 – System Analysis Techniques*

System analysis remains critical in the design of the ATM system. New techniques are required to understand how desired service capabilities are delivered by the system. In the first instance, capability requirements should be defined independently of how they are achieved. We should then analyse the machine and the human to determine the combination best matched to deliver the needs of the operational environment. As discussed by the EGHD[14], the new techniques should not devalue the human to justify the machine, nor should it criticise the machine to rationalise the human – instead, it considers the human-machine system as a functional unit to amplify both.

Availability of digitalisation will bring new opportunities and challenges to the interaction between the human and the machine and influence our methods of work. Promoting Joint Cognitive System theory to help us in the design of the system will become critical as higher-levels of automation are considered and introduced into the aviation system. New system analysis techniques will help new functionality within the machine and changes to the roles and responsibilities of the human being seamlessly introduced to efficiently deliver the predicted benefits. Overall, this will result in a more agile approach to ATM system evolution as we introduce higher levels of automation.

The techniques should draw upon Safety-II and focus on the concept of guided adaptability and how best to achieve it to help us manage performance variability. The techniques should be simple to apply to ensure they are accessible to all air traffic organisations and technology suppliers. This will also ensure best practice is considered in our future change programmes.

## *Principle 6 – Service Effectiveness Criteria*

An ANSP should document its service effectiveness in terms of service risk and service performance using the same criteria. The criteria should be linked to the interfaces where ATM services contribute to Flight Safety through provision of specific functions. The criteria will be linked to the criticality of the functions as described under Principle 3 and used to influence the assurance level approach described in Principle 4. To this end a criticality scheme should be defined for ATM service delivery based on the ability of the system to provide that function. Similar to a traditional risk classification scheme it should include severity and likelihood. This scheme will help guide prioritisation of resources as well as the required strength of the ATS service functions.

Service risk and service performance methods may need to be different for each specific function within the service. Service risk should be based on the analysis of the system that delivers the function and the level of risk in achieving the objective of that outcome. Service performance should be measured based on what went right and what went wrong.

---

[13] https://canso.org/publication/canso-standard-of-excellence-in-human-performance-management/

[14] EGHD Position Paper: The EGHD's vision for the 'ideal flight' in 2035: optimising the role of the human in the design of the ATM/ANS system

Performance indicators should be linked to those system design elements that have been used to inform the judgement of service risk. This will ensure that service performance provides intelligence on the effectiveness of the service today and informs the judgement of delivery risk for tomorrow.

## *Principle 7 – Quality Management Practices*

This principle integrates 'safety management' within ATM/ANS providers with 'quality management' or, in other words, creating an integrated approach to service delivery through integrated management systems. Our message is that we need to stop treating safety as a separate discipline – we don't *do safety* in ATM – it is an emergent property seen as an outcome of delivering high quality services.

An ANSPs quality policy, quality objectives and plans to meet those objectives, combined with allocation of responsibility for quality across the business provides an appropriate the framework[15] for achieving the desired service outcomes. ISO9001:2015 and Quality-by-Design[16] concepts provide us with the tools to help us plan and manage our quality activities. The development of an Integrated Management System based on the CANSO Management System framework is recommended. This should be strengthened using the service management principles of ISO 20000 and the guidance from the IT Infrastructure Library (ITIL).

The following topics should be considered, as a minimum, in the development of the IMS.

1) Flight Safety (ICAO Annex 19 and EU Regulation 2017/373)
2) Information Security (ISO27000)
3) Environmental Management (ISO14000)
4) Health and Safety (ISO45001) (including Health and Wellbeing and Fatigue Management)
5) Systems Engineering (ISO15288)
6) Human Performance (CANSO Standard of Excellence in HPM)

These elements directly or indirectly support the effectiveness of service delivery.

## *Principle 8 – Culture as Pillar of Management Systems*

The safety of the aviation industry relies on fostering a positive safety culture within all aviation organisations and service providers. The existing eco-system has created a trust framework for all those within the organisations to openly report, exchange and use information with confidence from and with external parties.

The continued service transformation of our ATM system will introduce new data and air traffic service providers into the market. This process should be managed appropriately to ensure the data quality level (e.g., resilience, accuracy, integrity, security and availability) is maintained. No matter the benefits of outsourcing key functions to an external provider, assurance in all aspects of the service should be provided.

Our robust aviation culture should continue to be promoted through strong leadership from the industry and where appropriate new assurance frameworks should be introduced to ensure integrity of data transferred between service providers and with suppliers.

[15] ISO9001 requires you to set objectives and targets related to the performance outcomes relevant to your business. The objectives should be flowed down through the organisation so that everyone can articulate how they contribute to them.

[16] Quality by Design (QbD) is a concept first outlined by quality expert Joseph M. Juran. Juran believed that quality could be planned, and that most quality crises and problems relate to the way in which quality was planned.

## About To70

To70 is a leading aviation consultancy providing research and advisory services to the global aviation community. Our mission is to help society and industry address the air transport challenges they face by delivering outstanding independent consultancy services. To70 has a global presence with 15 offices across Europe, Asia, Australia and the Americas.

Learn more - www.to70.com

## About the Authors

**Huw Ross** is a Senior Consultant and Managing Director of To70 UK. He has spent his career preventing and minimising the impact of accidents on people. His career started 20 years ago designing new workplace systems through analysis of occupational health and safety incidents. He has spent the last 15 years working in aviation both directly for NATS UK and more recently as a Consultant working across the aviation industry. Huw has experience in designing, implementing and applying safety management systems and is passionate about sharing this knowledge to drive improvement. He has held a range of senior advisory and leadership posts including: Safety Adviser to the European Commission Performance Review Body, CANSO Global Safety Steering Group member and currently is a Co-Chair of the CANSO Next Generation SMS Workgroup. Huw also is an Expert Adviser to the ICAO Safety Management Panel.

**Roger Dillon** is an Applied Physics graduate with 37 years' experience in the aerospace and aviation industry. He has had a long career working in safety leadership roles at NATS UK. Roger has significant experience in the development and application of a wide range of Safety Management and Safety Assessment techniques. He has represented CANSO and NATS on EASA Rulemaking task forces related to regulatory development and as well as leading several major technical and airspace change programmes at NATS. He also held the role of Manager Safety at the London Area and Terminal Control Centre. Roger is well recognised with the Air Traffic Industry and led both the CANSO Global Safety Development Workgroup and the CANSO Europe Safety Directors group whilst working at NATS.

to70