

ARMS Exercises

Capt. Gustavo Barba
Member of the Board of Directors



ERC – Event Risk Classification Exercise

Air Safety Report:

TCAS "Climb" RA in uncontrolled airspace on a low-level transit. TC clearance for low level transit was "Rwy 01, VFR departure, left turn back to XX NDB, then heading 115° for 20 NM, thereafter to YYY, initial altitude 2300 ft." The crew wished to join controlled airspace but were offered this departure by ATC.

After take-off they were given Radar Service and Deconfliction Service. Speed was 180 kt, heading was 105°, about 15 to 20 NM from XX NDB. The crew was constantly receiving traffic advisories and avoidance headings from Radar Service to avoid traffic. The airspace was full with VFR aircraft and TCAS showed constantly 5 and more aircraft at a range of 5 NM. Crew was highly alerted to monitor and identify traffic and requested again to join controlled airspace.

Although avoidance headings had been given, a TCAS Climb RA was triggered with 2000ft/min or more. After clear of conflict the crew descended back to 2300ft and reported back to Radar

ERC

Event Risk Classification

First step for all incoming data

HOW TO DO IT:

Question 2 What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				Question 1 If this event had escalated into an accident outcome, what would have been the most credible outcome?		Typical accident scenarios
Effective	Limited	Minimal	Not effective			
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

ERC – Event Risk Classification Exercise

Answer Question 1:

- Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour.
- Do not filter out improbable scenarios. Question 2 will take the (low) probability into account.
- Among the scenarios with an accident outcome, pick the most credible one, and select the corresponding row in the matrix.

The resolution manoeuvre was rather aggressive, so it is reasonable to assume a significant loss of separation.

Considering also the amount of traffic in the vicinity of all potential accident scenarios, a mid-air collision scenario is the most credible one.

- This may seem like a very improbable scenario, but in line with the second bullet above, the “probability” aspect of risk will be taken into account in the Question 2 below.
- Here, the important thing is to focus on identifying the accident scenario

ERC – Event Risk Classification Exercise

Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?			
Effective	Limited	Minimal	Not effective
50	102	502	2500
10	21	101	500
2	4	20	100
1			

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?		Typical accident scenarios
Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

ERC – Event Risk Classification Exercise

Answer Question 2:

- To assess the remaining safety margin, consider both the number and robustness of the remaining barriers between this event and the accident scenario identified in Question 1.
- Barriers, which already failed are ignored
- Select the column of choice:
 - The **extreme right column**, if the only thing separating the event from an accident was **pure luck or exceptional skill, which is not trained nor required**
 - The **3rd column from the left**, if some barrier(s) were still in place but their **total effectiveness was “minimal”** – e.g. this could be a GPWS warning just before an imminent CFIT.
 - The **2nd column** if the effectiveness of the barrier(s) was “limited”. Typically, this is an abnormal situation, more demanding to manage, but with **still a considerable remaining safety margin** – e.g. a moderate error in loadsheet or loading vs. slight rotation problems at take-off.
 - The **extreme left column**, if the safety margin was “effective”, typically consisting of **several good barriers** – e.g. passenger smoking in the lavatory versus in-flight fire accident.

The barrier that stopped the escalation was the TCAS. Visual detection of the other aircraft would have been another potential barrier and a warning from ATC a third one. What is the combined effectiveness of these remaining barriers?

- TCAS is generally effective, but it requires that the system is operative on at least one aircraft. It is not uncommon that VFR traffic operates without a transponder, rendering the TCAS system useless. Similarly, ATC’s capability to detect the VFR traffic and warn about it could be severely compromised.
- Visual detection and avoidance of other (small) aircraft is unreliable. Therefore, the remaining barriers are considered of Minimal effectiveness.

ERC – Event Risk Classification Exercise

Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Effective Limited Minimal Not effective

50 102 502 2500

10 21 101 500

2 4 20 100

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

Catastrophic Accident Loss of aircraft or multiple fatalities (3 or more)

Major Accident 1 or 2 fatalities, multiple serious injuries, major damage to the aircraft

Minor Injuries or damage Minor injuries, minor damage to aircraft

No accident outcome No potential damage or injury could occur

Typical accident scenarios

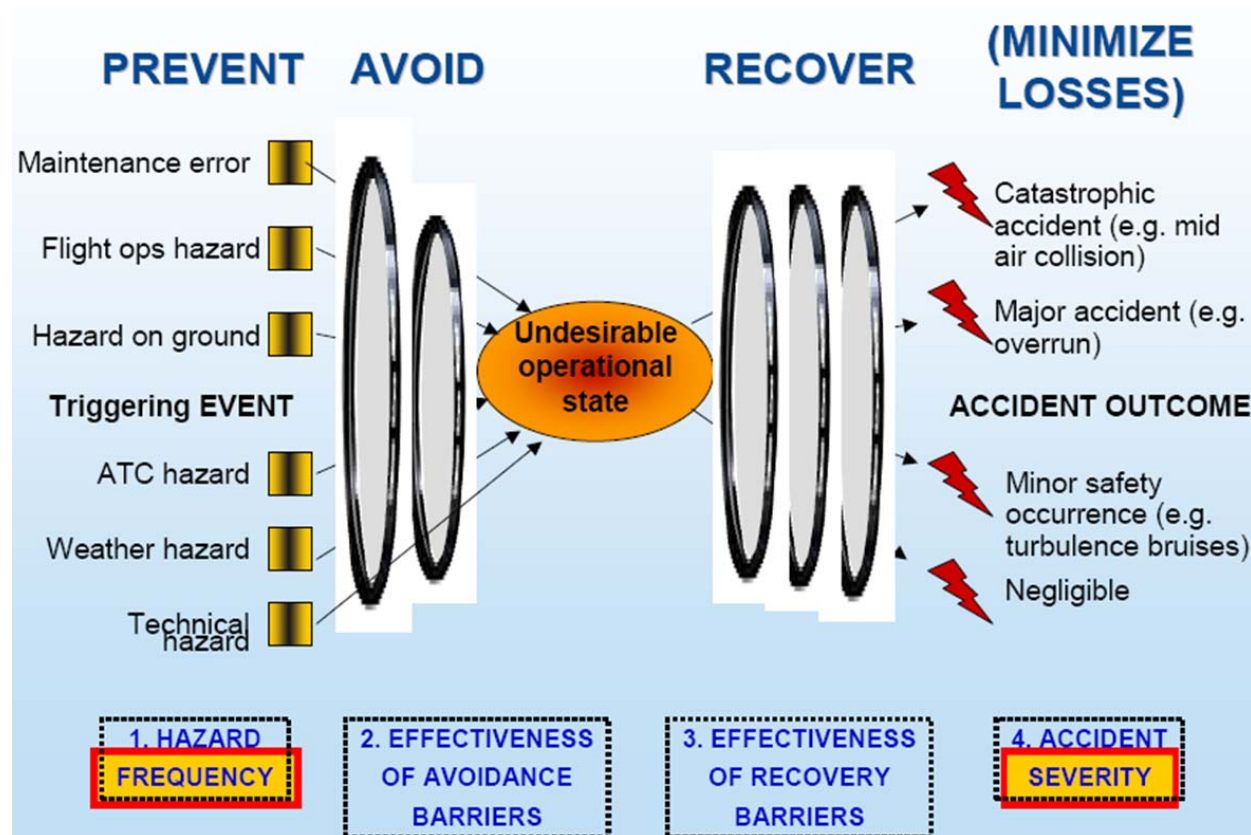
Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain

High speed taxiway collision, major turbulence injuries

Pushback accident, minor weather damage

Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

SIRA – Safety Issue Risk Assessment Exercise



SIRA – Safety Issue Risk Assessment Exercise

An incident happening to another company motivates the MRO “MyMx” to study the Safety Issue of cross-connecting the flight controls (left-right or push-pull). MyMx has no idea how improbable it is that such a maintenance error could take place.

- **Step 1: Define the Safety Issue precisely**
- The Safety Issue is an accident (at takeoff) due to cross-connected flight controls of the Pilot Flying (PF). MyMx currently is maintaining only Airbus fly-by-wire aircraft, so these will be the a/c types under study.

SAFETY ISSUE RISK ASSESSMENT (SIRA) TOOL	
1 Safety Issue title:	Accident (at takeoff) due to cross-connected flight controls of the Pilot Flying (PF).
2 Define/scope the SI:	
Description of Hazard(s)	Maintenance error where flight control wires are cross-connected on one or both sides.
Description of Scenario	The accident scenario is total loss of the aircraft due to handling problems after lift-off (Loss Of Control, LOC).
A/C types	Airbus fly-by-wire
Locations	At MRO homebase airport
Time period under study	Next 12 months.
Other	

SIRA – Safety Issue Risk Assessment Exercise

- Step 2: Develop the related accident scenarios.
 - The accident scenario is total loss of the aircraft due to handling problems after lift-off (Loss Of Control, LOC).
- Step 3: Analyse the Scenario using the SIRA model:
 - **The triggering Event** is the maintenance error of cross-connecting the wires on one or both sides (capt/first officer).
 - This must involve cross connecting both the command and monitoring channels, otherwise the aircraft itself would detect the problem.
 - **The Undesirable Operational State** can be defined as “taking off with an aircraft with the above maintenance error”. (note that the UOS always takes place within the Flight Operation)
 - **The accident** is LOC at takeoff.
 - With the above definitions, **the Avoidance barriers are**: any actions postmaintenance that would enable either the MyMx or the operating flight crew to detect the problem before (or latest during) the takeoff roll.
 - **The recovery barriers** are flight crew actions enabling a safe flight despite the aircraft taking off with cross connected controls.

SIRA – Safety Issue Risk Assessment Exercise

3 Analysis of potential Accident Scenario				
3.1 Triggering event		3.2 Undesirable Operational State		3.3 Accident Outcome
Maintenance error where both command and monitoring channels are cross-connected.		Taking off with the above maintenance error		Loss of control at takeoff after liftoff.

4 Describe the barriers				
	4.1 To avoid the UOS		4.2 To recover before the Accident	
	The maintenance team is supposed to make an operational check after the maintenance task. This barrier could fail either because the check is omitted or not done carefully enough ("it moves" is not enough, the direction needs to be correct). Estimated conservative failure rate is: 1/100 times. During taxi-out, the pilots make a flight controls check. This may fail for the same reasons as for the maintenance team. The estimated failure rate is the same 1/100.		The Recovery Barrier consists of two things: either only one side is affected and by luck the Pilot Not Flying (PNF) side; or the PF manages to control the aircraft despite the cross-connection. This is deemed very difficult and subject to wind effects just after lift-off.	

SIRA – Safety Issue Risk Assessment Exercise

Step 4: Determine/estimate the values for the four factors of SIRA.

- **Triggering event:** There is no information on how frequent or rare such a maintenance error could be. It has never taken place in MyMx in its 8 years of existence. Therefore, this SIRA risk assessment is carried out “backwards”, leaving this value initially open.
- **Avoidance barriers:** the maintenance team is supposed to make an operational check after the maintenance task. This barrier could fail either because the check is omitted or not done carefully enough (“it moves” is not enough, the direction needs to be correct).
 - Estimated conservative failure rate is: 1/100 times. During taxi-out, the pilots make a flight controls check. This may fail for the same reasons as for the maintenance team. The estimated failure rate is the same 1/100. For both to fail, we get an Avoidance Barriers failure rate of: 1/10,000 times.
- **The Recovery Barrier** consists of two things: either only one side is affected and by luck the Pilot Not Flying (PNF) side; or the PF manages to control the aircraft despite the cross-connection. This is deemed very difficult and subject to wind effects just after lift-off. Therefore, it is considered that a conservative “fails practically always” barrier effectiveness level must be used.
- A Loss of Control at takeoff is considered a Catastrophic accident.

SIRA – Safety Issue Risk Assessment Exercise

- As the Triggering Event frequency is unknown, we work backwards by targeting a resulting risk class, which is “secure” or better. By fixing the barrier values and the accident type and varying the Triggering Event frequency, it can be seen that the maximum allowable frequency is: “every 100,000 sectors”.

5	Risk Assessment				
	The estimated frequency of the triggering event (per flight sectors) is:	The barriers will fail in AVOIDING the UOS...		The barriers will fail in RECOVERING the situation before the ACCIDENT...	The accident severity would be...
	About every 100000 sectors	Once in 10 000 times		Practically always	Catastrophic
	1.E-05	1.E-04		1.E+00	
			UOS frequency:		Mean Accident frequency:
			1.E-09		1.E-09
6	Result				
	6.1 Resulting risk class	Secure			
	Comments on actions:				

Safety Assessment – Management of Change Exercise

Procedures for the connection of ground power after arrival on stand.

The current practice is to start the APU after landing and subsequently shutdown both engines before the Ground Power Unit (GPU) is connected. This is perceived as a normal, conventional, safe operation. The proposed change is to keep number 2 engine running until the GPU is connected. This would reduce APU cycles and save fuel.

1. **The Safety Issue** is the risk of ingesting personnel who approach the aircraft into the operating engine.
2. **Triggering event**: arrival of aircraft with this procedure in effect. (→ every flight)
3. **UOS**: an operating engine with ground personnel within the danger zone of ingestion.
4. **Accident outcome**: Person ingested into engine (fatal). → Major
5. **Avoidance barriers**: Procedures to keep all personnel away from aircraft until the GPU has been plugged and the engines have been shutdown. The revised procedure would have both personnel and equipment approaching the aircraft to plug in the GPU. (→ estimated to fail 1/1000 times)
6. **Recovery barriers**. Barriers that would keep people who went to the aircraft despite the running engine, away from the engine danger zone. Depends on location of engines, ingestion size of danger zone, etc. If somebody accidentally goes to the aircraft, he might realise that the engine is running, or simply not need to go close to the engine, but there is no actual protection in place (→ estimated to fail 1/1000 times).

SIRA result (using the excel tool): “IMPROVE” (risk too high). → This means the proposed change is beyond the acceptable level of risk and cannot be implemented unless new avoidance or recovery barriers can be created.

TCAS incident ERC

Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?			
Effective	Limited	Minimal	Not effective
50	102	502	2500
10	21	101	500
2	4	20	100

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?		Typical accident scenarios
Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

The whole Risk Assessment process

Consider the ERC example one (TCAS). The red result means several things:

- Typically, immediate risk reduction must be possible or flying to such areas must be suspended.
- Even one single event with a red ERC rating becomes a “Safety Issue” of its own. It has to be judged whether the SI will cover only the particular zone where the event took place or also other/all similar areas.

As single event, the event contributes to ERC statistics. As a Safety Issue, it will now be assessed using the SIRA. The SIRA assessment must then be repeated from time to time to make sure the risk level becomes/remains acceptable.