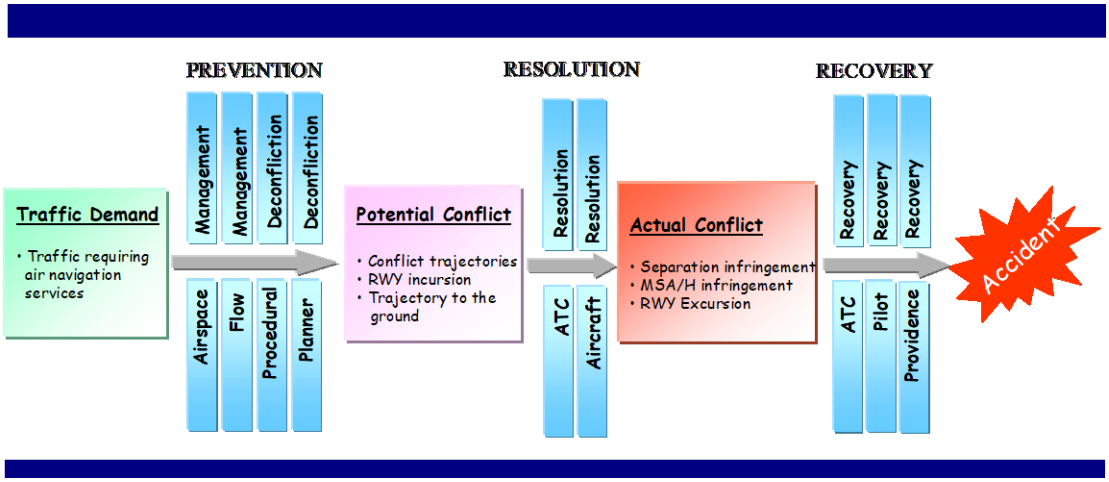
I

GUIDANCE MATERIAL:

BARRIER ANALYSIS

This Guidance Material provides information on one possible way to perform a barrier analysis for ATM such as illustrated in the figure here after.



In this barrier model described in the figure here above, the following terms mean:

- ***Prevention*** of potential conflicts, like airspace design, flow management, procedural de-conflicting of the routes;
- ***Resolution*** of potential conflicts, like ATCO instructions;
- ***Recovery*** from actual conflicts, like ACAS supported avoiding action;

- **Traffic Volume (Demand)**. Risk of mid-air collision is roughly proportional to the square of the traffic, and risk of the collision with the ground or with obstacle on the ground is roughly linearly proportional to the traffic; and/or
- **Potential Conflict**. Potential conflicts (Level Bust, Runway Incursion, Conflicting trajectories on the ground and in the air, Conflicting trajectory to the ground, Unauthorised Infringement of airspace) are adverse operational situations, which can become actual conflict (incident) if certain credible conditions are fulfilled (like presence of another aircraft in proximity); and /or
- **Actual Conflict:** such as separation infringements, Minimum Safe Altitude Infringements, Runway Excursions etc.

This Barrier model is based on EUROCONTROL SPF (Strategic Performance Forecast) which is using a NATS study. This material does not intend to assess the safety aspects of an EATMP Programme but to help EUROCONTROL management to assess its safety importance in terms of potential for risk and benefit/improvement.

The following paragraphs provide guidance material for safety assessment based on a simple conceptual framework that shows where risk might arise in any ATM system. The model is intended to provide a relative assessment of safety (compared to an existing or baseline system) rather than a full quantification of risk. However it is possible that, with sufficient data, a quantified risk assessment using an adaptation of the basic model might be possible.

It should be stressed that the intention is not to produce a detailed and comprehensive Guidance Material for the Safety Assessment Methodology. It is rather to provide a simple, easy to apply method that is sufficiently flexible to be used to assess the high-level safety implications for any future concept.

The safety assessment framework is based on a high level conceptual model of how risk can arise in any ATM system. (For the purposes of this paper the term ATM system is taken in its widest possible sense and includes both ground and airborne elements.) The conceptual model is built around three types of safety-related events: Accidents, Incidents and Critical Events. The definitions for Accidents and Incidents are those given by ICAO and SRC, and are given in Table I-1. The safety targets for ATM systems are defined in terms of both accidents and incidents. The idea of a Critical Event has been developed specifically for use in this safety assessment framework. An example of a critical event is a pair of aircraft on conflicting paths, where failure to change the path of one or both aircraft would result in a loss of separation.

The principal assumption behind the conceptual framework is that for each type of accident there are associated incidents and, for each type of incident, associated critical events. For instance, for mid-air collisions the associated incident would be a loss of separation between a pair of aircraft and the associated critical event would be a pair of aircraft on conflicting paths. Different phases of flight have different characteristic accidents, incidents and critical events. It should be noted that the process described here does not cover one possible type of ATM related accident. In theory it would be possible for ATM to cause an accident by providing an instruction that resulted in an aircraft performing an unsafe manoeuvre not involving a conflict with another aircraft or object (for instance slowing down below stall speed). The framework does not yet take account of this type of problem.

ACCIDENT (from ICAO)	An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which: a) a person is fatally or seriously injured as a result of: • being in the aircraft, or • direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or • direct exposure to jet blast, except when the injuries are from natural causes, self-inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew; or b) the aircraft sustains damage or structural failure which: • adversely affect the structural strength, performance or flight characteristics of the aircraft, and • would normally require major repair or replacement of the affected component except for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damages limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin; or c) the aircraft is missing or is completely inaccessible. Note 1.-For statistical uniformity only, an injury resulting in death within thirty days of the date of the accident is classified as a fatal injury by ICAO. Note 2.- An aircraft is considered to be missing when the official search has been terminated and the wreckage has not been located.
INCIDENT (from JAA)	An occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation.
CRITICAL EVENT	An occurrence in which an appropriate (ATM) action is required to avoid a loss of separation between two aircraft or between an aircraft and another object.

Table I-1: Definition of Terms

Table I-2 lists different types of ATM related accidents and their associated incidents and critical events.

PHASE OF FLIGHT	ACCIDENT	INCIDENT	CRITICAL EVENT
En-route	Mid-air collision	Loss of separation	Conflicting aircraft pair
En – route, Approach or Departure	Wake Vortex Accident	Wake vortex encounter	One aircraft passes through a region where the vortex of a preceding aircraft might be
Approach or Departure	Controlled Flight Into Terrain on approach / departure	Deviation from approach / departure path leading to loss of separation with terrain or object on ground	Points on approach / departure path where deviation could lead to loss of separation.
Take-off or Landing	Runway collision (between two aircraft or an aircraft and another vehicle)	Runway Incursion, Uncleared Landing, Uncleared Take-off	Conflicting: Runway crossing, line up, landing or take-off
Taxi	Taxiway collisions (between aircraft and another mobile vehicle)	Uncleared/Incorrect manoeuvre, Incorrect clearance	Taxi conflict event
Taxi	Taxi collision with static object (permanent or temporary)	Uncleared/Incorrect manoeuvre, Incorrect clearance	Taxi past obstacle

Table I-2: ATM Accidents and Their Precursors

Within this conceptual framework the ATM system can minimise risk by controlling the number of critical events that occur, by preventing critical events developing into incidents and by stopping incidents from becoming accidents. Hence there are three safety-related functions of an ATM system:

- Critical Event Generation,
- Critical Event Resolution; and

- Incident Recovery.

Figure I-1 shows this high level framework schematically. Any of the three ATM safety functions can be affected by the introduction of an OI (Operational Improvement). The following sections of this paper describe simple models for each of the three ATM safety functions that are designed to help determine what effect a particular OI might have. These models are designed to be generic and applicable to most situations. However, in some situations it might be necessary to develop additional elements to provide a comprehensive analysis.

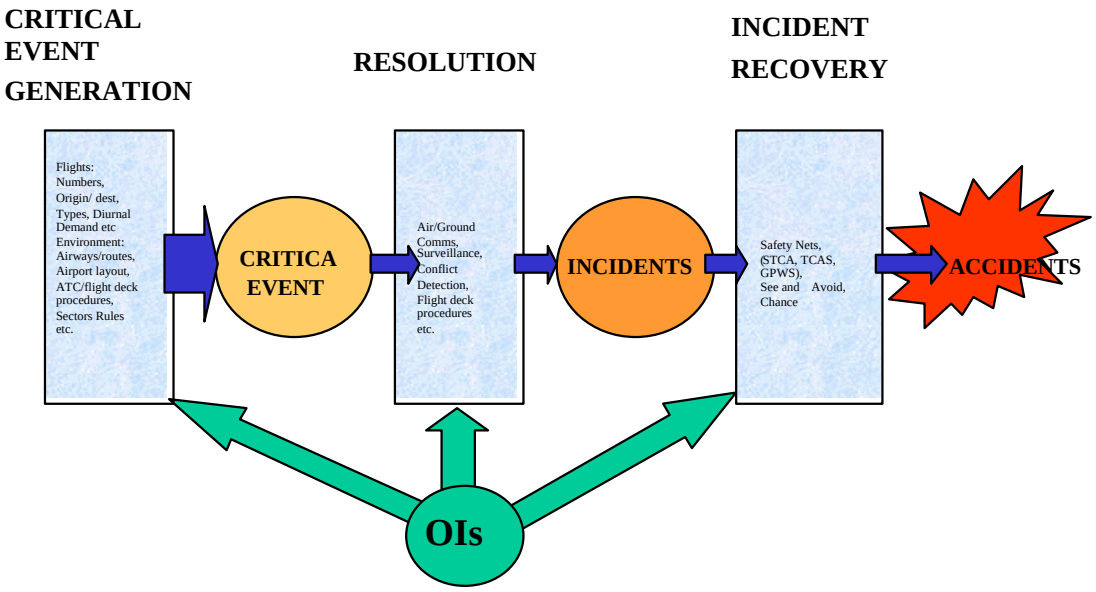


Figure I-1: The High Level Conceptual Model

The generation of critical events is potentially the most complex part of the model. There is very little information on critical events for existing systems as these are normal elements of any ATM operation. Therefore the model proposed for generation is necessarily very simple and also very difficult to validate.

The generation model has three main elements. These are traffic, environmental factors and procedural de-confliction. Each of these is described in the following sections. Figure I-2 shows a schematic representation of the conceptual model for critical event generation.

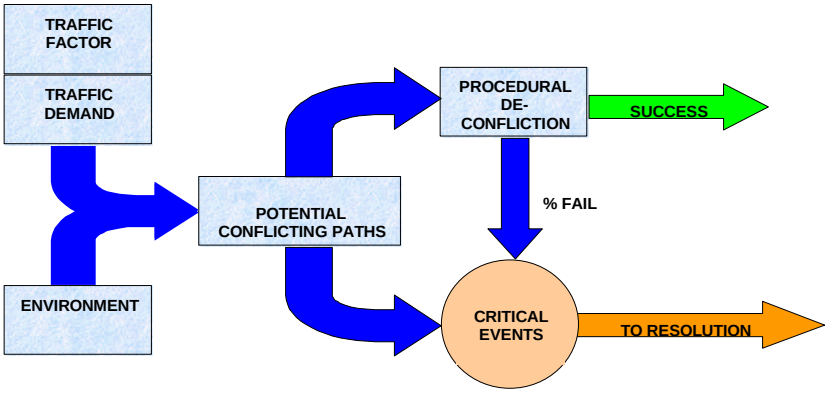


Figure I-2: Critical Event Generation

All critical events (by definition) involve aircraft interacting with other aircraft or objects. Therefore the most important element in generating critical events is the number of aircraft that pass through the ATM system. Most OIs will not in themselves change the traffic levels. If the traffic levels do change, the effect on the number of critical events will depend on whether they involve interactions between pairs of aircraft or between aircraft and other objects.

If the critical event of interest is conflicts between pairs of aircraft then the number of events will increase with the square of the traffic flow. If interactions between aircraft and other objects is of interest then this type of critical event can be expected to increase linearly with traffic. Within the model this difference is included using a parameter called the Traffic Factor. The traffic factor takes the value 2 for critical events involving pairs of aircraft and 1 otherwise.

There are many other factors that will also affect the generation of critical events. These include, but are not limited to:

- Separation Minima,
- Other Traffic (at airports),
- Airspace Design,
- Taxiway/Runway Design (at airports),
- Ground Obstacles.

Together all of these elements are described as environmental factors. If an OI is expected to change any of these factors then it will be necessary to estimate how this change might affect the number of critical events. It is not possible to provide a fully generic method for taking account of these environmental factors and each OI will need to be considered separately.

In order to include the effect of environmental factors it is necessary to estimate what the relative number of critical events will be after the implementation of the OI (with the same traffic).

In some OIs, systemisation might be used to reduce conflicts between aircraft. This can be achieved by providing flights with detailed de-conflicted routes, either on a flight by flight basis or by the application of general rules (the use of Standard Instrument Departure (SID) routes is a common example of this). This type of de-confliction is described in the model as procedural de-confliction.

Two parameters are required for procedural de-confliction:

- *The proportion of critical events that are resolved by procedural de-confliction process; and*
- The proportion of time that the process fails (either because of an error/inaccuracy in the de-confliction or due to failure of an aircraft to follow.

In order to link Critical Events to Incidents a model of the key elements in the resolution process is required. Resolution can be thought of as a four-phase process as follows:

- Detect the Critical Event
- Develop a Solution
- Deliver the Solution
- Execute the Solution

Figure I-3 shows the model for resolution schematically.

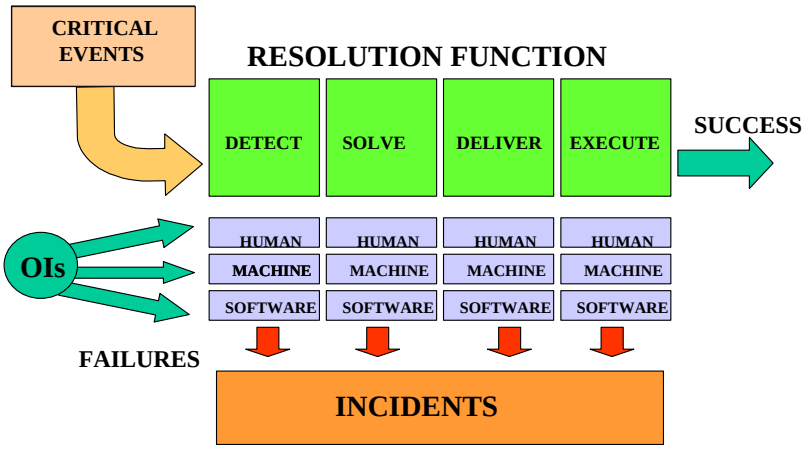


Figure I-3: The Resolution Process

For example, in a tactical radar environment a controller would detect a pair of aircraft on conflicting paths using the radar display system, then determine how to solve the conflict and finally deliver appropriate instructions to the pilot(s) of the aircraft. The pilot(s) would then execute the solution by changing the path of the aircraft. A failure in any of these stages of resolution is assumed to lead to an

incident. (This is of course not entirely true, for instance a pilot might make an error in execution that does not lead to an incident, but this factor will make little difference in most practical applications.)

Each of the resolution functions could be undertaken by a combination of human operators, equipment and software systems. In order to assess the impact of an OI on the resolution function some understanding of how this process works in the current system (or a baseline system) is required. An OI will only change the resolution function if either the type of critical event changes (for instance a change in the geometry of conflicts making them more difficult to detect) or if one or more of the resolution functions are affected.

If the OI is expected to alter resolution it will be necessary to have some understanding of how it works in the baseline system and the relative importance of each of the resolution functions. It should be possible to categorise incidents according to which element of the resolution process failed and then make some estimates of how these relative failure rates will change with the introduction of the OI.

For some OIs there may not be any data on performance available from specifications or simulations. In this case it will be necessary to use approximations. The SPF Safety Group agreed the following simple guidelines, based on their experience of safety assessments. If the task involves a human task the failure rate can be assumed to be between 10^{-3} and 10^{-4}. If it involves a complex software system a failure rate of 10^{-5} can be used. If it is a well proven mechanical system or a simple software system a failure rate of 10^{-6} can be used. If a task involves more than one element then the value for the least reliable of the elements should be used. For instance, if the detection function involves a radar system detecting an aircraft (10^{-6}), a software system processing and displaying the information to a controller (10^{-5}) and a controller using the radar display to detect a conflict (10^{-4}) then the failure rate is 10^{-4} . These are clearly only very crude values and it should be possible to model most systems more accurately using human factors analysis, fault trees etc.

A large percentage of all ATM incidents involve human error either as a causal or contributory factor. In the resolution process, the human operator has a significant role to play in the detection of the critical event, the development of a solution, the delivery of the solution, and the execution of that solution. For this reason, it is necessary to ensure that the failure rate of the human operator is considered when attempting to evaluate the impact of an operational improvement on safety.

In order to ensure that the contribution of human error is adequately considered, it is necessary to determine the ways in which the operator can fail, and the frequency with which these failures are likely to occur.

This section describes each of these processes in turn, beginning with the determination of the ways in which human operators can fail.

A great deal of work has been undertaken in the last three years by EUROCONTROL and NATS to develop tools and methodologies for the analysis of human error in ATM incidents. The general principles involved in such methodologies are the identification of the forms of human error that occur as part of an incident, and the decomposition of these errors to determine the

psychological mechanisms behind the error, and hence the reasons why the errors occur.

With regard to the development of a model of human error for the Strategic Performance Framework, such research provides a great deal of information on how human operators can fail. At a high level, errors fall into a number of categories associated with the task that is being performed (e.g. radar monitoring, strip handling, etc.). Each of these errors can have a number of underlying causes (e.g. judgement, planing or decision-making failure, perception and vigilance failures). The ultimate cause of an error is the psychological mechanism that results in the operator making an error. Such mechanisms include perceptual tunnelling (when the operator focuses on one particular situation at the expense of all others) and information processing failure (where the operator's information processing system is unable to cope with the type or quantity of information presented).

For the purposes of considering the human operator as part of the overall assessment of safety, it is not necessary to consider the underlying psychological causes. For a reasonable estimate of how the operator can fail it is adequate to derive an approximate probability of task errors.

For the purposes of the analysis of human errors in ATM incidents, a taxonomy has been developed for task errors, which is shown in Table I-3 below, alongside the relevance of each error type to the stages of the resolution process.

Task Error	**Detect**	**Solve**	**Deliver**	**Execute**
Separation Error	✓	✓		
Controller-Pilot Communications Error			✓	✓
Radar Monitoring Error	✓	✓		✓
Aircraft Observation / Recognition Error (TWR Only)	✓	✓	✓	
Co-ordination Error	✓	✓		
Flight Progress Strip Usage Error	✓	✓		
Control Room Communications Error	✓	✓	✓	
Handover / Takeover Error	✓	✓		
Aircraft Transfer Error	✓	✓		
Operational Materials Checking Error	✓	✓		
HMI Input & Functions Use Error	✓	✓	✓	✓
Training, Supervision or Examining Error	✓	✓	✓	✓

Table I-3: Task Errors and Applicability to the Resolution Process

An analysis of one year's worth of AIRPROX data was conducted on these error categories to determine the approximate frequency of each error type. Published AIRPROX data from 1997 relating to ATC errors in civil airspace were used, over which period there were 1,179,000 civil traffic movements.

Table I-4 shows the number of errors observed in each category along with an approximate error probability per traffic movement.

Task Error	Number	Probability
Separation Error	0	0
Controller-Pilot Communications Error	55	4.66×10^{-2}
Radar Monitoring Error	14	1.19×10^{-2}
Aircraft Observation / Recognition Error (TWR Only)	0	0
Co-ordination Error	4	3.39×10^{-3}
Flight Progress Strip Usage Error	8	6.79×10^{-3}
Control Room Communications Error	2	1.70×10^{-3}
Handover / Takeover Error	2	1.70×10^{-3}
Aircraft Transfer Error	0	0
Operational Materials Checking Error	0	0
HMI Input & Functions Use Error	1	8.48×10^{-4}
Training, Supervision or Examining Error	18	1.53×10^{-2}

Table I-4: Number of Observed Errors in 1997, and Approximate Error Probability.

A number of error types are new to the taxonomy this year (separation error, aircraft observation / recognition error, and aircraft transfer error) and therefore 1997 data relating to the error type was not available. In the case of 'operational materials checking error' none of the 1997 incidents involved this error type.

The above information has been incorporated into the algorithms of the resolution module, as shown in Figure I-4 and Figure I-5. Changes to the system, procedures, training, etc which may impact on these error types are recorded in the model in the same way as the hardware and software factors. The resulting probability of human failure is propagated upwards into the resolution matrix where it is combined with the effects of hardware and software changes and fed forward into the recovery module.

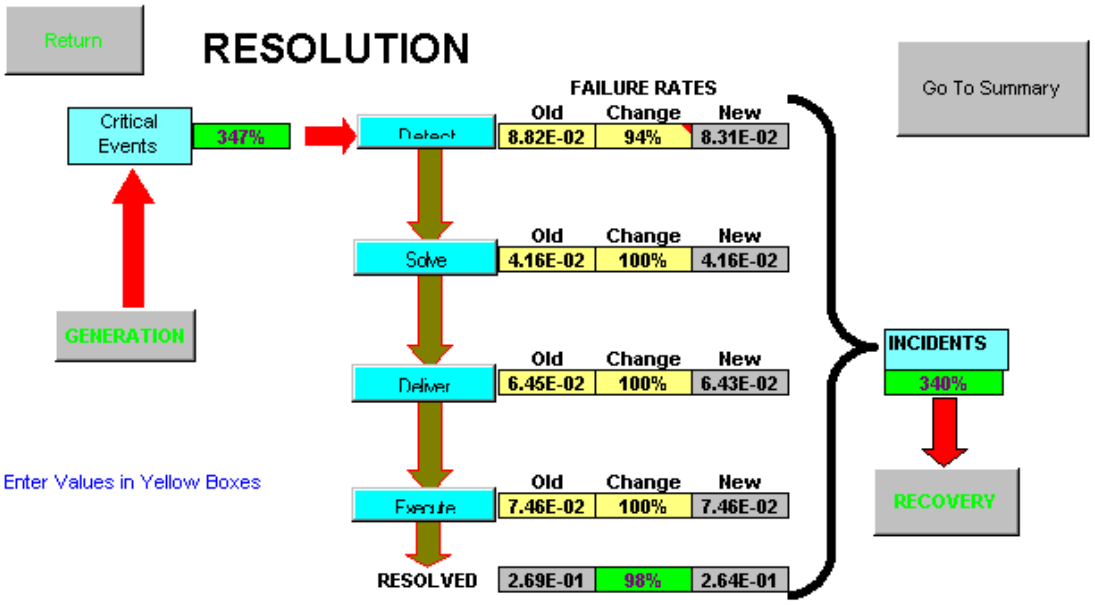


Figure I-4: Resolution Module

When evaluating a future operational improvement, the user would be required to estimate to what degree the human error types represented in the model would be affected by the operational improvement. This need not be a complex process – the introduction of a position handover checklist could reduce the number of handover errors by 10%.

The error probabilities described here are estimates based upon a limited data sample, and are intended to serve as reasonable estimates of baseline human error probability. The relative change in probability as calculated within the SPF model is also at present a relatively crude method of assessing the effect of future systems. However, if more robust data were required, predictive error analysis could be used later in the project lifecycle using prototypes of future operational improvements. Studies of future NATS systems using our predictive error analysis tools have predicted 95% of errors later observed during simulations.

Clearly, the probability that a human operator will make an error does not merely affect the resolution of the conflict, it also has a strong influence on the recovery from the situation, which will be discussed further after.

DETECT

	Old	Change	New
Separation Error	0.00E+00	100%	0.00E+00
Controller - Pilot Comms	4.66E-02	100%	4.66E-02
Radar monitoring	1.19E-02	100%	1.19E-02
Aircraft Observation/Recognition	0.00E+00	100%	0.00E+00
Co-ordination Error	3.39E-03	100%	3.39E-03
FPS Usage Error	6.79E-03	60%	4.07E-03
Control Room Comms Error	1.70E-03	100%	1.70E-03
Handover/Takeover Error	1.70E-03	50%	8.48E-04
Aircraft Transfer Error	0.00E+00	50%	0.00E+00
Operational Materials Checking	0.00E+00	100%	0.00E+00
HMI Input & Funtions Use Error	8.48E-04	100%	8.48E-04
Training, supervision, examining	1.53E-02	90%	1.37E-02
TOTAL:	8.82E-02	94%	8.31E-02

Rank

SOLVE

	Old	Change	New
Separation Error	0.00E+00	100%	0.00E+00
Radar Monitoring	1.19E-02	100%	1.19E-02
Aircraft Observation / Recognition	0.00E+00	100%	0.00E+00
Co-ordination	3.39E-03	100%	3.39E-03
FPS Usage Error	6.79E-03	100%	6.79E-03
Control Room Communications	1.70E-03	100%	1.70E-03
Handover/Briefing	1.70E-03	100%	1.70E-03
Aircraft Transfer Error	0.00E+00	100%	0.00E+00
Operational Materials Checking Error	0.00E+00	100%	0.00E+00
HMI Input & Functions Use Error	8.48E-04	100%	8.48E-04
Training, supervision, examining	1.53E-02	100%	1.53E-02
TOTAL:	4.16E-02	100%	4.16E-02

Rank

DELIVER

	Old	Change	New
Controller - Pilot Communications Error	4.66E-02	100%	4.66E-02
Aircraft Observation / Recognition Error	0.00E+00	100%	0.00E+00
Control Room Communications Error	1.70E-03	90%	1.53E-03
HMI Input & Functions Use Error	8.48E-04	100%	8.48E-04
Training, Supervision and Examining Error	1.53E-02	100%	1.53E-02
TOTAL:	6.45E-02	100%	6.43E-02

Rank

EXECUTE

	Old	Change	New
Controller - Pilot Communications Error	4.66E-02	100%	4.66E-02
Radar Monitoring Error	1.19E-02	100%	1.19E-02
HMI Input & Functionms Use Error	8.48E-04	100%	8.48E-04
Training, Supervision and Examining Error	1.53E-02	100%	1.53E-02
TOTAL:	7.46E-02	100%	7.46E-02

Rank

Figure I-5: Human Error in the Resolution Module

The model for incident recovery described here is illustrated schematically in Figure I-6. It divides incidents into three domains depending on the mechanism that acted to prevent if from resulting in an accident. These domains are defined as follows:

- ATC: This domain includes incidents where the problem was identified and successfully resolved by air traffic control.
- AIRCRAFT: This domain includes incidents where air traffic control failed to act successfully but the incident was detected and resolved by the aircrew.
- PROVIDENCE: Incidents that reach this point in the scheme were not resolved successfully by ATC or the aircrew. The only thing that prevents these incidents resulting in accidents is chance.

In order to use this model it is necessary to have some information on the performance of the baseline system. Information on incidents can be used to estimate values for the success/failure rates for each of the barriers. If such information is not available it is possible to use estimates based on operational experience.

Again, once an estimate for the baseline system has been made the impact of the OI needs to be assessed. Aspects such as changes in safety nets, performance shaping factors (such as workload) and the nature of the tasks involved in each of the barriers will need to be considered.

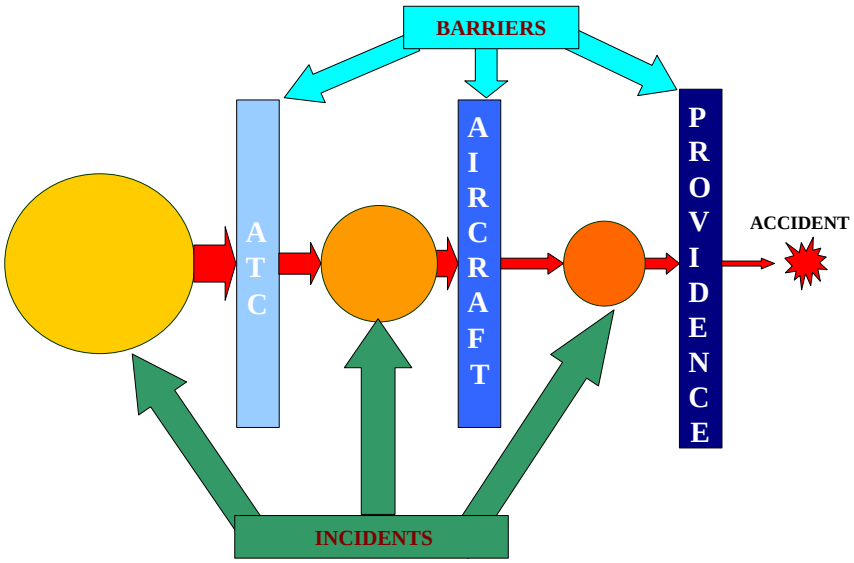


Figure I-6: Recovery

In terms of the recovery process, the potential for human error has an impact on the integrity of both the ATC and aircraft barriers. There is also a degree of overlap between the recovery and resolution processes.

In general terms, the human operator's role in the recovery process can be expressed in terms of the following stages:

- The operator must detect the situation. The situation may be detected by the controller directly, by another controller, by an automated ATC system;
- The controller must have developed an effective solution to the situation, which must be delivered to the pilots(s) involved in a timely and effective manner;
- The pilot must react appropriately in compliance with transmitted instructions in a timely manner.

Within this process there are two broad types of barrier in operation. Firstly there is the human barrier, characterised by the detection and resolution of the incident by human operators without the need for automated systems. Examples of the human barriers include detection by the controller, timely and accurate compliance by the pilot, and further down the line successful see and avoid action by the pilot.

Secondly, there are automated barriers that serve to alert the user to impending problems. In the event that the human barrier fails at any point, the automated barrier is used to initiate the detection process. At present, ATM safety nets are only used to aid detection, not to assist in resolution.

It should be noted that by the time a safety net has drawn the attention of the operator to a problem, the time pressure to derive, deliver and execute the solution will be far greater than if the operator had detected the problem without assistance. This needs to be considered when examining the recovery process.

The estimated probability that a controller will fail to detect a potential conflict prior to STCA activation is 1.19×10^{-2}. Def Stan 00-56 (Ref. 6) suggests that the probability of an error in decision making under increased stress levels (e.g. under additional time pressure following STCA activation) tends to be between 2×10^{-1} and 3×10^{-1}. In other words, as stress levels increase, the probability of failure increases by a factor of 16 to 25.

An analysis has not been performed to date to determine the probability of human failure following STCA activation and comparing this figure to the probability of failing to detect the conflict earlier. Therefore it is not possible to determine the validity of the Def Stan 00-56 estimate in the ATC environment. It is recommended that such an estimate be obtained for use in the evaluation of the ATC barrier.

When considering the effectiveness of the ATC barrier, the analyst should bear in mind the results of the Resolution module. In particular, care should be taken to ensure that any changes that affect human error probability are considered not only as part of resolution, but also as part of recovery.