Safety Evolution Guide:

Safety by Design, SA 8.1

Tempest

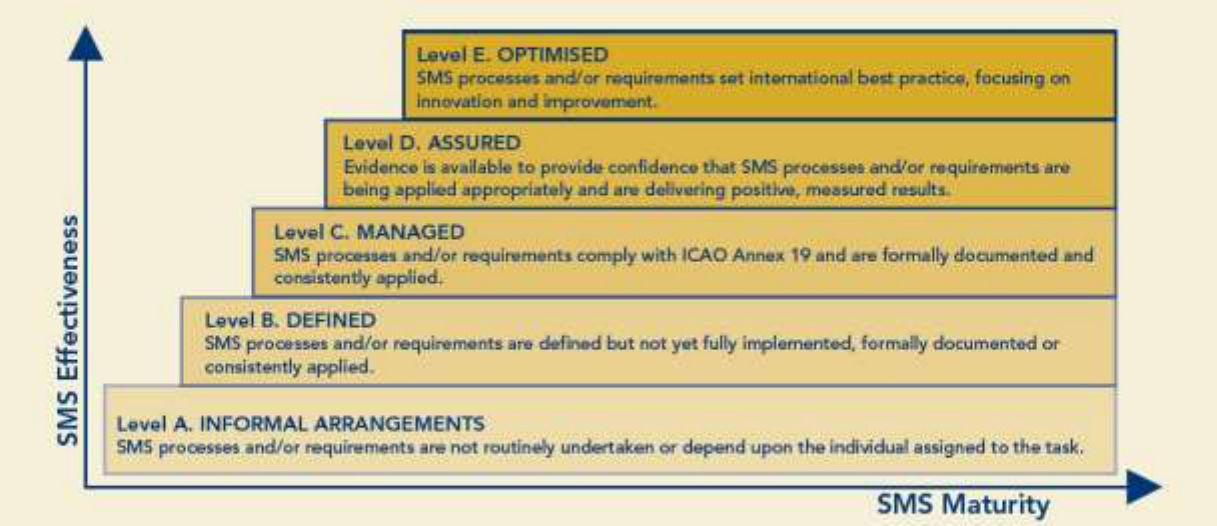
An Evolution Guide for an SMS practice which has been recognised as Optimised by the CANSO Safety Standing Committee

1. OBJECTIVE OF GUIDE

Members of the Civil Air Navigation Services Organisation (CANSO) are committed to the improvement of their services. As part of this commitment, organisations share their practices in efforts transfer learning across the industry.

This guide captures:

- The practices of an Air Navigation Service Provider (ANSP) in one element of the CANSO Standard of Excellence (SoE) in Safety Management System (SMS).
- The practices of this ANSP have been recognized by their peers as being an optimised practice within the industry (see Figure 1).
- The optimised practices have been selected on the basis of their novelty, innovation or the recognition of their potential to manage operational risks.



Level E. OPTIMISED
SMS processes and/or requirements set international best practice, focusing on innovation and improvement.

Level D. ASSURED
Evidence is available to provide confidence that SMS processes and/or requirements are being applied appropriately and are delivering positive, measured results.

Level C. MANAGED
SMS processes and/or requirements comply with ICAO Annex 19 and are formally documented and consistently applied.

Level B. DEFINED
SMS processes and/or requirements are defined but not yet fully implemented, formally documented or consistently applied.

Level A. INFORMAL ARRANGEMENTS
SMS processes and/or requirements are not routinely undertaken or depend upon the individual assigned to the task.

2. APPLICATION OF THE GUIDANCE

CANSO recognizes that this guidance will not be relevant to all ANSPs. The maturity of any ANSP's Safety Management System will be dependent on their specific context. This context will be a reflection of factors including the size and complexity of the organisation, domestic regulations and the risk appetite of the organisation.

ANSPs do not necessarily need to adopt all the practices and processes promoted by CANSO but may consider the relevance of the practices promoted in this guide to their operational environment.

3. OPTIMISED PRACTICE

This guide addresses a SMS process which was identified in 2018 as being optimised, it details how one Air Navigation Service Provider, NATS, is actively implementing its safety policy through a safety strategy and associated implementation plan. The approach was reviewed by a panel of experts from the Future Safety Working Group of the Safety

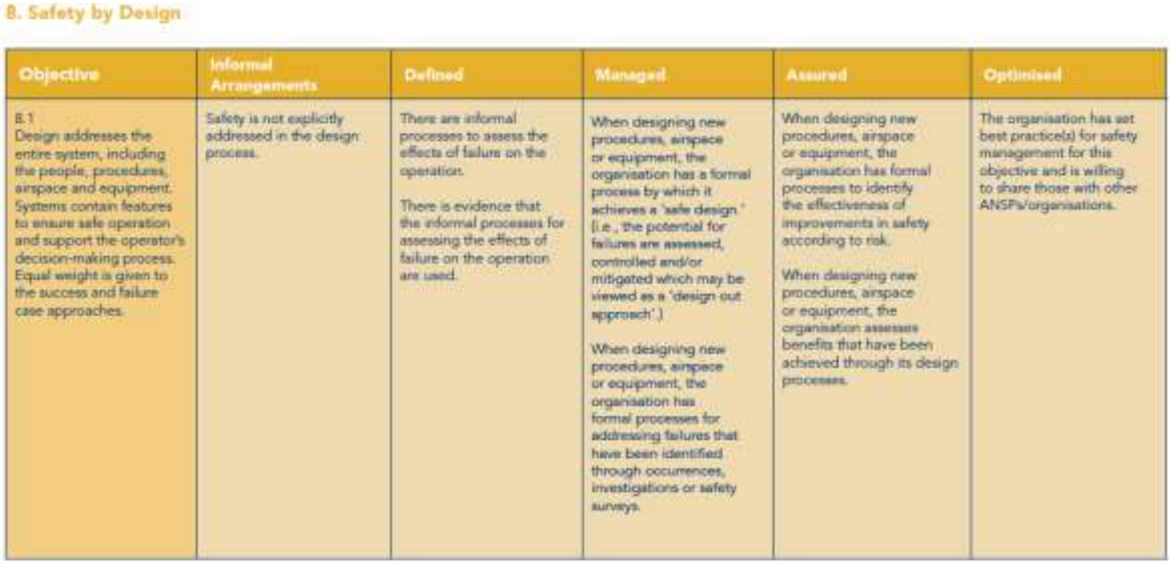
Standing Committee. The approach meets CANSO's requirements for SoE in SMS Study Area SA 8.1 (see below).

4. SCOPE OF GUIDE

This guide aims to provide an insight into what NATS has done in terms of designing and implementing its Safety by Design process, detailing why this approach was taken. Examples of the type of activities are included in this guide to provide a starting point for other ANSP's wishing to adopt a similar outcome from implementation of a safety strategy.

5. APPLICABLE STANDARDS AND REQUIREMENTS

CANSO Standard of Excellence in Safety Management Systems



8. Safety by Design

Objective	Informal Arrangements	Defined	Managed	Assured	Optimised
8.1 Design addresses the entire system, including the people, procedures, airspace and equipment. Systems contain features to ensure safe operation and support the operator's decision-making process. Equal weight is given to the success and failure case approaches.	Safety is not explicitly addressed in the design process.	There are informal processes to assess the effects of failure on the operation. There is evidence that the informal processes for assessing the effects of failure on the operation are used.	When designing new procedures, airspace or equipment, the organisation has a formal process by which it achieves a 'safe design' (i.e., the potential for failures are assessed, controlled and/or mitigated which may be viewed as a 'design out approach'.) When designing new procedures, airspace or equipment, the organisation has formal processes for addressing failures that have been identified through occurrences, investigations or safety surveys.	When designing new procedures, airspace or equipment, the organisation has formal processes to identify the effectiveness of improvements in safety according to risk. When designing new procedures, airspace or equipment, the organisation assesses benefits that have been achieved through its design processes.	The organisation has set best practice(s) for safety management for this objective and is willing to share those with other ANSPs/organisations.

Extract from CANSO Standard of Excellence in Safety Management Systems

https://www.canso.org/system/files/CANSO Standard of Excellence in Safety Management Systems.pdf

6. PREDICTING SAFETY BENEFITS

Tempest is a method to estimate the potential safety benefits and disbenefits that will be realised by major projects and operational change. The safety benefits are assessed in terms of the effect on NATS ATM Ground Points as assessed using the Eurocontrol Risk Analysis Tool (RAT). The Tempest model is based on the barrier model that lies behind the RAT. The effect on each element of the RAT on any change to the operational system is assessed using a combination of operational data and expert judgement. Rather than trying to model the way the score is applied (there is considerable room for interpretation and judgement in the scoring mechanism despite the comprehensive guidance) the Tempest model has been based on the historical RAT score. This data-driven approach uses the scores as they have been assigned by investigators when evaluating changes to the system and then evaluates how system changes might impact these scores.

Using historical data in the model has the advantage that the scores represent the reality of how the RAT has been applied to real events. RAT has been applied formally since January 1st, 2015 with past events being back marked since January 1st, 2011. The scoring is considered to be complete and reliable from January 1st, 2013. The baseline data sample used by the model will increase with ongoing usage.

The Tempest Framework (based on a simplified process flow broken down into the elements of the RAT).

The operational data and expert judgement information is combined with a prediction of how the RAT score might change with the predicted growth in traffic to produce an overall forecast of future safety performance.

This safety by design forecast method is used in NATS to assess the overall programme of change and identify any shortfalls in performance against our targets or opportunities for additional improvement.

7. METHODOLOGY

7.1 RAT METHODOLOGY

The Eurocontrol RAT scoring method has five different versions depending on the type of occurrence being evaluated and the type of ATM operation involved. The Tempest method is based on the version of the RAT used to evaluate incidents involving loss of separation between two or more aircraft. The basic structure of this model is illustrated in Figure 1.

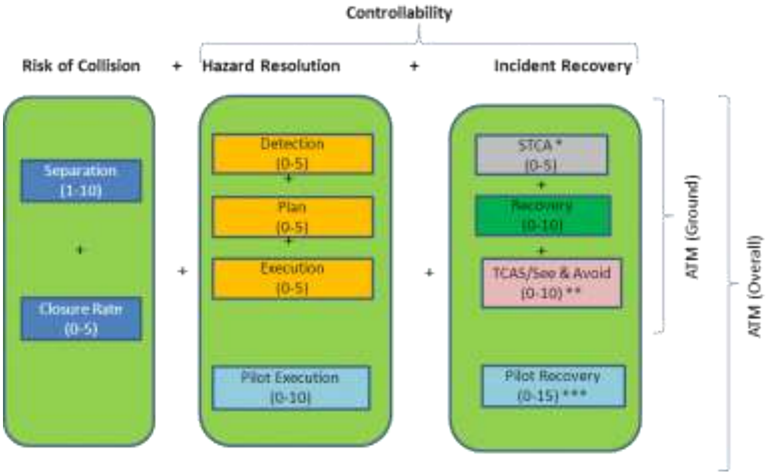


Figure 1: Schematic view of RAT Scoring for Incidents with More than One Aircraft

The RAT score has two components, ATM (Ground) for the score assigned to the ATM service provider and ATM (Overall) including the contribution from Pilot Execution and Pilot Recovery. The scores for ATM (Ground) and ATM (Overall) are calculated as the points that each of the elements in Figure 1 receives.

The score for Separation (relative to the required minimum) plus the score for Closure Rate (at the point of loss of separation) is described as 'Risk of Collision' although it might be better described as a geometry score[1].

The 'Risk of Collision' is assigned to ATM (Ground) if ATC caused the incident or contributed to its occurrence.

The Hazard Resolution score has three components for ATC: Detection of conflict, plan for resolution and Execution of resolution. The Pilot resolution has a single score for Execution.

'Incident Recovery' gives a score for the effectiveness of the controller and pilot recovery actions (these are the actions that occur after the point of loss of separation or imminent loss of separation). Scores are applied to the ATM Ground side if STCA does not work correctly or if TCAS or See and Avoid actions by the pilot were required to resolve the conflict. The TCAS/See and Avoid points do not count towards the Overall ATM score but are only added to the ATM Ground Score. The pilot incident recovery score can also be increased if the pilot reacts incorrectly to a TCAS Resolution Advisory.

The score for Hazard Resolution plus Incident Recovery is described as 'Controllability'. 'Severity' is the sum of 'Risk of Collision' and 'Controllability' shown in RAT barrier model framework in Figure 2.

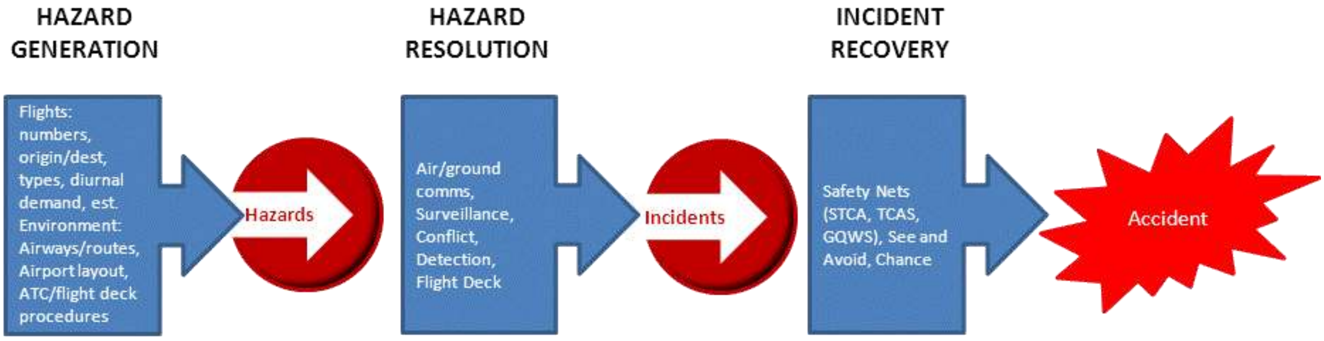

HAZARD GENERATION
Flights: numbers, origin/dest, types, diurnal demand, est. Environment: Airways/routes, Airport layout, ATC/flight deck procedures
Hazards
HAZARD RESOLUTION
Air/ground comms, Surveillance, Conflict, Detection, Flight Deck
Incidents
INCIDENT RECOVERY
Safety Nets (STCA, TCAS, GQWS), See and Avoid, Chance
Accident

Figure 2: The Barrier Model behind the Eurocontrol RAT

[1] The Eurocontrol Risk Analysis Tool documentation uses different terminology to that commonly used in safety management and defines some common terms such as risk and severity in a unique way.

7.2 THE TEMPEST FRAMEWORK

For the ATM (Ground) element of the RAT, the process begins with the generation of a pre-LoS event (i.e. a conflict) due to traffic trajectories and airspace design. A pre-LoS event is a situation in which the trajectories of the aircraft are such that some action is required to prevent a loss of separation. Changes to airspace design or network management can alter the number of pre-LoS events. Traffic levels are also an important factor in conflict generation. However, initially Tempest seeks to assess the relative effect of operational changes excluding any traffic changes – the effect of traffic is considered when forecasting future performance.

The pre-LOS event can then be resolved either by a pre-tactical planning process or by the tactical controller. The resolution is broken down into three functions – Detect, Plan and Execute in line with the RAT. Changes to any of these functions may change the effectiveness of the resolution.

When a Loss of Separation occurs, the rate of closure at the point of LoS is then assigned a score. This may change if the geometry of encounters is altered, e.g. if more or less encounters involve head-to-head trajectories. The closest point of approach relative to the separation minimum is also assigned a score. This score might alter if the separation minimum changes. These two geometry factors do not influence the relative accident risk but do impact the RAT score.

Once a loss of separation has occurred the system has an opportunity to recover the LoS and restore separation. Systems to alert the controller to a LoS or improve the resolution function may alter the Recovery score. Systems that support the pilot may also help resolve a LoS and reduce the risk of an accident although this will not impact the RAT ATM (Ground) score. Figure 3 shows this process flow.

To evaluate the potential impact of an operational change the performance of each element of the model following the proposed change is evaluated relative to its performance in the baseline scenario. For instance, if an airspace change is expected to reduce the number of potential loss situations by 20% through the implementation of procedurally separated routes then the generation element of the process will reduce the number of pre-LoS events by a factor of 0.8.

Multiplying the relative changes in Generation, Resolution and Recovery together gives an approximate estimate for the relative reduction in accident risk. The relative change in Closure Rate and Separation at the Closet Point of Approach [CPA] is included in the model to help estimate the effect on the overall RAT score although it does not directly influence the predicted change in accident risk in the Tempest model.

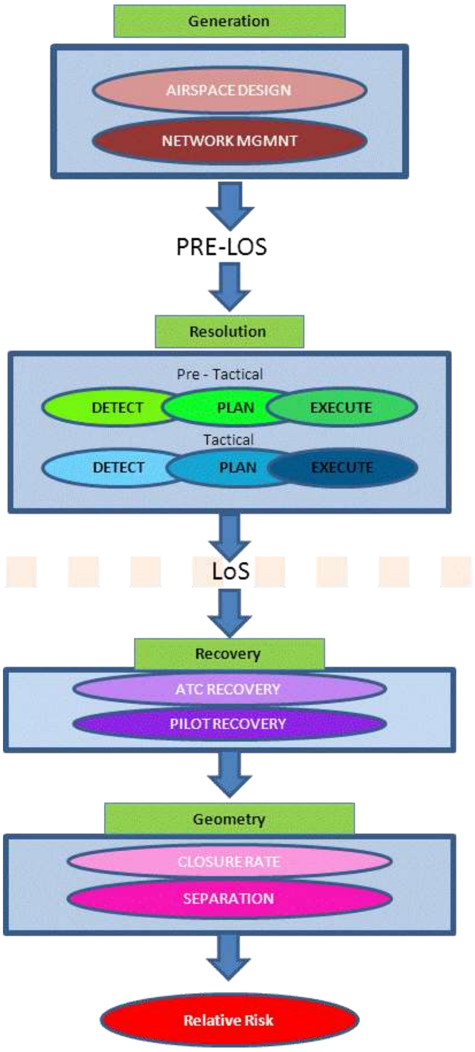


Figure 3: ATM Ground Process Flow for Tempest

8. ESTIMATING THE CHANGE IN RAT SCORE

As the overall RAT ATM (Ground) Score is only indirectly related to the probability of an accident, the expected value of the RAT cannot be calculated by simply multiplying the baseline RAT score by the relative risk estimate. Instead, each individual component of the RAT score needs to be considered separately and adjusted according to the changes in the elements of the model that might affect it. It is necessary to make some simplifying assumptions in order to achieve this.

The aggregated baseline ATM (Ground) RAT score is broken down into six components: Detection, Plan, Execute, Recovery, Separation and Closure Rate. The guidance document for the RAT evaluations states that the default score for Plan should be the same score as for Conflict Detection and that the Execution score should not normally be less than the Plan score.

Therefore, any score for late Detection will be duplicated in the score for Plan and Execution and hence the total number of RAT points accrued from late detection will be three times greater than the points allocated to Detect. The aggregate scores attributed to Detect have therefore been adjusted accordingly for use in Tempest. Similarly, the points for Plan and Execution have also been adjusted as shown in Table 1. This adjustment leaves the total number of points attributed to Resolution the same but redistributes them across the components.

Resolution Component	Aggregated Score	Adjusted Score
Conflict Detection	D	3xD
Plan	P	2x(P-D)
Execution	E	(E-P)
Total	D+P+E	3D+(2P-2D)+E-P = D+P+E

Table 1: Adjusted RAT Resolution Scores

To calculate the impact of a change on the RAT ATM (Ground) score, the points from the six individual elements are multiplied by the appropriate estimated relative changes. Since there is only one route through the model (see Figure 3) any change to an element of the model affects that element and all of the subsequent elements of the model.

9. USEAGE

The Tempest model is used as part of the NATS Safety Benefits process to assess whether investment is likely to result in an appropriate improvement in safety as measured by the number of RAT points. It allows us to predict whether we will meet our own internal safety targets and is also used in discussion with our customers on the levels of investment required to improve or maintain an acceptable level of safety performance.

10. SUMMARY

The practices in this guide present an example of how one ANSP has designed and implemented a safety by design process to estimate the potential safety benefits and disbenefits that will be realised by major projects and operational change.