EXPLORATORY RESEARCH

sesar JOINT UNDERTAKING

D6.3 Safety and Resilience Guidelines

Deliverable ID:	**D6.3**
Dissemination Level:	**PU**
Project Acronym:	**FARO**
Grant:	**892542**
Call:	**H2020-SESAR-2019-02**
Topic:	**SESAR-ER4-06-2019 - Safety and Resilience**
Consortium Coordinator:	**CRIDA**
Edition date:	**20/05/2022**
Edition:	**00.02.00**
Template Edition:	**02.00.03**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval[1]

Authors of the document

Name / Beneficiary	Position / Title	Date
Fedja NETJASOV/ UB-FTTE	WP6 Lead	20/05/2022
Bojana MIRKOVIC/ UB-FTTE	Project Contributor	28/03/2022
Doroteja TIMOTIC / UB-FTTE	Project Contributor	28/03/2022
Tamara PEJOVIC/ ECTL	Project Contributor	28/03/2022
Christian VERDONK/ CRIDA	Project Coordinator	28/03/2022
Fernando GÓMEZ / UPM	WP4 Lead	28/03/2022
Anthony SMOKER/ LU	WP5 Lead	28/03/2022
Carlo Dambra / Zenabyte	WP3 Lead	28/03/2022

Reviewers internal to the project

Name / Beneficiary	Position / Title	Date
Christian VERDONK/ CRIDA	Project Coordinator	26/05/2022
Rosa ARNALDO/UPM	Project Contributor	16/03/2022
Fernando GÓMEZ/ UPM	WP4 Lead	28/03/2022
Tamara PEJOVIC/ ECTL	Project Contributor	28/03/2022
Patricia RUIZ/ ENAIRE	Project Contributor	28/03/2022
Irene BUSELLI / ZENABYTE	Project Contributor	28/03/2022
Nnenna IKE / LU	Project Contributor	16/03/2022
Anthony SMOKER/ LU	WP5 Lead	28/03/2022

Reviewers external to the project

Name / Beneficiary	Position / Title	Date

[1] The beneficiaries/consortium confirm(s) the correct application of the GA, which includes data protection provisions, and compliance with GDPR or the applicable legal framework with an equivalent level of protection, in the frame of the Action. In particular, beneficiaries/consortium confirm(s) to be up to date with their consent management system.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Approved for submission to the SJU By - Representatives of all beneficiaries involved in the project

Name / Beneficiary	Position / Title	Date
Fedja NETJASOV/ UB-FTTE	WP6 Lead	31/05/2022
Christian VERDONK/ CRIDA	Project Coordinator	31/05/2022
Carlo Dambra / ZENABYTE	WP3 Lead	29/03/2022
Fernando GÓMEZ / UPM	WP4 Lead	28/03/2022
Anthony SMOKER/ LU	WP5 Lead	28/03/2022
Tamara PEJOVIC/ ECTL	Project Contributor	28/03/2022
Patricia RUIZ/ ENAIRE	Project Contributor	29/03/2022

Rejected By - Representatives of beneficiaries involved in the project

Name and/or Beneficiary	Position / Title	Date

Document History

Edition	Date	Status	Name / Beneficiary	Justification
00.00.01	11/02/2022	Draft	UB-FTTE	Document Structure definition
00.00.01	02/03/2022	Draft	UPM	Contribution
00.00.01	07/03/2022	Draft	LUND	Contribution
00.00.01	16/03/2022	Draft	UB-FTTE	Integrated draft version
00.00.02	25/03/2022	Draft	CRIDA	Contribution
00.00.03	28/03/2022	Draft	UB-FTTE	Integrated draft version
00.01.00	29/03/2022	Final	UB-FTTE	Final version
00.01.00	13/04/2022	Final	S3JU	Revision
00.02.00	20/05/2022	Final	UB-FTTE	Revised version after the Final Maturity Gate and Comments received from SJU

EUROPEAN PARTNERSHIP

Co-funded by the European Union

FARO

SAFETY AND RESILIENCE GUIDELINES FOR AVIATION

This deliverable is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 892542 under European Union's Horizon 2020 research and innovation programme.

Abstract

Do you plan to introduce changes to your ANS/ATM system? How would these changes affect the safety of your operations? Would they increase resilient performance of the system?

Deliverable "D6.3: Safety and Resilience Integration Guidelines" is framed within FARO WP6 and is related to FARO project objective "Provision of design guidelines and identification of future research needs" (O4). Deliverable ultimately provided a description of the Safety and Resilience integration process and covers the:

a) overview of how possible changes introduced in ANS/ATM system can impact safety and resilience of operations,

b) description of safety and resilience integration process containing five steps, as well as introduction to SEESAW concept and SR-BBN model both proposed by FARO project for the integration of safety and resilience, and

c) recommendations related to data, safety and resilience performances, SEESAW concept and SR-BBN model.

This deliverable is written in a way to be used as standalone document providing enough information to interested stakeholders and referring to other deliverables for more details.

Finally, the Deliverable "D6.3: Safety and Resilience Guidelines" has been renamed as agreed with the SESAR 3 JU to avoid confusion with the Final Project Results Report (D1.3), which gathers the project results and next steps in the research.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

List of Tables

EUROPEAN PARTNERSHIP
Co-funded by the European Union

List of Figures

1 Introduction

Safety and Resilience: an introduction

The traditional approach to safety (Safety I), and its relevant models and methods, have contributed much towards enhancing the safety of industrial systems, but they are limited when dealing with safety issues in **complex socio-technical systems,** like ATM [1]. FARO attempts to observe the ATM's Safety in terms of system's technical, organizational, human and procedural characteristics [2]. In addition, FARO explores Resilience Engineering (RE), and subsequently Safety II, in response to the trend that emerged and gained attention over the last two decades.

Safety I methods are about finding and fixing causes of an accident, meaning they are designed relying on "what can go wrong" in the system. Safety II and resilience engineering rely on the "what goes right", learning from a system's ability to adapt in everyday situations. The traditional safety concept and safety management system use as references anticipated work situations (prescribed through rules and procedures) and environmental changes (**work-as-imagined – WAI**). But it is not possible to develop WAI optimized for all working situations, in the system with complex interactions between functional elements. In practice, human workers carry out their tasks constantly adapting to their work conditions, changing demand and environment, and currently available resources. This actual work (**work-as-done – WAD**) is a cause of many successful work outcomes and very rarely failed work outcomes (accidents and incidents). New safety concepts consider accidents as abnormal results in overall work processes and change the perspective of human errors – not as a root cause, but as an indication of poor system design.

Traditional safety is in principle reactive (learning from failures), while Safety II and RE are proactive approaches (learning from success). Even if we do our best to manage system safety proactively, incidents and accidents can still happen. Once they do, we need to find the ways of mitigating the negative effects and preventing its recurrence. That means these traditional and new safety approaches need to be combined.

Models for safety assessment are mostly quantitative, while available models for resilient performance assessment are qualitative. FARO project aims to quantify safety in ATM as complex socio/technical system, quantify resilience, and to demonstrate the synergy between the traditional approach to safety and resilience engineering.

Safety

A specific objective of the "Safety Analysis" part of the FARO project is to define the ATM **Safety Performance Functions** (SPF) by using the organisational, technical, human and procedural precursors to characterise and predict **Separations Minima Infringements** (SMIs) as a function of those precursors. The term Safety Performance Function (SPF) is used in many industries to refer, in a general way, to mathematical models that have the capacity to explain, but above all, predict the occurrence of safety events [3].

One of its main applications in ATC/ATM field is focused on the analysis of SMIs. SMI is a situation in which the prescribed separation minima were not maintained between aircraft. The **Bayesian Network** (BN) – Safety Performance Functions approach was developed and applied in FARO project. The proposed methodology aims at deriving a model able to characterise and predict the occurrence of SMIs between en-route aircraft.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The BN as a probabilistic approach is based on Bayesian statistics and has a high predictive capacity, which allows integrating knowledge modelling with data inference and has proven to be useful to estimate low probability events such as SMIs [4].

Resilience

The specific objective of the "Resilience Analysis" part of the FARO project is to develop a resilient performance framework by understanding the resilient performance in ATM for a baseline case and use cases, identifying critical characteristics and developing indicators of resilient performance to gain an understanding of the impact on resilient performance for the automation introduced with the use cases.

Resilient Performance (RP) is characterised as how system performance is sustained under expected and unexpected scenarios. A complex system (containing technology, organisation and people – TOP paradigm) is resilient if it adapts effectively to surprises/events. The purpose of resilient performance assessment is to develop an understanding of how the system performs, adapts, responds, and manages performance variability and how it sustains performance and operation.

The **performance indicators** provide the means to assess resilient performance and are partially derived from analysis of interview data and explicated by the synthesis of workshops, interviews and other data sources [3].

1.1 Purpose of the document

Deliverable "D6.3: Safety and Resilience Guidelines" is framed within FARO WP6 and is covering the: a) overview of how possible changes introduced in ANS/ATM system can impact safety and resilience of operations overview of changes introduced in ATC/ATM system as well as the impact of those changes on safety and resilience of ATM operations, b) description of safety and resilience integration process containing five steps, as well as introduction to SEESAW concept and SR-BBN model both proposed by FARO project for the integration of safety and resilience, and c) integration process recommendations related to data, safety and resilience performances, SEESAW concept and SR-BBN model.

This deliverable is written in a way to be used as standalone document providing enough information to interested stakeholders and referring to other deliverables for more details.

Deliverable "D6.3: Safety and Resilience Guidelines" has been renamed as agreed with the SJU to avoid confusion with the Final Project Results Report.

1.2 Document Structure

This document is structured as follows:

- Section 1 is an introduction,
- Section 2 gives an overview of how possible changes introduced in ATC/ATM system can impact safety and resilience of operations,
- Section 3 provides description of safety and resilience integration process containing five steps, as well as introduction to SEESAW concept and SR-BBN model,
- Section 4 provides recommendations related to data, safety and resilience performances, SEESAW concept and SR-BBN model.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1.3 Acronyms and Terminology

Term	Definition
ACC	Area Control Centre
ANS	Air Navigation System
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
ATFCM	Air Traffic Flow and Capacity Management
BCN	Barcelona Area Control Centre
BN	Bayesian Networks
BBN	Bayesian Belief Network
CB	Cumulonimbus cloud
CMP	Unit Complexity
CNS	Communication, Navigation, Surveillance
CPA	Closest Point of Approach
CWL	Control Workload
FLAS	Flight Level Allocation System
IFR	Instrument Flight Rules
KPA	Key Performance Area
NM	Nautical Mile
ODL	Opposite Direction Levels
RE	Resilience Engineering
RP	Resilient Performance
SMI	Separation Minima Infringement
S&R	Safety and Resilience
SPF	Safety Performance Function
SR-BBN	Safety and Resilience Bayesian Belief Network
STCA	Short-Term Conflict Alert
TOP	Technology, Organization and People
TRF	Traffic Volume
UAB	Units of Adaptive Behaviour
UC	Use Case
WAD	Work-As-Done
WAI	Work-As-Imagined

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Combined use of Safety and Resilience

2.1 Introduction of changes in ANS/ATM system

The Challenge

ATM is a complex multi-agent system. As such, it is founded in the balance of **technology, organization and people**. These three pillars work together (the **TOP** approach) in equilibrium, pursuing a safe, efficient and resilient system.

Any change in these pillars represents a shift in the balance. Changes might be a new tactical procedure, adjustments in the organisations or placing advanced systems in place. In summary, alterations in the allocation of functions and roles within the ATM agents.

The approach herein described facilitates the understanding of the balance between **safety** and **resilient performance**, and of how the latter is created. Following the TOP paradigm, it addresses this challenge from a **systemic** perspective, considering human, system and organizational factors [2].

An Integrated view of Safety and Resilient Performance

In ATM, **safety** is the outcome of ATM's work as a whole. In this sense, safety is more related to the functioning in normal conditions rather than when it fails [4]. **Resilient performance** in ATM is about producing a safe outcome, even in conditions out of the design operating point [5].

How safe a given situation will be depends on the *supply* of resources (availability, timeliness and coordination costs of these resources) by the organisation and the humans, and its effective application by using the technology available[2]. Resilient performance under unforeseen circumstances is created by the generation of strategies for an effective application of these resources, which widen the operating conditions of the system while maintaining accepted safety levels.

These two notions, *safety as an outcome* and a supply side that can expand beyond its design operating conditions make the case for an integrated view on safety and resilient performance [3], [6].

When to use it?

Use FARO's S&R Approach if your organisation is exploring about:

1. the identification of the strategies that the organisation and humans use in their work,
2. the transformation of these strategies into quantifiable data,
3. the observation and quantification of the application of strategies over time to cope with unforeseen circumstances as well as normal operations,

[2] So far, these resources are cognitive and are associated to workload.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4. the sensitiveness of the safety outcome to operating conditions and the application of strategies by the different actors,

5. identify your operating conditions in terms of supply side and safety levels in your current operations,

6. identify when your system has been operating under "resilient" operation to learn the strategies that have been used and how they affected safety levels, and

7. identify when the system what has been prone to an unsafe operation.

Also, Use FARO's S&R approach if your organisation when designing a new system if:

8. you want to evaluate variations in the safety levels in normal or abnormal conditions if the use of a given strategy is altered by a change in the system, and

9. elicit the data requirements (at system level) at an initial stage that will facilitate the assessment in terms of resilient performance and safety levels.

2.2 Impact of the changes on safety of operations

Safety Performance Functions

When describing a scenario in terms of safety from the point of view of **Safety Performance Functions** (SPFs), the focus is on the outcomes; the starting conditions of the scenario; and on some intermediate variables implemented in the SPFs.

SPFs go far beyond the conventional safety indicators (number, type, such as the number of SMIs, predicted SMIs for airspace, and statistical descriptors such as median, standard deviation, quintiles and confidence intervals, relative to the number of controlled IFR flights, etc.).

SPFs complement these metrics extending the safety assessment of the scenario. SPFs intend to capture additional outcomes that help to characterise a scenario in terms of safety and seek also to capture the characteristics of the scenario that leads to those outcomes[3], all in an integrated view.

The transmission of the SPF results is complex. The SPFs' outcomes derive from the conceptual model implemented and are described in terms of the statistical probability distribution of its main elements. The SPF conceptual model developed in this project considers the general scenario where aircraft trajectories evolve and focuses on the analysis of the Closest Point of Approach (CPA), for any possible aircraft pair in an air traffic sector, and on the understanding and quantification of the process that leads to such CPA. The model is integrated by several Bayesian Networks (BNs), and each of them contains probabilistic nodes representing the following information:

- **Input variables** representing general features that characterise the scenario and its traffic. Regarding the inputs, safety dimensions or possible precursors to be considered, we

[3] FARO identifies them as safety dimensions and precursors (see D2.1)

Co-funded by the European Union

proposed a group of 12 areas[4]: Traffic Demand, Airspace, Organization and Management of Human Resources, Human Resources, ATFCM Regulations, Planning Compliance, Operations, Potential Conflict, Safety Management, Economic Management and Results, Aeronautical Information, CNS / ATM Systems.

The inputs to the model are characterised as probability distributions and refer to the general conditions that characterise the sector and its traffic.

- **Intermediate variables** represent variables that the model predicts as intermediate calculation and that are used to stochastically derive the prediction of the main outcome variables[5]. **Outcome variables** representing the safety metrics predicted by the model. The safety metrics predicted by the model are of two different types:
    - **Predicted probability of success of the ATM barriers included in the model.** These are binary variables.
    - **Predicted probability distribution of the vertical and horizontal separation of the aircraft at CPAs**. Prior and final CPA distances probability distribution can be considered depending upon the availability of data. These outputs are discrete probability distributions representing the vertical or horizontal separation in the CPA for aircraft pairs. This corresponds also to four states probability distributions that stand for the following concepts:
        - Probability distribution of the vertical separation between aircraft at the CPA.
        - Probability distribution of the horizontal separation at the CPA between aircraft, for those with vertical separation less than 1000 feet.

A detailed description of these key model elements and how they are implemented and quantified can be consulted in Deliverable D4.1 [2].

Representation of SPF Results

FARO WP4 proposed a synthetic representation of the model results, intended to support decision making, to quickly convey the predictive information about the performance of a future ATM system change or modification. **For a synthetic representation of the results offered by the model the emphasis should be put on the main pieces of information, at the proper level of detail.** These pieces of information are represented by the input variables and outcome variables as indicated in Table 1**.**

[4] The optimal set of variables and parameters was extensively discussed in Section 4 of D4.1 [4]. Because of data unavailability, the models developed in this project were only incorporating those inputs related to temporal distribution of demand, traffic density, flows and airspace structure, ATFCM Measures, changes in the Flight Plan, adherence to the trajectory, among others.

[5] The complete list of intermediate variables for FARO UC1 and UC2 was defined in Section 7 of D4.1 [4].

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table 1. Input and outcome variables

Input Variables	Outcome Variables	
Safety dimensions and precursors (general features that characterise the scenario and its traffic) [2]	Predicted probability of success of the ATM barriers included in the model	Predicted probability distribution of the vertical and horizontal separation of the aircraft at CPAs.
Input variables as defined in Section 7 of D4.1 [4] (e.g. Occupancy, Entries, AC distribution by FL, etc)	Probability of aircraft Interaction defined as two aircraft within 20 NM of each other. Probably of Potential conflict, based upon predicted trajectory, without the action of the controller. Probability of conflict identification Probability of conflict resolution Probability of STCA alert Probability of Conflict resolution after STCA	Probability distribution of the vertical separation between aircraft. Probability distribution of the horizontal separation between aircraft, for those with vertical separation less than 800 feet.

Although intermediate variables could certainly be of interest for the user, these offer very detailed operational information. This detailed low-level information **will be useful in the design phases of an ATM change** and can help in the evaluation of alternatives and "what-if" analysis. However, it is too low level to directly support decision making process. This information would be anyway available from the model just by picking in the network nodes.

For the sake of clarity, the presentation of the key information is organized like a triptych or dashboard with 3 main panels. Figure 1 shows the triptych with the schematic graphic summary of the inputs and outcomes of the model developed so far (the triptych is fully explained in FARO Deliverable D4.2 [6]).

The left-hand side of the triptych summarizes the input variables. As it can be seen, the inputs are characterised as probability distributions and refer to the general conditions that characterise the sector and its traffic. The figure includes some examples of input variables such as the distribution of aircraft entries in the sector, the distribution of FL at the point of entry of aircraft in the sector, the distribution of aircraft speed, etc.

The outputs of the network, also characterised by probability distributions, are summarized in the centre and right-hand side of the triptych. For a given state of the input variables, the central part of the triptych shows the predicted probability of success for the ATM barriers, for example, the probability of interaction between aircraft, probability of potential conflict, probability of detection of the conflict, probability of resolution of the conflict, etc. For a given state of the input variables, the right-hand side of the triptych shows the predicted probability distribution of the aircraft's vertical and horizontal separation at the CPAs.

Thus, with this graphic dashboard it is possible to draw and interpret conclusions about the impact that a modification in the network entry conditions would have on the effectiveness of the barriers and on the final distance distributions between aircraft in the CPA, thus estimating the probability of SMI.

Co-funded by the European Union

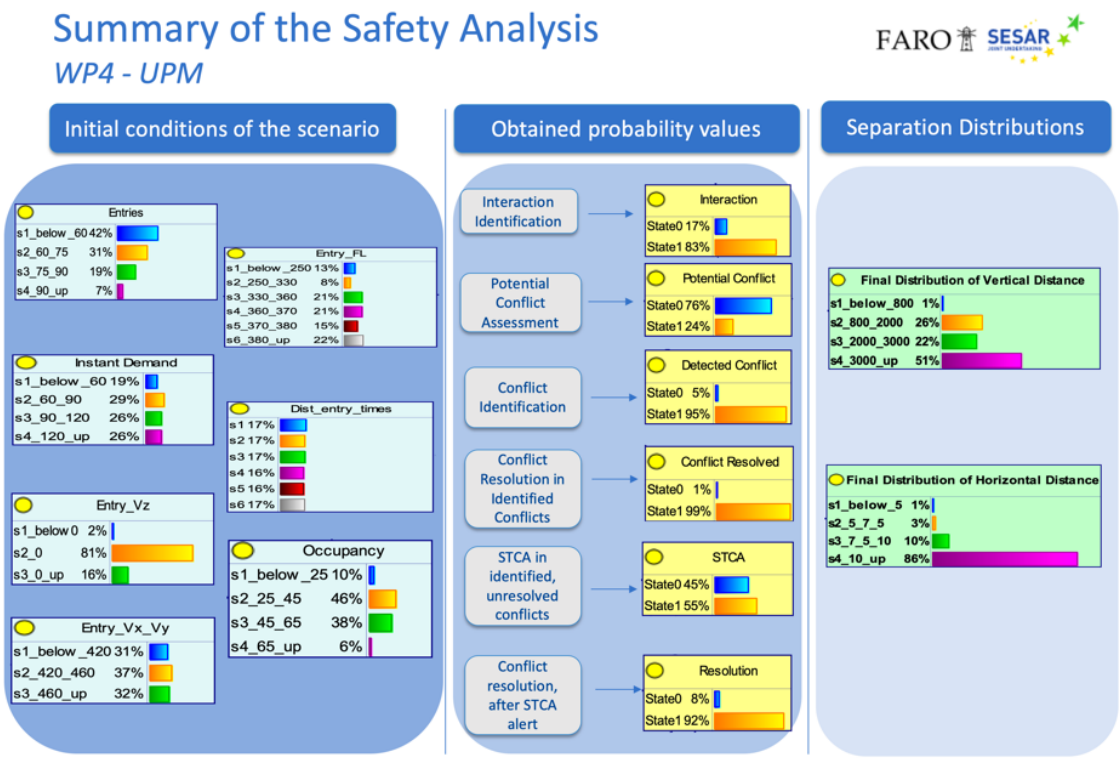


Figure 1: Triptych/dashboard with Safety Analysis results summary

Another important way to assess safety in a scenario is to look at **the most influential input variables, or combination of variables, for all sub-networks that predict the probability of success of the ATM barriers included in the model.** This analysis allows identifying which are the variables, or combination of variables, that have higher influence in the probability of success of such barriers, as well as quantify numerically that influence.

Numerical quantification of this influence allows setting acceptability limits on the values of these variables to keep the probability of success of the corresponding ATM barrier contained within a certain range of values. For example, the percentage change of a set of input variables can be limited to a certain increase, say 10%, to achieve an equivalent increase or decrease in the effectiveness of the probability of conflict detection.

The analysis encompasses a big amount of complex information about the 10 most influential variables, and how much they impact, on each of the ATM safety barriers of the model. Tables, like the one shown below (Table 2), are used for this purpose[6]. Green cells indicate the variables that positively most influence effectiveness of a particular barrier, while cells in red indicate the variables that negatively most influence the effectiveness of a particular barrier.

[6] Detailed information on how to obtain and interpret this table is provided in Section 3.4 of D4.2 [7].

Co-funded by the European Union

Table 2. Most influential variables (part of)

1 to 5 Months δ / 10% δ	Prob. of traffic interaction	Prob. of Potential Conflict	Prob. of Conflict Detection
Influence	**"Occupancy" between 25% and 45%** over the maximum value & **"Entries" below 60%** over the declared capacity	No **"FL overlap" &"heading convergence"**	**"Proportion Vertical Speed Difference" less than 35%** of ACs have vertical speed difference & **"Entry Vertical Speeds Distribution"** avenge vertical velocity difference at the sector entry **equal to 0**
	"Instant demand" below 60% over the maximum instant capacity	No **"FL overlap" & No"heading convergence"**	**"No Planned AC" below 35%** of the complexity that it could provide
	"Instant demand" above 120% over the maximum instant capacity	**"FL overlap" & No"heading convergence"**	**"Performance"** performance gap **below 35%** & **"Proportion Vertical Speed Difference" less than 35%** of ACs have vertical speed difference & **"Proportion Horizontal Speed Difference" between 35% and 70%** of ACs have horizontal speed difference

Varying Conditions before and after the change

The **final consideration for the assessment of the safety of a scenario is to understand how safety outcomes perform for different traffic loads (high and low occupancy).** This type of analyses can be consulted in detail in D6.2 [6]. For each high and low occupancy scenario, different datasets were considered in order to obtain a good representation of safety levels. In particular, for high occupancy corresponding to 90%, 80% and 70% occupancy rates and low occupancy with 20%, 30% and 40%. This process allows obtaining a very good picture of the whole operational spectrum of the sector in terms of safety as it indicates how all parameters behave both when there is high occupancy and traffic load and when there is low occupancy or traffic load.

2.3 Impact of the changes on the resilience

Digitalisation and automation involving greater integration of human and technology (i.e., complex socio-technical system such as the ATM), will lead to different patterns of activity, dependencies and interactions between system actors and agents. As operational and technological changes made across the lifecycle of a system (e.g., digitalised solutions, automation, new airspace designs, new concepts and methods of operations), new system conditions and behaviours are introduced into the operational environment. In response, the system adapts its behaviour to meet these condition(s) that have emerged. This raises questions to how these changes influence or change the nature of adaptive capacity and resilient performance of the ATM system [5].

Co-funded by the European Union

Exploring resilient performance of a system (units of adaptive behaviour (UAB)[7] is thus to understand how a UAB involves exploration of the system and hierarchical structure from an organisational perspective. A principal focus being how decisions taken at the macro level manifests at the meso/micro levels of the organisation. The view is that decisions made at a macro level often take the form of trade-offs in a resource-constrained operational environment, where system actors at the meso/micro level seek an optimal path to balance various organisational goals.

To determine how change(s) introduced to a system influences resilient performance of a system is thus, to:

1. assess the changing nature of adaptive strategies that are employed,
2. assess the trade-offs that are made and the strategies that enable sustained adaptability at the margins, and,
3. assess how buffers built into the work system are used or drawn upon in the old organisation (before the change) and in new organisation (after the change).

Herein, lays the approach and view that underpins Resilience Engineering (RE), which here is realised as resilient performance: the system is characterised as a network of interactions and interdependencies. An understanding of various perspectives and dimensions of how work is undertaken at different levels of the system hierarchy (macro, meso, and micro), functional roles, and the human operator working alongside system artefacts, is necessary to understand how the system achieves resilient performance.

This view of resilient performance extends beyond the traditional safety view of counting errors and failures (quantification) but rather, is interested in how the system adapts to a situation and sustains performance to achieve competing goals in a complex operational environment. By situation it is meant confronted with performance variability surprises and challenges. In this light, safety and adaptation are related, but performance in these terms is broader than safety alone as it includes the effectiveness of service provision for example. How the system is able to do so, can be different before and after the implementation of a change. Therefore, there are opportunities and benefits that can positively influence resilient performance.

Strategies

As an organisation responds to events, which can introduce competing demands on the system, strategies and decisions will be made that reconcile the core goals that the system strives to sustain whilst taking into consideration context, the developing situation and the surrounding environment. Strategies which may be deployed to respond to events that arise including challenges and surprises can be basic and/or complex strategies. For example, forces and situational conditions such as weather/CBs could lead to adaptive strategies deployed across micro, meso, and macro scale of the system hierarchy. In this scenario, this may involve rerouting of traffic away from the cumulonimbus cloud (CB) area (micro); band boxing (split or collapse of sector) - meso level; and/re-sectorisation and change to airspace structure (macro).

[7] An 'adaptive unit' – a unit of adaptive behaviour (UAB) is, 'units' that adapt activities, resources, strategies as they confront variability and uncertainty to sustain operations and maintain/achieve system goals through prioritisations. See FARO D5.1 [5].

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Not all the strategies identified from observation and interview texts can be derived from the system data (i.e., ATCos prediction of a fix an aircraft may route to, as seen in first example above) as some reveal adaptations and informal strategies deployed in the work system based on the human operator's knowledge and experience of the work that is being done. Therefore, quantification of resilient performance as a numerical outcome becomes a challenge and perhaps, of limited value in understanding safety performance in ATM operations.

Nonetheless, it is possible to derive indicators that characterise resilient performance. Hollnagel [7] describes four resilience potentials of a resilient system or organisation as anticipating, monitoring, responding, and learning. These potentials explain important aspects of a resilient system and thereby, resilient performance. A strategy may pertain to one or several of these abilities.

Applying a Resilience Engineering lens is thus to explore how the change (introduction of automation/new design solution, etc.) have led to changes in the nature of work and how work is done and undertaken. In assessing each strategy, the goal is to understand:

- What characterises resilient performance in sector operations before and after the change?
- What are the characteristics of surprise and challenge events (that can disrupt operations) before and after the change and what are the impacts on resilient performance and the ability to sustain adaptation that leads to sustaining service provision?
- How has resilient performance in sector operations changed after implementation of the solution?
- Have new strategies emerged that improve resilient performance in some way in this interaction?

Example: Sectorisation, implementation of new ATS routes, Flight Level Allocation System and change in operational procedures in Barcelona (BCN) ACC [9].

The change in the airspace structure and introduction of new routes resulted in new system states (i.e., differences in control tasks) and to manage the operational environment and sustain operations, the system adapts and changes its performance as users find ways beneficial to system performance to make the system work. These include evolution of new techniques for controlling (see Table 3).

Table 3. An example of transformation of strategy to indicators of resilient performance

Strategy	Indicators/Metrics	Link to Resilience
Reduce the number of interactions at a particular area/fix/crossing point by reducing the potential for interactions between the flow of traffic in the BCN area.	• Occupancy of the sector, • Compare Density of aircraft and instances of aircraft within 20NM of BCN, • Occupancy within 20NM of the BCN, • Traffic flow around the BCN VOR - east/west flow vs. north/south, • Direct routes: direct routes given tactically.	Are strategies for tactically managing the convergence of traffic overhead BCN in the new environment enacted in the same way or are new coordination loads introduced? Does the new environment deconflict traffic overhead BCN or is there an increase or change that introduces brittleness in the new organisation?

EUROPEAN PARTNERSHIP

Co-funded by the European Union

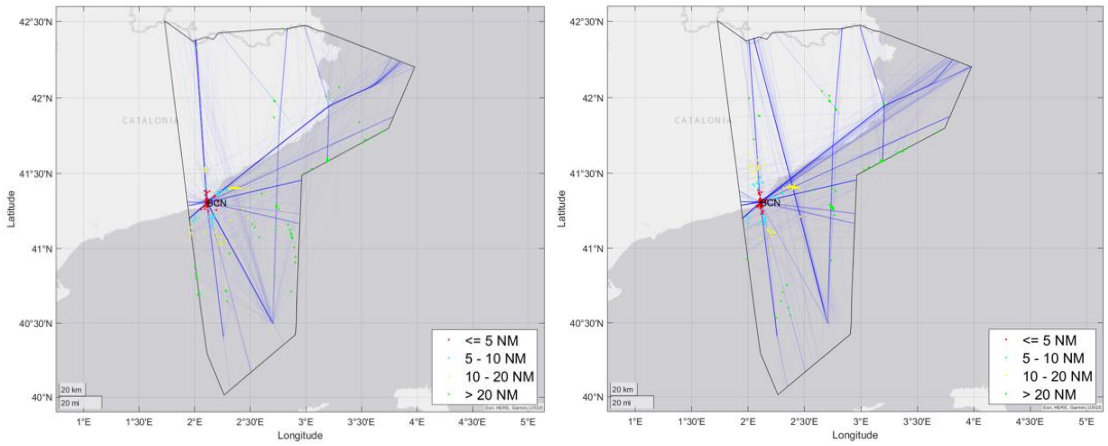


Figure 2. Visualisation of an indicator of the number of interactions at a particular area i.e., BCN - before the changes (left) and after the changes (right) made in the Barcelona Central Sector.

In Figure 2 above, integral to the changes in the Barcelona sector group through re-sectorisation and institution of a flight level allocation system (FLAS) that deconflicts N/S and E/W traffic flows, is the deployment of a strategy to spread out interactions avoiding convergence at BCN. The strategy is in the service of managing workload and creating buffer. This increases the number of reroutes given to aircraft.

The purpose of the system of indicators and metrics is then to support and facilitate developing an understanding of resilient performance of elements of a complex socio-technical system. The characteristics of a system's resilient performance have been, in the following example, described above. These indicators, therefore, individually and together provide explanatory power in understanding how the strategies and adaptations in response to performance variability, now operationalised, lead to identifiable different patterns of activities.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Integrated Safety and Resilience performance – stepwise approach

Aiming at combining the approaches to Safety and Resilience performance FARO project proposes a following stepwise approach for integration consisting of five steps (Figure 3) which emerged as a result of inductive reasoning throughout FARO project.

For any particular use case (STEP 0) which considers certain ATC/ATM system changes, a first step is: STEP 1 - Identification of necessary data. After that integration process contains two parallel steps (already explained in Section 2): STEP 2 – Safety performance functions and STEP 3 – Resilience performance.

In STEP 0 the selection and detailed description of the Use Case is made as well as the identification of the safety and resilience data dimensions (commensurate to data availability). At the same time the definition of a proposal for safety and resilience performance indicators to be measured is provided. STEP 1 describes a data-hub through which necessary data will be collected, stored and transferred for safety and resilience purposes. It provides a detailed description of the data sources specific for each Use case, introduced into the data-hub. STEP 2 describes how to develop Safety performance functions – SPF, how to calibrate and adjust them, and how to perform a SPF sensitivity analysis. STEP 3 - describe a Resilience Model for the ATM system through use of resilience engineering and systems theory to assess and understand resilient performance of the work system and the strategies that are used by all actors to adapt to changing and varying operating conditions and states.

Finally, the integration approach contains another pair of steps (will be explained in following sections) which are using outputs from previous steps as inputs: Step 4 - **SEESAW concept** and Step 5 – **Safety & Resilience Bayesian Belief Network (SR-BBN model).**

At the end of the process, conclusions can be drawn.

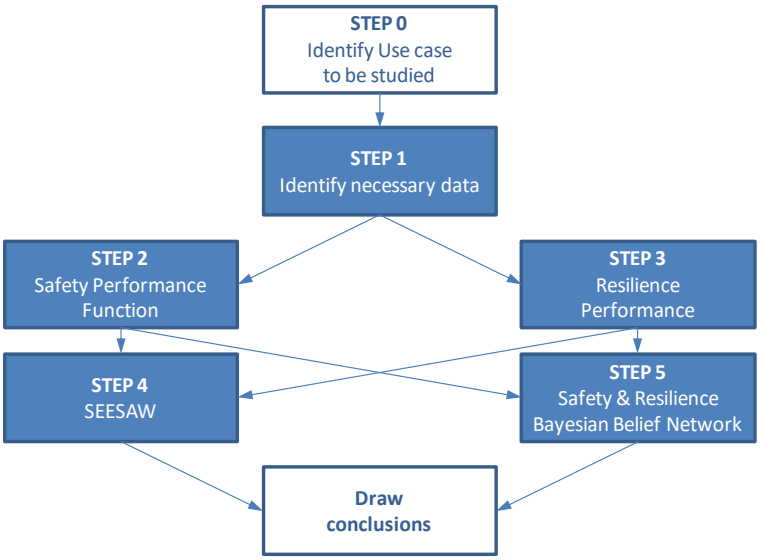


Figure 3. Safety and Resilience performance integration process

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3.1 Introduction to SEESAW Concept

FARO uses an analogy of a lever mechanism (SEESAW concept) to demonstrate the synergies between safety and resilience and help Air navigation service providers (ANSPs) to better understand the relationship between the two. The proposed concept aims to provide a high-level understanding on the balancing between the demand (including the uncertainties) and available resources on the supply (ATC) side that considers ATCOs on their working positions within a given Area Control Centre (ACC) unit, tools and working procedures.

SEESAW elements

The SEESAW concept in the context of FARO project is depicted in Figure 4.

The left-hand side represents the demand. In the context of the SEESAW concept – traffic volume (TRF) represents the load and unit complexity (CMP) represents the distance from the fulcrum i.e. the resistance arm. These two compose the torque (blue, counter-clockwise) i.e. system expected interactions per unit of time. The blue arrows indicate that the system can safely handle different traffic volumes depending on the CMP (producing the same resultant torque).

On the right-hand side (supply side) work-as-done in ATC as a socio-technical system is represented. The area reflects ATC system's adaptive capacity. Its boundaries have been defined and inspired by an application of the Rasmussen's model [10] to the railway system [11]. The boundaries are the safety boundary, capacity and operational efficiency boundary (+ economic boundary) and workload boundary.

The shape of the area varies depends on the ANSPs and it is a result of the activities of their people, procedures, equipment, environment, as well as their interactions. These system boundaries should reflect the trade-off between different Key Performance Areas (KPAs) – safety, capacity, cost and operational efficiency, but also try to differentiate between ***base adaptive capacity*** and ***extra adaptive capacity***.

In the context of the SEESAW concept – the effort to balance against the traffic load is represented by available resources/capacity and the distance from the fulcrum (the effort arm) is unit ATC's control workload (CWL). Multiplied they produce the resulting torque (yellow, clockwise), i.e. system output workload in a unit of time needed to balance the system expected interactions.

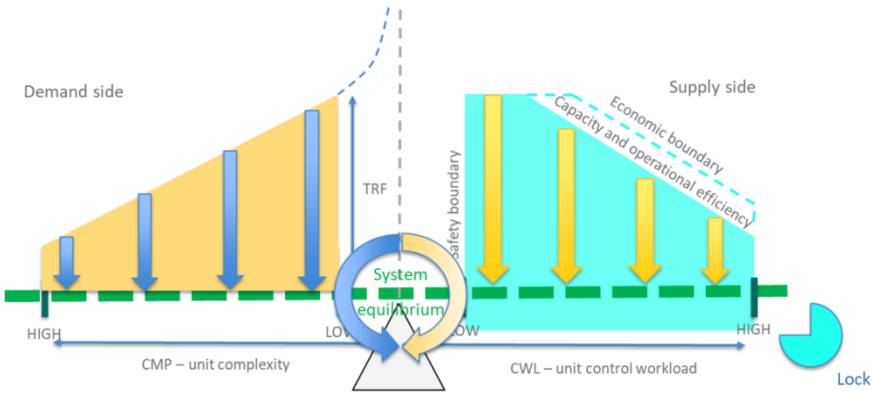


Figure 4. SEESAW concept of safety and resilience

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The system balance can be maintained with a smaller number of resources absorbing a higher number of workload units, or higher number of resources operating under lower workload. A "lock" is introduced to constrain the imbalance is clock-wise direction. It indicates the limit after which the system goes towards creating cost inefficiencies.

Interpreting the SEESAW

The supply side should adapt to changes on the demand side in order to maintain the system balance at all times. The system's ability to adapt results from how the system responds to anticipated performance variations and how the system copes with unanticipated events with a component of surprise or challenge.

Small-scale uncertainties in traffic evolution can be resolved without the system getting out of balance, because of the buffers designed into the system. On the other hand, changes on the demand side associated to high uncertainty or intensity can lead to undesired imbalances (Figure 5), and require a set of ("normalised" and individual) efforts to recover and maintain safety. In such situations, the system's recovery depends on how much its adaptive capacity can extend.

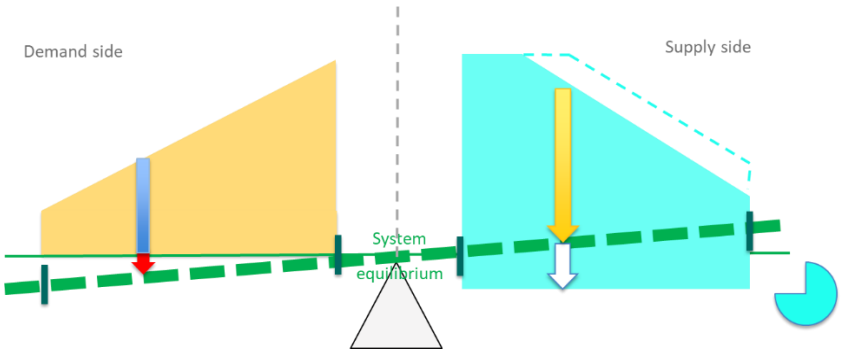


Figure 5. Imbalance due to high uncertainty or intensity

The size of the supply side indicates adaptive capacity in responding to unexpected, unanticipated, surprise or challenging events, relying on skills and competences learned during standard training (yellow "push" forces), combined with individual skills developed and exercised in everyday operations (white "pull" forces). The first component is related to predetermined operating strategies, based on anticipation, predefined responses and the concept of risk. The second one concerns the way socio-technical system generates the behavior that maintains safety. The depth below the equilibrium line on the supply side reflects the extra adaptive capacity.

SEESAW in the context of system changes

After every successfully solved unexpected event, the supply side area is hypothesized to expand. The learning process is established and helps improving safety. The same applies whenever some changes are introduced in the system, like new operational procedures, airspace organisation, introduction of new decision support tools, replacing experienced with young ATCos, etc.

As aforementioned, the introduction of automation expands the boundaries on the supply side, Figure 6 a). It allows higher operational complexity to be absorbed (right boundary), increases capacity and operational efficiency (upper boundary), meanwhile the lower boundary movement depends on trust in automation.

After fully adopting changes in the system, the supply side area moves up, indicating an increase in base adaptive capacity, which is a precondition for the demand side to expand, Figure 6 b).

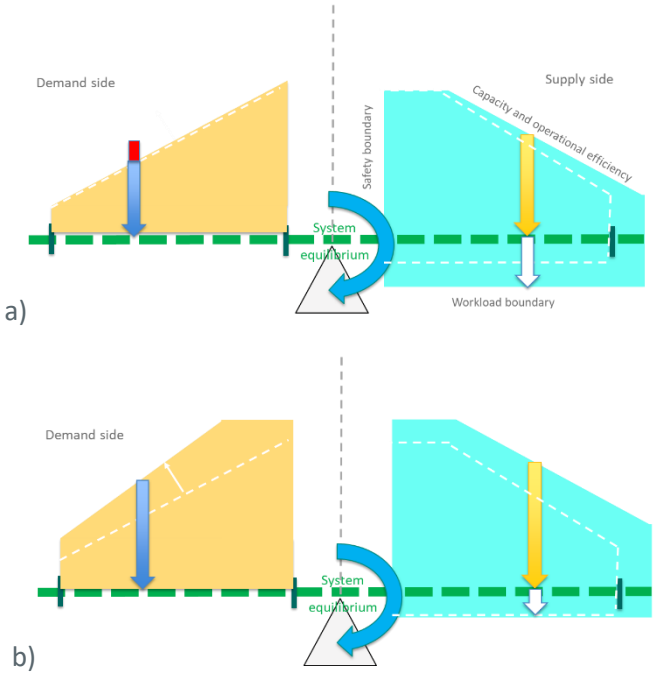


Figure 6. Supply side changes due to automation: a) transition period; b) changes are fully adopted

SEESAW concept illustration

A data-driven approach was used to demonstrate SEESAW concept application. The quantification uses selected parameters to describe the demand and the supply side and is used to compare between scenarios (high vs. low occupancies, before vs. after changes, etc). For illustration purposes, an example with following characteristics will be shown here: High occupancy, Nominal vs. Severe weather scenario.

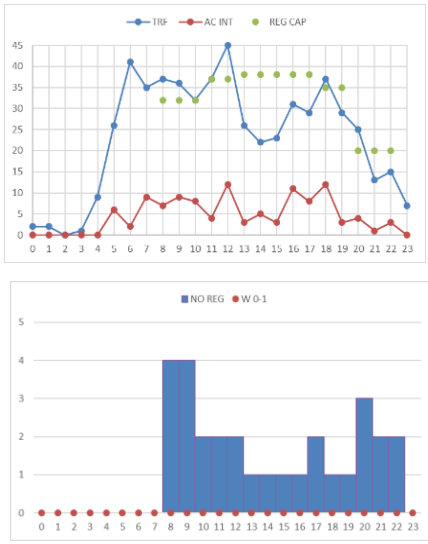
In severe weather scenarios (Figure 7) there is no increase in the maximum number of active sectors during the day, but the sector scheme changes occur more often than in nominal high occupancy scenario (Figure 8). The number of ATCo restrictions per sector is slightly higher in severe weather scenario. In nominal and severe weather scenarios there are periods during the days with traffic above declared capacity (Figure 9).

EUROPEAN PARTNERSHIP

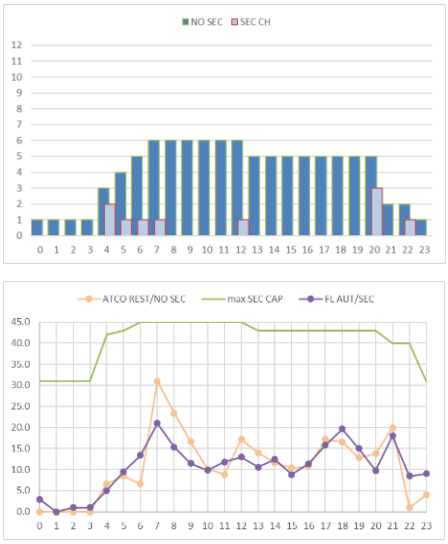
Co-funded by the European Union

NOMINAL CONDITION, AFTER CHANGE: 16-07-2017

Demand side



Supply side



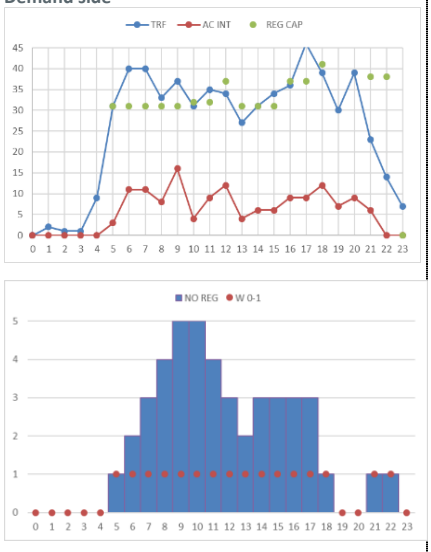
TRF – actual traffic entry count
AC INT – aircraft interactions (<10NM, <300ft)
REG CAP – minimum Total Rate set of all active regulations
NO REG – number of active regulations for the traffic volume LECB
W 0-1 – the regulation is for weather reasons (NO-0, YES-1)

NO SEC – maximum number of active sectors
SEC CH – number of sector changes
Max SEC CAP – maximum capacity of active sectors
ATCO RESR/SEC – number of ATCO restrictions per sector
FL AUT – number of FL authorizations per sector

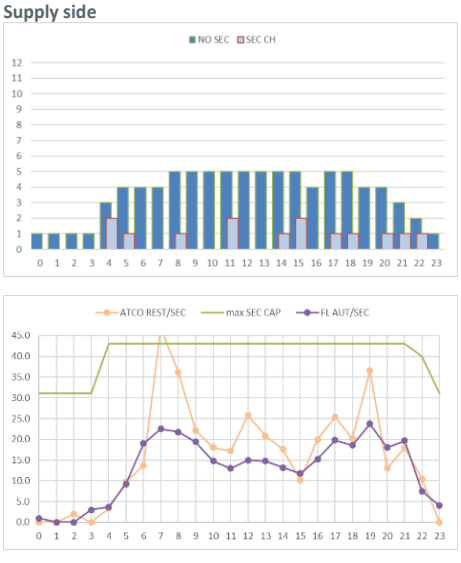
Figure 7. High occupancy, Nominal conditions, after change

SEVERE WEATHER CONDITIONS, AFTER CHANGE: 14-07-2019

Demand side



Supply side



TRF – actual traffic entry count
AC INT – aircraft interactions (<10NM, <300ft)
REG CAP – minimum Total Rate set of all active regulations
NO REG – number of active regulations for the traffic volume LECB
W 0-1 – the regulation is for weather reasons (NO-0, YES-1)

NO SEC – maximum number of active sectors
SEC CH – number of sector changes
Max SEC CAP – maximum capacity of active sectors
ATCO RESR/SEC – number of ATCO restrictions per sector
FL AUT – number of FL authorizations per sector

Figure 8. High occupancy, severe weather conditions, after change

EUROPEAN PARTNERSHIP

Co-funded by the European Union

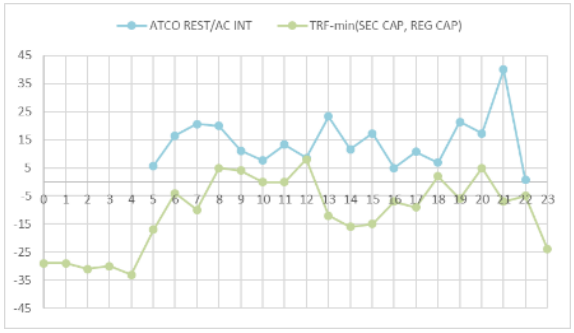
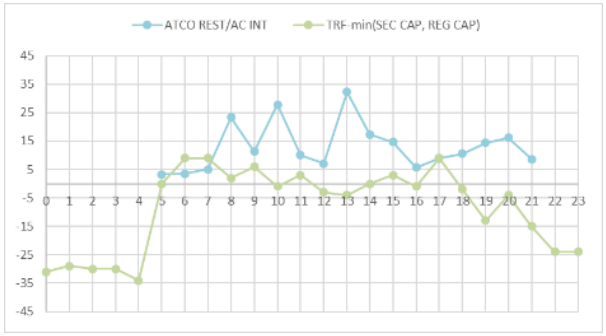
Nominal condition, after change	Severe weather conditions, after change
	
ACTO REST/AC INT - number of restrictions per aircraft interaction i.e. workload to reach and maintain "safe" level of traffic complexity.	TRF-min(SEC CAP, REG CAP) – tactically absorbed capacity (positive values indicate traffic above declared capacity).

Figure 9. High occupancy, Nominal vs. Severe weather conditions, after change

3.2 Introduction to Safety and Resilience Bayesian Network Model

The safety analysis approach proposed in FARO is quantitative, while resilience analysis were traditionally based on a qualitative approach. To bridge this gap in the integration between these two approaches, FARO proposes to build a new model that relies on the Bayesian Network model used for the safety analysis but including additional variables that represent the system's resilient performance. Unlike the BN model developed for safety analysis, which is entirely data-driven, the combined model is proposed to be a Bayesian Belief Network (Safety Resilience-BBN) model combining both the data-driven and knowledge-based approaches.

The SR-BBN model integrates safety variables (relying on the knowledge gained in the safety analysis) and resilience strategies identified as the most relevant in describing the resilient performance, and populate all of them with available data (Figure 10). The SR-BBN model developed is limited to en-route airspace [5].

The first group of variables is related to the separations. It takes into account the planned and actual vertical and horizontal separation of aircraft pairs in their CPA. The second group of variables is related to external and nominal conditions. These conditions refer to effects external to the ATCO that may influence the behaviour and dynamics of the sector. The third group of variables are those related to the strategies applied by the ATCO in a tactical horizon or by the ATM system in pre-tactical or even strategic horizon. The block of ATCO strategies is related to resilient performances, and it is specific per use case (Table 4. Identified ATCO strategies, Table 4).

The application of SR-BBN model showed that it is useful for the prediction of safety outcomes after the changes introduced in the system. Especially important is the sensitivity analysis which enables the user to identify the most influential variables on the target nodes.

Co-funded by the European Union

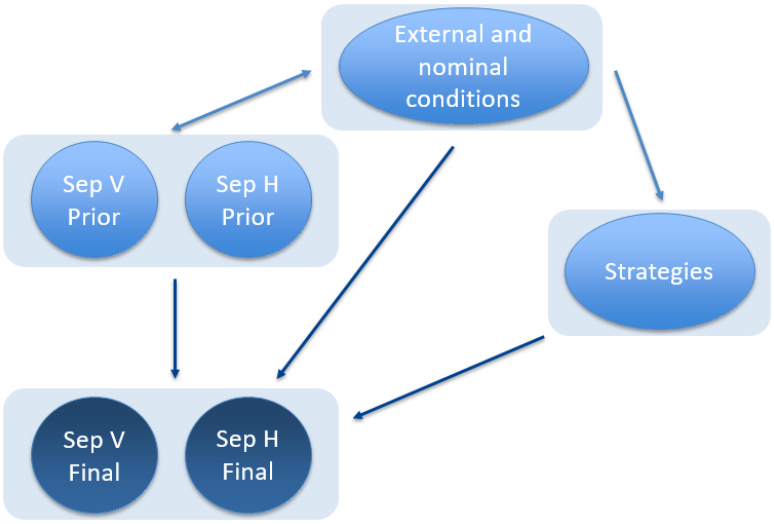


Figure 10. Schematic simplification of the SR-BBN model

Table 4. Identified ATCO strategies [9]

Strategy	Description	Variables
Strategy 1	ODL (Opposite Direction Levels)	The use of ODL to avoid conflict.
Strategy 2	Vertical route management	Use of level changes to avoid conflict.
Strategy 3	Lateral route management	Use of speed changes or lateral deviations to avoid conflict.
Strategy 4	Tactical radar headings	Use of radar heading clearances to avoid conflict.
Strategy 5	Sector split/reconfiguring the airspace	Change of configuration to deal with the excess of demand or unforeseen problem.
Strategy 6	Planned sector capacity (with its buffer)	Planification of the sectorisation is by nature a strategy that adds a buffer for contingency.
Strategy 7	Regulation	Regulation or restriction that affects the operation.

For illustration purposes an example will be shown here: High occupancy, Before vs. After change scenario.

In case of “Before Change” the variable that refers to the sector configuration is Strategy 5, and its value is set to zero while in case of “After Change” its value is set to one. The main changes caused by high occupancy are given in Table 5.

There is an important difference between “Before Change” and “After Change”, and it is that there are significant differences in the use of Strategy 1 and Strategy 2. In the case of Strategy 2, it shows a *decrement* in the use of the Strategy, which indicates that the aircraft follow more procedural strategies in this scenario. In addition, the prevalence of Strategy 7 halves on the case of “Before Change”. Another remarkable change is the presence of “IfWeatherActual” for the “After Change” situation (max deployment), which confirms what the prior knowledge on the UC2 (see D2.2) hinted on the use of this deployment to tackle adverse weather scenarios.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table 5. Main changes between "Before Change" and "After Change"

	"Before Change" (LECBCCC)		"After Change" (LECBCCU + LECBCCL)	
	Standard occupancy	High occupancy	Standard occupancy	High occupancy
Strategy 1	9%	24%	10%	16%
Strategy 2	90%	90%	88%	80%
Strategy 3	5%	7%	4%	4%
Strategy 4	1%	8%	2%	5%
Strategy 6	11%	57%	18%	65%
Strategy 7	11%	76%	7%	36%
IfWeatherActual	4%	64%	2%	2%

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4 Integrated approach requirements

Specific requirements for each step in safety and resilience performance integration process are presented in following text. They have emerged throughout FARO project and are complimentary to those given in D2.3 [12].

4.1 STEP 1: Data management requirements

These guidelines on the data management are summarising in more details requirements related to data in STEPs 2 3 and 4.

Guidelines	Description	Checklist (Has this be done?)
Guideline 1: **Gather experts' requirements on data for their analysis**	**Identify** the basic data associated to the conceptualisation of Safety and Resilience Engineering associated to the change to be analysed. • **Iterate** with experts over metrics and indicators that will be representative of the Safety and Resilience Engineering associated to the changes to be analysed. Generate mock-up visualisations and create narratives on how you would derive these metrics and indicators from basic data that can support the workshops. • **Agree** on a closed definition of metrics and indicators. Include a description on how the metrics are constructed from the basic data as much as possible.	☐
Guideline 2: **Identify the scope of the data.**	Ensure that the data scope is fully set in terms of geographical location and temporal intervals. • **Identify** which temporal intervals must be analysed and the temporal granularity according to Guideline 1 (hourly, daily, 20-min, etc.) • **Identify** limitations in the analysis due to unavailability of data and mitigations looking for fusion of datasets. • **Identify** privacy requirements and agree on **anonymisations** of the data along all the information cycle.	☐
Guideline 3: **Identify appropriate sources of traffic data according to the requirements**	Ensure that the data transformations can be conducted for generating the required metrics and indicators. • **Identify** data sources that fully cover the Guideline 1 (derivation of metrics and indicators) • **Ensure** that the data sources are compliant with the agreed temporal and geographical locations (Guideline 2). • **Identify confidentiality requirements** of the data source and ensure that appropriate provisions and data management actions are included for enforcing them.	☐
Guideline 4: **Data adaptation, association and transformation**	Adaptation of the different data sources and final transformations. • **Associate and conform** the basic descriptive information (for example, *flight identifiers*) along the different data sources to ensure coherency. • **Identify** which information is extracted directly from the raw data or have basic transformations and which information is derived from complex transformations. This step helps to identify the source of potential errors in the final analyses. • **Anonymise the data** as required (Guideline 3.3) • **Verify** the transformations for controlled sets of data against the data requirements with the safety and resilience experts.	☐

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.2 STEP 2: Safety performance functions requirements

Although SPFs have a great potential for safety assessment and predicting, they are complex models based on both knowledge and data, and their development can be a complex and demanding process for an organisation. Here are summarised some of the main requirements and steps of this process.

Guidelines	Description	Checklist (Has this be done?)
Guideline 1: **Identification and access to an optimal set of information**	Safety is intended to be analysed as a systemic factor, therefore, the possible influence of many areas that can be affected must be taken into account. Thus, the organisation must have the ability to collect data from all areas of interest. Without such information it will not be possible to represent the influence of the identified aspects on safety. • Identify the organisational, technical, human and procedural precursors that are used to conceptualise the SPF. The identification of these precursors, as well as the data and variables to support their characterisation and quantification, will determine the optimal set of information that would be desirable for the model. • Identify the limitations due to data availability or other reasons (confidentiality). Not all mandatory data is available for use in the model as data limitations will be encountered that prevent access to the information that would ideally be desired. Identify in the early stages of design the Safety Conceptualisation that will be used for evaluating the model and ensure that the data is available for creating it afterwards.	☐
Guideline 2: **Data processing**	Depending upon the organisation tools and standards, data could require different pre-processing in order to extract from them the features required by the model. • Ensure that the data transformations are feasible, traceable and reproducible. Identify the data requirements derived from the conceptualization of the previous stage.	☐
Guideline 3: **Network development and training**	• **Definition in detail of the structure of the subnetworks**. You should find the causal relationships between the variables, that is, the topology of the Bayesian Network. This structure can be defined directly from the database, or through the knowledge of experts. • **Discretisation of the input variables**. The discretisation of variables consists of converting the variables that are continuous into variables grouped by intervals. This step is necessary, since Bayesian networks consider discrete or continuous variables, but it is not possible to obtain a hybrid model from the data. The discretisation of variables can be based either on statistical characterization or in expert knowledge. **Discretisation should ensure that no information is lost or considered as an excess of states.** • **Obtention of the conditional probability tables for each node**. These tables are obtained directly from the frequencies observed in the data. This process is included in the parametric learning. • Evaluation and verification of model usefulness. For this purpose, a sensitivity analysis has to be carried out. Sensitivity analysis is a technique that can help validate the probability parameters of a Bayesian network The discretization of the input variable is a key stage in this process. Involve experts from early phases of the design stage, as it has a deep impact on the Data Processing (see Guideline 2).	☐
Guideline 4: **Adaption of generic SPF**	The SPF is *Operating Environment* dependent, what means that the generic BN model needs to be adapted for each Operating Environment. That means that the conditional probability tables in the model are specific to each Use Case and have to be learned from data of the specific elements under analysis. The adaptation of the generic model to the	☐

Guidelines	Description	Checklist (Has this be done?)
models to the characteristics of the operating environments analysed	characteristics of the sector analysed in each Use Case implies: • Gathering and processing all the data from the traffic under analysis in the Use Case. Processing involves the discretisation of the data for each model variable. Discretization scheme is knowledge-driven. So far, it cannot be automated and it might be different for each operating environment because it depends on sector features and traffic profile. • Parametric learning, i.e. obtaining the required a priori and conditional probabilities tables from the frequency observed directly from data • Sensitivity analysis using the "tornado" diagram to tune the network and identify the most influential variables for each particular operating environment. • Backward and forward analysis to define thresholds in the variables that might impact safety performance in a scenario, if applicable. • This approach will be carried out subnetwork by subnetwork, so that particularized information can be acquired for each of the defined barriers and lead to a summary of the network as a whole	
Guideline 5: **Analysis of the most influential factors, as well as the applicability thresholds in each of the developed models**	One of the main tasks to be carried out is the application of the model to the case studies in order to quantify the influencing factors of each case study and to determine the criteria and thresholds of applicability of the SPF. • For each subnetwork the variables that have the largest influence in the subnetwork outcome should be identified. A systematic +/-10% probability variation is recommended to be applied to each state of each variable, so the ones producing the highest change in the outcome variable can be identified and retained. The percentage of variation will be used to set some thresholds of variables or states where applicable.	☐
Guideline 6: **Validation of the model**	The basic concept in the validation of the SPF is the goodness of fit of the model. Thus, the validation of the model itself represents the goodness of fit of the whole model. • The goodness-of-fit of the model shall be evaluated by means of *test data*, i.e. not used for the training of the model. • Compare the predicted outcomes of the SPF with the actual ones. A worked example: • SPFs are complex structures. Therefore, a specific validation approach is necessary. Applying classical validation techniques, two different scenarios need to be defined to test the goodness of fit of the entire BN superstructure in each of FARO UCs. The two scenarios represented extreme conditions of the use case. For each scenario, a representative data set was separated from the learning data, and subsequently used to test the predictive ability of BN. Scenario 1 consisted of a set of data with high occupancy rate in the sector and Scenario 2 consisted of a set of data with low occupancy rate in the sector. • The predicted outcomes of the BN (Predicted probability of success of the ATM barriers included in the model and Predicted probability distribution of the vertical and horizontal separation of the aircraft at their CPAs) was compared with the actual ones. To determine the validity of the statistical approach we ensured that we verified the goodness of fit of the complete Bayesian Model is satisfying	☐
Guideline 7: Application of the model to different case studies	Once the model has been adjusted for each scenario and its goodness-of-fit validated, it can be used to assess the impact of changes in a scenario on its safety performance. • Every change to be analysed in a scenario should be fed into the model as a variation in the probability distribution of the parent nodes. The main use of the model is to predict the effects, that is, the probability of the output-child nodes by	☐

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Guidelines	Description	Checklist (Has this be done?)
	setting the probability distribution of the parent-input nodes • Given the new probability distribution of the various input nodes, then the model will propagate these uncertainties through the network and will cause a change in the probability distribution in the outcomes of the network. By varying the probability distribution of the input nodes, it will be possible to predict the probability distribution of the outputs. • Therefore, this is the way to quantify the impact of the change. Thus, it is considered that the "safety practitioner" should define the change in terms of probability impact on entry to the network.	
Guideline 8: Interpretation and Communication of the results	The SPF developed in FARO project are complex tools composed by interconnected BN. The model is quite powerful but also complex and has plenty of details. Interpretation and communication of this information is not an easy task. • Use graphical tools to make this interpretation and communication easier and straightforward, and to support the decision-making process (you may use the ones proposed by FARO. With this type of graphic representation, all the information about a predictive scenario can be summarised into a unique graphic that provides information about the scenario and its traffic and about the impact of safety in terms of vertical and horizontal separation distribution and probability of success/failure of the ATM barriers. Each organisation will need to tune this tool for their own use, and maybe to develop new communications tools bespoke for their own circumstances	

As kind of summary, Figure 11 synthesis the main steps followed in Deliverable D4.2 [6] to apply the SPF to specific Use cases. This could serve as a guideline for safety practitioners on how to apply the models and perform the intended safety studies.

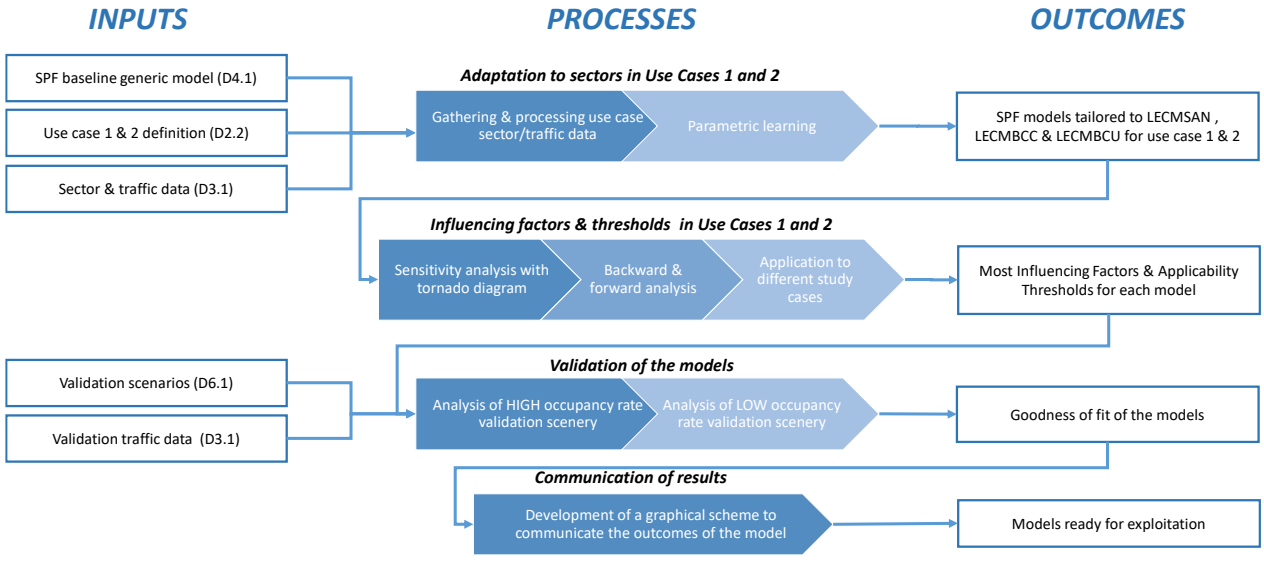


Figure 11. Methodology in Deliverable D4.2 [7]

EUROPEAN PARTNERSHIP
Co-funded by the European Union

4.3 STEP 3: Resilient performance requirements

One of the challenges that FARO has confronted is transforming qualitative narratives of resilient performance that are amenable for use by data science as quantitative data. The approach adopted by FARO as far as possible, is transforming the qualitative data elicited from practitioners into indicator set to explore resilient performance at the micro scale of the work system. That is a proximal view.

Whilst, from several sources, a view of distal i.e., meso and macro scale views were identified, the research was limited to the available data sources principally at the micro scale. Where it was possible, hypotheses of meso and macro dimensions were drawn from an interpretation of the structure and organisation of the work system as well as discussions ANSP staff. For example, one indicator of resilient performance was derived with reference to the declared capacity of sectors as defined through internal processes within the ANSP. In a limited sense, this is a macro scale component that influences the micro and meso scale.

The different scales in which a system (such as the ATM system) can be considered offer significant dimensions of resilient performance at the macro level that influences resilient performance at the meso and micro levels.

To assess or determine changes to resilient performance of the system, the following guidelines are recommended:

Guidelines	Description	Checklist (Has this be done?)
Guideline 1: **Know and understand the system across functional scales (macro, meso, micro).**	• An in-depth knowledge and understanding of the system is required. This can be achieved by implementing a system map to identify relationships between functions, roles and responsibilities, human actors/operators, technological artefacts, procedures, etc. Where is the system boundary? What are the interfaces internal or external to the system that enables system performance? (e.g., Coordination with the Network Manager, adjacent sector groups, other ANSPs, etc). Identify system actors/functions across macro, meso and micro scales and how each level influences the other: one or bi-directional? Is the effect operational or strategic or both? For example, a decision made at the macro level on the number of ATCos to be deployed is managed at the meso level by bandboxing of sectors, reduce demand, reroute of traffic away from the sector and impacts the micro level in terms of increased workload and deployment of strategies to manage tasks. • Involve sharp end practitioners and stakeholders in the system mapping process are essential to gaining a robust understanding of the system. This is especially so as often, there may be system actors or elements (such as informal channels) which are not visible or written down on procedures, but practitioners occasionally rely or draw upon these resources. • It is essential that the individual or team tasked with assessing a system's resilient performance should have broad understanding of Resilience Engineering – its principles, methods, concepts, and tenets [10] [11].	☐
Guideline 2: **Observe Work-as-Done, and speak to those who do the work to**	All procedures, rules, processes, etc., that inform how work is carried out are underspecified and require the human actors to adapt. • Interview and speak to those who do the work (sharp end) to understand the system's capability to adapt to variations in the work environment. Sharp end practitioners are knowledgeable and have built experience & knowledge over a long	☐

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Guidelines	Description	Checklist (Has this be done?)
understand how the system achieves resilient performance	period of time from the work environment. They know what works or does not, can spot cues and pre-empt future criticalities, and deploy/adapt strategies (tactical, strategic) in response to system behaviour and performance. • Observe the work system and how work is undertaken in the operational environment at different levels of the system hierarchy, functional roles, and the contribution of artefacts. Coordination, common ground, dependencies (hidden or otherwise) and availability are all probes that enable an understanding of how the work system achieves resilient performance. The benefit of observing work as done (in addition to interviews) is that it could reveal strategies and forms of adaptation not recalled during interviews but show actions undertaken by the work system to achieve resilient performance (sustain operations). Plan, using the identification of system actors, who interact with whom that have the ability to influence adaptation. A key finding is the nature of coordination and the cost of coordination that can inhibit or restrict adaptive strategies.	
Guideline 3: **Identify/uncover strategy (tactical or strategic; base capacity or extra adaptive capacity) and the intended goal**	Based on the data/information collected through interviews, observation, simulation reports etc (Guideline 1 and 2), identify tactical and strategic strategies and adaptations. The goal of this step is to view each strategy in terms of interpreting the demand (and surrounding contexts, i.e., weather, staffing availability, traffic volume, etc) the system is faced with and how this informs trade-off decisions at macro, meso, and micro abstractions. Bear in mind that units of adaptive behaviour (UABs) are limited by resource availability and as a result, the system adapts by deploying available resources, generating additional resources or reconfiguring the system structurally in a way and manner that sustains system objectives i.e., optimality and sustained adaptability. But that consideration of the coordination costs of such adaptations needs to be added. • Questions to considered and investigated at this stage (may require additional interviews with front end practitioners) is why a particular strategy was deployed and not another? What was the intended goal of the deployed strategy? For example, a sector group may decide to apply regulation/restrictions downstream to manage airspace capacity instead of splitting sectors and putting on more ATCos. The strategies should reveal the system's ability to deploy base adaptive capacity[8] or extra adaptive capacity[9] to manage and deal with the inevitable performance variability that the ATM system confronts and responds to as part of everyday work.	☐
Guideline 4: **Identify strategies that are operational expressions of resilient**	Based on strategies identified, derive dimensions (areas of analysis) of resilient performance that reflect the *reality of operational practice* with respect to 'work-as-done' and suit the specific characteristics of the system as they adapt to sustain operations and production and resilient performance. It is necessary to keep in mind that not all strategies identified from interview texts/observation can be derived from the system data as some may reveal adaptations	☐

[8] The base adaptive capacity will be a repertoire of strategies and responses that can deploy capacity and resources to manage disruptive events. These can take the form of contingency plans or trained strategies that are enacted tactically.

[9] Extra adaptive capacity - existing procedures and training will not be sufficient to manage sustaining performance which may mean solving problems rife with uncertainty and a different tempo needing dynamic problem solution. Adaptation in these circumstances involves adapting to changing situations and adopting novel ways in responding to the changing operational environment.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Guidelines	Description	Checklist (Has this be done?)
performance	and informal strategies deployed in the work system based on the human operator's knowledge and experience of the work that is being done. • Identify areas of analysis that cover the entire spectrum of possibilities with which to explore resilient performance should be identified. For example: ○ Airspace (flow and airspace structure, sector configurations, etc), ○ Operational procedures (strategies used by ATCos for solving and managing traffic flows e.g., use of speed control, managing descent flows, sequencing, etc), ○ Traffic Demand (traffic counts, vertical profile, traffic density), ○ Potential conflict (Number of opposite heading). • Example of strategies/indicators of operational expressions of resilient performance include: ○ Frequency of use of opposite direction levels (ODL) as intermediate cleared level or as a cruising level, ○ Variations of top of descent points to achieve defined coordination conditions (standard transfer levels) for specific flows of traffic, ○ Number of direct routes given tactically, ○ Trade-offs and prioritisation, i.e., number of level offs in the vertical plane for aircraft climbing and descending etc. The indicators reveal patterns how UABs adapt to respond to foreseen and unforeseen (surprise) events and how this have changed or may change (through simulation) in the new organisation, i.e. the controlling techniques, the interaction, dependency, and coordination with other sectors/units.	
Guideline 5: **Select candidate days to enable the evaluation and analysis of the numerical data obtained from system data**	Select candidate days for use in exploring system data that are closely representative of system variability for situations that are both regular or frequent sources of variation as well as for irregular or infrequent situations: • Presence of variable conditions such as weather incidents, CBs, increase in non-scheduled/regular flights, • Days with similar representation in traffic parameters (e.g., traffic mix considering that ATCos task load is informed by the amount of traffic in descent/climb vs. cruise level), • Days with varying peak periods and shoulders around these periods – this provides opportunity to explore in-depth possible causes of the variations in peak periods and identify adaptations and strategies that are thus deployed in response to the variability in the system, • Days with relative similarity between traffic level in situation before and after changes to aid comparison in data with shared similarities and what this means in terms of staff resourcing, number of sectors open/ band boxing, etc. • Day of the month or known events that are known to generally impact the amount of traffic - i.e., Christmas day may be discounted/not selected. By applying one of these criteria in the selection of the candidate days for the analysis, a range of different scenarios (i.e., weather activities, unusual pattern of activity) can be explored to identify characteristics of resilient performance of the ATC sectors and extended adaptability. That is, how the system adapted in response to these variable conditions (e.g., collapse of sectors/band boxing, staff resourcing, etc.).	☐

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Guidelines	Description	Checklist (Has this be done?)
Guideline 6: **Data analysis and synthesis**	Transform selected candidate strategies (Guideline 4) into quantitative data elements to be explored in the analysis of the system's resilient performance after deployment of new design solutions. • Identify indicators and metrics to investigate resilient performance. A worked example: System conditions: The uncertainty around the aircraft entering the sector and its associated entry point at the boundary with adjacent ACCs on transfer to the sector. Identified Strategy: Controllers predict a fix that the aircraft may route to, which provides an initial routing into the sector which is then updated once the aircraft comes on frequency. Parameters (to investigate the strategy) using system data: • Tactical actions to aircraft before sector entry, • Aircraft planned and actual trajectory, • Sector Entry (planned and actual), • Managing route and lateral profiles (Lateral route efficiency). Indicators and Metrics: • Deviation in sector entry points for planned and actual entry. Number of clearances issued per aircraft both for nominal and actual trajectory, • Tactical actions given to aircraft before sector entry, • Routing of aircraft within sector, • Deviation in exit points where aircraft is sent direct to a point in the receiving sector (as a tactical strategy to deconflict traffic) after coordination with the receiving sector. Links to resilient performance: 1. What is the nature of changes to the Planning controller's task? 2. What is the additional workload that is placed on the sector team due to uncertainty in Free Route Airspace? These questions would reveal aspects of resilient performance related to: • Adaptive Behaviour, • Adaptive Capacity, • Sustained adaptability, • Optimality, • Brittleness, • Opportunities, • Trade-offs.	☐

Guideline 7:
 	
Data visualisation and interpretation
	• Use visualisation/graphical imagery to interpret the data.
	• The purpose of the system of indicators and metrics elicited in Guideline 6, is to support and facilitate developing an understanding of resilient performance in the old and/or new organisation.
	• Visualisation of the data based on the indicators/metrics developed, enables
	  ○ elicitation in patterns of activity,
	  ○ use of raw data to provide explanatory power in delving into the differences, and changes in the work systems, and
	  ○ the development of narratives in evaluating the impact of new solutions on the resilient performance of the system.	

EUROPEAN PARTNERSHIP

Co-funded by the European Union

In summary:

- Monitor and understand typical or normal work, where these terms refer to adaptations and how the work system adjusts to patterns of activity that lead to adaptation. Adaptation is typical work: work-as-done and work-as-imagined are two starting points to explore adaptation.
- Some sources of performance variability are very familiar, others are not. Both need to be considered when considering the challenge and surprise events that a work system can be confronted with. Some are in fact elements of the typical work undertaken and in essence tacit knowledge that needs to be elicited.
- Understand and derive the conditions that support or enable adaptations in terms of coordination, procedure, and rule under-specification common ground, etc.
- Understand that resilient performance is an activity that needs to consider cross scale interactions and interdependencies.
- Activities to investigate and assess resilience and resilient performance of the system needs to be undertaken in an ongoing manner, multiple times across the lifecycle of the system as opposed to a one-off exercise. The goal each time being to identify new sources of resilient performance and adaptation (as well as how it may have changed or continues to evolve) as the human element of the system adapts resources, strategies, and activities in response to threats and opportunities.

4.4 STEP 4: SEESAW requirements

The proposed safety and resilience models are designed to assess the impact of changes (airspace design, organization and automation) on safety and resilient performance. Finally, FARO proposes a general SEESAW concept for the integration of these two, aiming to contribute to the overall understanding of safety and resilient performance variables and metrics [1].

In order to quantify SEESAW concept, i.e. safety and resilience performance integration the following requirements should be meet:

Guidelines	Description	Checklist (Has this be done?)
Guideline 1: **SEESAW concept - assessing balance**	In order to determine whether the system is in balance or not, the same units on both sides of the SEESAW need to be used, so the torques can be subtracted. One way to do that is to use risk of conflict as a proxy for both complexity and workload. Risk of Conflict (RoC) for the actual traffic is a proxy for complexity on the demand side (CMP), and risk of conflict for planned traffic is a proxy for controller workload (CWL) on the supply side [INT6]. Complexity and workload represent distances from the fulcrum in the context of lever (SEESAW) mechanism. The ratio between them translates to the ratio between load (traffic volume) and effort (resources/capacity). The following requirements need to be met: • Availability of planned and actual data sets: o for the demand side: actual number of flights per unit of time, actual number of aircraft interactions and existence of severe weather,	☐

Co-funded by the European Union

Guidelines	Description	Checklist (Has this be done?)
	○ for the supply side: maximum sector capacity, regulated sector capacity, planned number of flights per unit of time, planned number of aircraft interactions, • Availability of models for calculation of complexity and workload, i.e. their proxies, expressed in the same unit. • The model used in FARO project to calculate Risk of Conflict from planned and actual traffic the following requirements need to be met: ○ Availability of Flight Trajectories (both planned and actual) - Flight trajectories are used as inputs for the model for calculation of RoC as proxies for traffic complexity and ATCO workload. The provision of flight trajectories data may facilitate calculation of traffic complexity and ATCO workload. Planned as well as actual flight trajectories are necessary. They could be in widely recognised EUROCONTROL DDR2 format or other similar formats. ○ Synchronization of Flight Trajectories (both planned and actual) - Flight Trajectories are presented as sequences of points, were each points correspond to certain time stamp (time moment) and inconstant duration between those points. In order to compare pairs of flight trajectories with aim to discover whether potential losses of separation exist, it is necessary to have synchronized trajectories – meaning their points should correspond to the same time stamps, and duration between points should be constant.	
Guideline 2: **SEESAW concept - scenario comparison**	To use SEESAW concept to compare between series of nominal and non-nominal (severe weather or intruder aircraft) scenarios, demand and supply side of the SEESAW (load and effort side of the lever) do not necessarily need to be expressed in same units. Instead, set of available data can be used to visualize each side. For that purpose, the following requirements need to be met: • Availability of operational data (both planned and actual): ○ for demand side visualization: actual number of flights per unit of time (traffic entry count), actual number of aircraft interactions, number of loses of separation, number of active regulations, regulated capacity (total rate limitation), indication if the regulation is related to weather conditions or not, ○ for supply side visualization: min and max number of active sectors during 1-hour period, max and min sector capacity of all active sectors, number of ATCo instructions, number of sector scheme changes,. Operational data are used to visualize both demand and supply side of the SEESAW through a set of charts. Comparing a series of scenarios with similar demand sides (e.g. Sundays, periods with high traffic volume) enables to track the variation in the 'response' of the supply side, i.e. on its adaptive capacity.	☐

4.5 STEP 5: SR-BBN requirements

The SR-BBN was conceived as a tool that integrates, synthesises and illustrates the different approaches, models and achievements of the FARO project. It is an attempt to bring together and integrate in a predictive Bayesian Network Model the knowledge and data an organization has about its safety and resilience performance, and to achieve a combined and balanced view of the system performance.

One of the challenges of the Safety and Resilience joint assessment is how to integrate the different dimensions of safety and resilience performance that arise from the different scales of ATM system operation (macro, meso and micro levels). It is also a challenge to capture, in a single and integrated view, the interdependences and influences between those scales. This is precisely where BN comes in hand, because of its potential to capture the conditional dependency between variables regardless of their nature. To take advantage of this capability the SR-BBN considers 3 mains groups of variables. The first group of variables is related to safety and separations. The second group of variables is related to external and nominal conditions, which can influence the behaviour and dynamics of the sector. Finally, the third group of variables are those related to the strategies applied by the ATCO in a micro or meso scale or by the ATM system at the macro scale.

However, this type of modelling requires that the organization has previously gained experience in the areas developed by FARO: predictive safety modelling, safety and resilience performance indicators and data-driven assessment, and the SESAAW concept. It also requires that the organization has become familiar with the use of BN technology.

In order to be able to jointly and predicatively assess safety and resilience performance of the system through a BN, the following guidelines are recommended.

Guidelines	Description	Checklist (Has this be done?)
Guideline 1: **Build a multidisciplinary team with expertise in S&R performance assessment, data management and predictive modelling using BNs.**	The advances and the FARO proposal have only been possible thanks to a group of experts on these domains who have been able to work together as an integrated team, applying and combining their knowledge into new processes and products. Additionally, this team needs to have themselves a deep understanding of the system under analysis. They also need to complement this technical knowhow with skills and abilities required to elicit and capture system interrelationships from direct interaction with practitioners and stakeholders, and to transform this knowledge into quantifiable information, quantitative data elements and models.	☐
Guideline 2: **Have accomplished a prior assessment of safety and resilience of the ATM system in accordance with FARO guidelines.**	Safety and resilience performance indicators should be derived and reported from data. As discussed in the previous guidelines for safety and resilient performance requirements, this is not an easy straightforward process. A deep understanding of the system is required, as well as a strong technical background on safety, resilience, data management and modelling. Organisations have to go through a process and a learning curve that cannot be skipped. Each organisation needs to develop its own safety and resilience models and resolve all the difficulties that will be encounter during the process. Both, performance analysis, safety and resilience, are scenario dependant and have to be defined for each system and condition. Before being able to accomplish a more complex integrated S&R analysis, organisations need to master individual approaches, and deploy and implement a systematic framework that allows them to perform the assessment in its full extension and communicates their results.	☐
Guideline 3: **Familiarise and gain experience with the general**	Although safety and resilience perspectives are complementary, the proposed models are quite different on nature and methodologies (one is quantitative and the other one qualitative), which makes their integration counter-intuitive. The lever mechanism exemplified by the SEESAW concept also requires the organisation to gain real and practical experience in its adaptation and application in order to	☐

Guidelines	Description	Checklist (Has this be done?)
concept of S&R integration and exercise the SEESAW approach according with FARO guidelines.	understand and interiorise the principles of a combined safety and resilience performance analysis.	
Guideline 4: **Identification of Key S&R indicators and variables for a joint integrated analysis**	Safety and resilience analysis proposed in FARO are very detailed models that provide a deep understanding of the system performance from both points of view. A combined Safety & Resilience analysis involves a higher level of abstraction, and requires an effort to identify which elements from the original whole safety and resilience analysis needs to be addressed by the integrated SR-BBN. The development of a SR-BBN needs to achieve a balance between the details and depth of the information and variables in of the model and their complexity. Since the scale and dimensions of both safety and resilience can be different, their integration implies and exercise of synthesis and abstractions to identify the elements that the model should retain in terms of safety and separations; external factors and nominal conditions, and applied strategies. Practitioners shall make use of the information provided by the SPFs and resilience models to filter and select the dimensions that are more relevant to defining the integrated S&R model.	☐

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Conclusion

The integration between Safety and Resilience Engineering methods has the potential to facilitate the understanding and evaluation of interdependencies between competing goals. These methods facilitate the understanding on how a change in the operating system (human, technology, organisations) can impact in the balance between safety and resilient performance.

Proposed models for the integration of Safety and Resilience Engineering (SEESAW and SR-BBN) are both adapted only for en-route environment (FARO use cases are just illustration, but the experience gained through this approach could be used much broader, i.e. for other use cases as well). They are complementary models as they should be used by organisations that reached different levels of safety and resilient performance analysis.

SR-BBN model can be used by organizations with mature data-bases, as detailed post-ops data are needed to successfully build and train Bayesian Belief Networks. Furthermore, such an organisation should also have advanced level of resilient performance awareness, with already identified sources of adaptive capacity (strategies). Familiarisation with BBN models is necessary in order to use the full potential of such model, like the prediction of safety outcomes after the changes introduced in the system, identification of the variations in the use of strategies, or identification of the most influential variables on the target nodes, etc.

On the other hand, the SEESAW concept is meant for organizations that only begin with resilient performance monitoring. It enables differentiating between base and extra adaptive capacity, and identify periods in time where one should look for the sources of adaptive capacity. In the next step, strategies can be determined e.g. by interviewing ATCos.

The benefits of using FARO methodologies (S&R Guidelines) are mainly allocated to the provision of safety benefits through a better understanding of the effects of changes. From a methodological perspective related to Performance Management, FARO's SPFs can be used to understand better the impact on safety levels of a specific operational improvement or a technological enabler. With regard to Resilience Engineering, the benefits are mainly allocated to the ability of exploring how the system (at all levels) is producing safety. At SEESAW level, apart from the benefits that may bring the evaluation of the interdependencies, the main benefit for the organisations is the identification of scenarios where the system was maintaining throughput because of resilience.

FARO S&R Guidelines could be considered to be added to the SESAR Safety Reference Material [14] and in the Guidance for its application [15], and also for reviewing the existent ones in relation to Resilience Engineering (Annex J).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

6 References

[1] FARO Consortium, “D2.1 Project Scope,” Brussels, 2020.

[2] FARO Consortium, “D2.2 Case Studies,” Brussels, 2020.

[3] FARO Consortium, “D6.1 Validation plan,” Brussels, 2021.

[4] FARO Consortium, “D4.1 Safety Performance Functions Methodology,” Brussels, 2021.

[5] FARO Consortium, “D5.1 Resilience Model Description,” 2021.

[6] FARO Consortium, “D6.2 Validation Report,” Brussels, 2022.

[7] FARO Consortium, “D4.2 Applicability of Safety Performance Function,” 2021.

[8] E. Hollnagel, “Safety II in practice: developing the resilience potential,” 2018.

[9] FARO Consortium, “D5.2 Applicability of the Resilience Model,” SJU, Brussels, 2021.

[10] J. Rasmussen , “Risk management in a dynamic society: a modelling problem,” *Safety Scince,* vol. 27, pp. 183-213, 1997.

[11] A. W. S. &. J. M. C. Schraagen, “ Measuring Workload Weak Resilience Signals at a Rail Control Post,” *IIE Transactions on Occupational Ergonomics and Human Factors,* vol. 2, no. 3-4, pp. 179-193, 2014.

[12] FARO Consortium, “D2.3 Data, Computing and Visualization Requirements,” Brussels, 2022.

[13] T. Saurin, “Criteria for Assesing Safety Performance Management Systems: Insights from Resilience Engineering,” *In Eds Nemeth and Hollnagel, E Resilience Engineering Practice ,* vol. 2 Becoming resilient, 2014.

[14] SESAR JU, “SESAR 16.06.01b Application of Resilience Guidance to Multiple Remote Tower and ASAS S&M: SJU 2016 Safety Reference Material,” SJU, Brussels, 2016.

[15] SESAR JOINT UNDERTAKING, “D4.0.060 SESAR Safety Reference Material. Edition 00.04.01,” Brussels, 2018.

[16] SESAR JOINT UNDERTAKING, “D4.0.050 Guidance to Apply SESAR Safety Reference Material. Edition 00.03.01”.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix A

A.1 Glossary of terms

Term	Definition	Source of the definition
Acceptable Level of Safety Performance	The minimum level of safety performance of civil aviation in a State, as defined in its State Safety Program, or of a service provider, as defined in its Safety Management System, expressed in terms of safety performance targets and safety performance indicators.	SM ICG
Adaptive Capacity	The potential for modifying what worked in the past to meet challenges in the future; adaptive capacity is a relationship between changing demands and responsiveness to those demands, relative to goals.	D5.1
Base Adaptive Capacity	The base adaptive capacity will be a repertoire of strategies and responses that can deploy capacity and resources to manage disruptive events. These can take the form of contingency plans or trained strategies that are enacted tactically.	**D51**
Extra Adaptive Capacity	Existing procedures and training will not be sufficient to manage sustaining performance which may mean solving problems rife with uncertainty and a different tempo needing dynamic problem solution. Adaptation in these circumstances involves adapting to changing situations and adopting novel ways in responding to the changing operational environment.	**D5.1**
Air Traffic Services Unit	A unit, either civil or military, responsible for providing air traffic services in a given airspace.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
Airspace User	The operator of the aircraft at the time when the flight is performed or, if the identity of the operator is not known, the owner of the aircraft, unless it can be proved that another person was the operator at that time.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
Area control centre	A unit providing air traffic services to controlled flights in its area of responsibility.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
Aviation System	The people, organisations, equipment, technology, and regulatory environment that interact to enable the development, production, operation, maintenance, and training associated with aircraft and aircraft components.	SM ICG
Best (good) practice	A method, initiative, process, approach, technique, or activity that is believed to be more effective at delivering a particular outcome than other means. It implies accumulating and applying knowledge about what is working and what is not working, including lessons learned and the continuing process of learning, feedback, reflection, and analysis.	EASA NPA 2019-10(B)
Brittleness	The sudden collapse or failure when events push the system up to and beyond its boundaries for handling changing disturbances and variations. Insufficient graceful extensibility to manage the risk of saturation of adaptive capacities.	Woods, 2015 Woods, 2018
Consequence	Actual or potential impact of a hazard that can be expressed qualitatively and/or quantitatively. More than one consequence may evolve from an event.	SM ICG

Co-funded by the European Union

Term	Definition	Source of the definition
Error	Non-intentional action or inaction by a person that may lead to deviations from accepted procedures or regulations.	SM ICG
Exceptional event	Circumstances under which ATM capacity is abnormally reduced so that the level of air traffic flow management ('ATFM') delays is abnormally high, as a result of a planned limitation induced through operational or technical change, major adverse weather circumstances, the unavailability of large airspace parts either through natural or political reasons, or industrial action, and the activation of the European Aviation Crisis Coordination Cell ('EACCC') by the Network Manager.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
Failure	The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.	FAA Safety Handbook, Appendix A
Functional System	A combination of procedures, human resources, and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions.	Commission Implementing Regulation (EU) 2017/373 of 1 March 2017[10]
Graceful Extensibility	Graceful extensibility is the opposite of brittleness, where brittleness is the sudden collapse or failure when events push the system up to and beyond its boundaries for handling changing disturbance and variations. Graceful extensibility is the ability of a system to extend its capacity to adapt when surprise events challenge its boundaries	Woods & Branlat, 2015 Woods, 2015 Woods, 2018
Hazard	A condition that could cause or contribute to an aircraft incident or accident	ICAO Annex 19 (2nd ed.)
Hazard Analysis	Part of the system processes for hazard identification.	SM ICG ICAO Doc 9859 (8.4.9.10)
Hazard Identification	A method for identifying hazards related to the whole organisation (operational + systemic hazards). Hazard identification focuses on conditions or objects that could cause or contribute to the unsafe operation of aircraft or aviation safety-related equipment, products, and services	SM ICG ICAO Doc 9859 (2.5.2.1)
Human Factors	Understanding the ways in which people interact with the world, their capabilities, and limitations, and influencing human activity to improve the way people do their work.	ICAO Annex 6, Part I, Definitions ICAO Doc 9859 Safety Management Manual
Incident	An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.	ICAO Annex 13

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0373&from=EN

Co-funded by the European Union

Term	Definition	Source of the definition
Likelihood	The frequency, in quantitative or qualitative terms, that an unsafe event may occur.	SM ICG
Loss of Separation	A defined loss of separation between airborne aircraft occurs whenever specified separation minima in controlled airspace are breached. Minimum separation standards for airspace are specified by ATS authorities, based on ICAO standards. A loss of separation between aircraft which are responsible for their own separation by visual lookout is not subject to definition. Usually, the occurrence of a 'near miss', termed an AIRPROX by ICAO, is defined only by the opinion of one or more of the parties involved, whereas Near Mid-air Collision (NMAC) is an AIRPROX that meets specified criteria.	https://www.skybrary.aero/index.php/Loss_of_Separation
Medium Risk	A level of risk that may be acceptable with review by the appropriate authority but tracking and management are required.	SM ICG
Occurrence	An accident or incident or another undesired safety-related event.	SM ICG
OCCURRENCES RELATED TO AIR NAVIGATION SERVICES AND FACILITIES Aircraft-Related Occurrences	(1) A collision or a near collision on the ground or in the air, between an aircraft and another aircraft, terrain or obstacle (1), including near-controlled flight into terrain (near CFIT). (2) Separation minima infringement (2). (3) Inadequate separation (3). (4) ACAS RAs. (5) Wildlife strike including bird strike. (6) Taxiway or runway excursion. (7) Actual or potential taxiway or runway incursion. (8) Final Approach and Take-off Area (FATO) incursion. (9) Aircraft deviation from ATC clearance.	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1018
Organisational Hazard	Hazards which arise from an organisation's policies, priorities and the manner in which work is carried out.	SM ICG
Performance Based Standards	Standards that use a set of performance metrics to determine whether the system is operating in accordance with design expectations.	SM ICG
Predictive	Any method that continuously analyses current and historical information to forecast potential future occurrences.	SM ICG
Reliability Factor (RF)	The level of confidence in the results of the scoring using the RAT methodology based on the available safety data related to a given occurrence.	RAT Guidance Material, Version 2.0
Risk	Risk' refers to safety risk and means the combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect. *[EASA NPA 2019-10(B)]* The assessed predicted likelihood and severity of the consequence(s) or outcome(s) of a hazard. *[SM ICG]*	EASA NPA 2019-10(B) SM ICG
Risk Management	An organisational function that assesses the organisation's system design and verifies that the system adequately controls risk. A formal risk management process describes a system, assesses hazards, analyses	SM ICG

Co-funded by the European Union

Term	Definition	Source of the definition
	those hazards to evaluate the risk, and establishes controls to manage those risks.	
Risk of Collision	The risk classification of an aircraft proximity in which serious risk of collision has existed.	ICAO Doc 4444
Runway incursion	Any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle, or person on the protected area of a surface designated for the landing and take-off of aircraft.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
Safety	The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level.	ICAO Annex 19 (2nd ed.)
Safety Assurance	Processes used to ensure risk controls developed under the risk management process achieve their intended objectives throughout the life cycle of a system. This process may also reveal hazards not previously identified and identify or assess the need for new risk control, as well as the need to eliminate or modify existing controls. This is one of the four components of SMS.	SM ICG
Safety culture	The shared beliefs, assumptions and values of an organisation and is part of the organisational culture.	EASA NPA 2019-10(B)
Safety Culture	An enduring set of values, norms, attitudes, and practices within an organisation concerned with minimizing exposure of the workforce and the general public to dangerous or hazardous conditions. In a positive safety culture, a shared concern for, commitment to, and accountability for safety is promoted.	CASA 3
Safety Data	A defined set of facts or set of safety values collected from various aviation-related sources, which is used to maintain or improve safety.	ICAO Annex 19 (2nd ed.)
Safety Impact	For the determination of the occurrences with 'safety impact' that are used for monitoring runway incursions (RIs) and separation minima infringements (SMIs), only a subset of the occurrences that may represent a risk to aviation safety should be selected. The indicators set out in point 1.2(a) and 1.2(b) of Section 2 of Annex I should include occurrences whose safety risk grade is red or amber in the European Risk Classification Scheme (ERCS) matrix. These are the indicators at Member State level. The indicators set out in point 1.2(c) and 1.2(d) of Section 2 of Annex I should include occurrences whose risk analysis tool (RAT) ground severity classification is A, B, or C. These are the indicators at airport or ANSP level.	EASA NPA 2019-10(B)
Safety Information	Safety data processed, organized, or analysed in a given context so as to make it useful for safety management purposes.	ICAO Annex 19 (2nd ed.)
Safety Management	An organisational function that strives to continually identify all safety hazards and to assess and manage the associated safety risks through a systematic approach that includes the necessary organisational structure, accountabilities, policies, and procedures.	SM ICG

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Term	Definition	Source of the definition
Safety Management System (SMS)	A systematic approach to managing safety, including the necessary organisational structures, accountability, responsibilities, policies, and procedures.	ICAO Annex 19 (2nd ed.)
Safety Performance	A State or a service provider's safety achievement as defined by its safety performance targets and safety performance indicators.	ICAO Annex 19 (2nd ed.)
Safety Performance Function	Predictive models of safety events as a function of organisational, technical, human, and procedural precursors to characterise and predict safety-related occurrences. Safety performance functions main characteristics are that it is a non-linear safety quantification methodology, flexible, and capable of accommodating different type of features.	FARO D4.1
Safety Performance Indicator	A data-based parameter used for monitoring and assessing safety performance.	ICAO Annex 19 (2nd ed.)
Safety Performance Target	The State or service provider's planned or intended target for a safety performance indicator over a given period that aligns with the safety objectives.	ICAO Annex 19 (2nd ed.)
Safety Risk	The predicted probability and severity of the consequences or outcomes of a hazard.	ICAO Annex 19 (2nd ed.)
Safety Risk Management	A process used to assess system design and verify that the system adequately controls risk. A formal risk management process describes a system, assesses hazards, analyses those hazards to evaluate the risk, and establishes controls to manage those risks. This is one of the four components of SMS.	EASA
SEESAW	A Concept for Safety and Resilience Integration. SEESAW uses an analogy of a lever mechanism to demonstrate safety and resilience synergy and help Air Navigation Service Providers to better understand the relationship between the two. It aims to provide a high-level understanding on the balancing between the traffic demand side (including the uncertainties) and Air Traffic Control available resources on the supply side that considers Air Traffic Controllers on their working positions within a given Area Control Centre unit, tools and working procedures.	FARO D6.1
Separation minima infringement	A situation in which prescribed separation minima were not maintained between aircraft.	COMMISSION IMPLEMENTING REGULATION (EU) Regulation 2019/317
System Description	A description of an aviation organisation's system including its structure, policies, communications, processes, products, and operations to understand critical factors for the purpose of identifying hazards. It is updated whenever there is a newly introduced element or change to the internal or external situation that could affect risk.	SM ICG

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union