AtkinsRéalis

Risk Assessment & Equipment Contribution to Risk to Life (ECtRtL)

Plan Design Enable

1

AtkinsRéalis

Learning Objectives

- Objective:
  - To introduce Risk Assessment
- Topics to be covered:
  - Introduce risk assessment within the MOD
  - Why conduct Risk Assessment
  - MAA Risk to Life Classification
  - Equipment Contribution to RtL – ASPIRE.

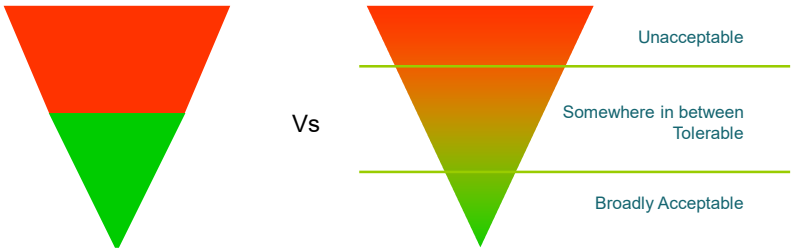
2

The Need for Risk (Safety) Criteria

- 'Traditional' prescribed safety legislation – typically does not evaluate the actual level of risk
  - Sets limits across the board without consideration to individual factors such as operational and environmental context:
    - Flight overland Vs Flight over water
    - Long Haul Vs Short Haul
- Risk based approach is more 'interactive' and specifically considers the operational and environmental context.

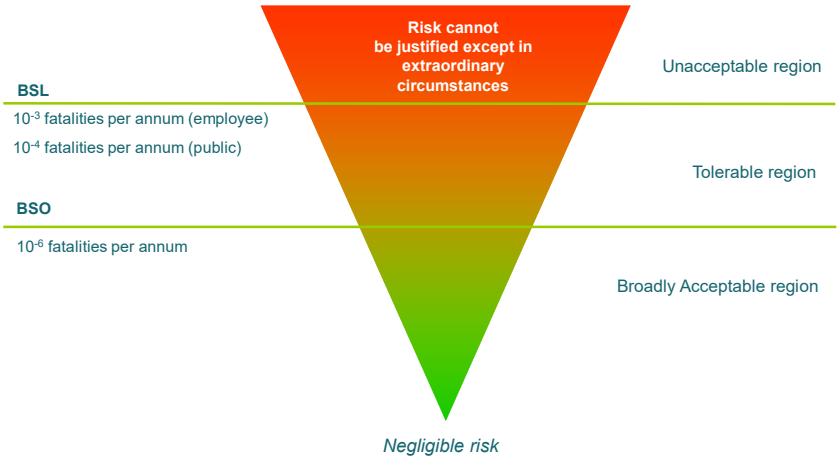
Why a Banded Approach ?

Why do we not just have a pass/fail criteria i.e. red/green?



- Risk assessment is not a precise discipline – it is not absolute
- Risk assessment is qualitative and subjective
- Probabilities are inherently uncertain.

HSE Risk Criteria Framework



Parameters of Risk

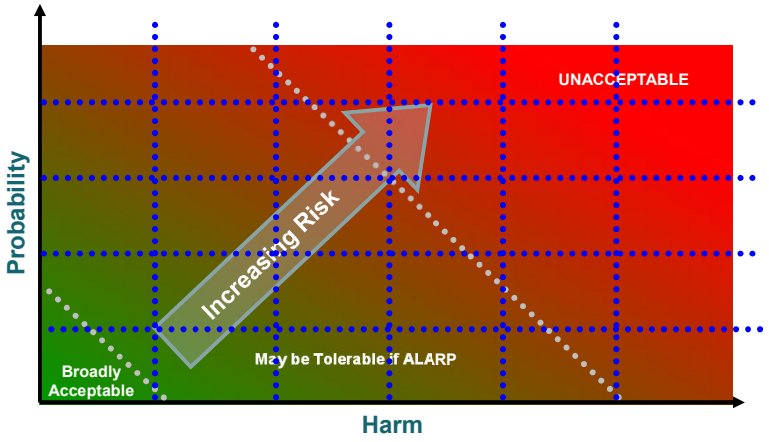
- Exposure to harm, danger or possible loss
- Basic parameters of risk
  - A defined undesirable consequence = severity of harm

  AND
  - Unit of exposure to the undesirable consequence = likelihood (probability/frequency) of that harm

Risk = Severity x Likelihood

- By classifying the severity and likelihood we can differentiate between outcomes, and the likelihood of those outcomes.

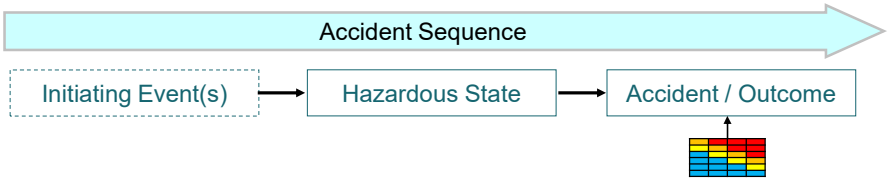
Risk Continuum



Typical Risk Classification Matrix

Likelihood	Severity			
	Minor	Major	Critical	Catastrophic
Frequent (>10^{-3})	H(10)	VH(6)	VH(3)	VH(1)
Probable (10^{-3} to >10^{-4})	M(16)	H(9)	VH(5)	VH(2)
Occasional (10^{-4} to >10^{-5})	L(17)	M(12)	H(7)	VH(4)
Remote (10^{-5} to >10^{-6})	L(19)	L(14)	M(11)	H(8)
Improbable (10^{-6} to >10^{-7})	L(20)	L(18)	L(15)	M(13)
Incredible (<10^{-7})	L(24)	L(23)	L(22)	L(21)

Accident Sequence



1. What is the accident sequence? – The steps from the initiating event to the point at which someone is harmed
2. Who is the individual or group most at risk from the accident sequence?
3. How badly could the individual or group most at risk be harmed?
4. How often could the initiating event occur?
5. What are the situational probabilities for each step of the accident sequence, from the initiating event through to the harm (Step 3) being incurred?
6. What is the likelihood of harm to the individual?
7. Assess the risk classification from the matrix.

Hazard Log

- The risk assessment is typically recorded in a Hazard Log in a way that captures and retells the accident sequence:

Ref	Hazard	Causes	Mitigation	Outcome	Severity	Likelihood	Risk

Describes the accident sequence

Provides the evidence to justify the risk likelihood

Categorises the risk

AtkinsRéalis

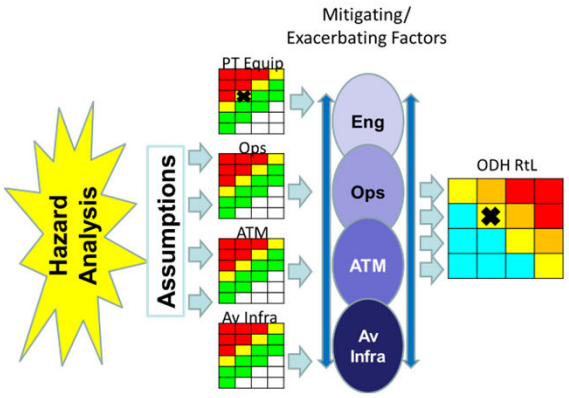
Deciding Outcomes

- Worst Outcome
  - The most severe outcome possible
- Most Likely
  - The most frequent occurring outcome but is not necessarily the most severe consequence
- **Worst Credible**
  - The most severe outcome that can be realistically expected
  - Requires a level of subjectivity and judgement.

AtkinsRéalis

Who Conducts the Risk Assessment?

- ADH owns the RtL
  - Therefore, it is incumbent on the ADH to assess and classify the Risk



MAA Hazard Risk Matrix *(RA1210)*

Likelihood		Severity			
		Minor	Major	Critical	Catastrophic
	Frequent	M	H	VH	VH
	Occasional	L	M	H	VH
	Remote	L	L	M	H
	Improbable	L	L	L	M

The Defence Aviation HRM (RA1210)

MAA Severity Categories *(RA1210)*

Severity	Worst Credible Risk Resulting from Hazard
Catastrophic	Three or more fatalities of MOD employees engaged in the activity in question or a single fatality of a member of the public
Critical	One or two fatalities of MOD employees engaged in the activity in question. A large number of major injuries must also be included in this category
Major	Major injuries to any person. A large number of reportable injuries must also be included in this category
Minor	Reportable injuries of any person

MAA Likelihood Categories *(RA1210)*

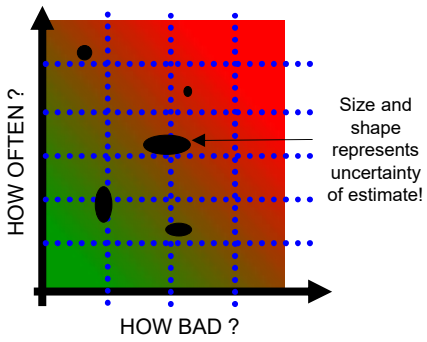
Likelihood Category	Generic Guidance Words to Assess Likelihood of Occurrence of Accident
Frequent	Likely to occur at least several times a year
Occasional	Likely to occur one or more times per year
Remote	Likely to occur one or more times in 10 years
Improbable	Unlikely to occur in 10 years

Why do Risk Assessment?

- By measuring Risk by its severity and likelihood, Risk can be classified
  - Unacceptable, tolerable, acceptable
  - Suggest if a change is to be made
  - Suggest if further study is required
  - Allows risks to be compared with each other
- This “Risk Classification” can then be ranked in order to **prioritise** where most effort (e.g. resources, funding) should be used to reduce the identified risks.

Qualitative Risk Assessment

- **Words of warning!**
- Risk Ranking is a qualitative method
  - Do not be fooled into thinking its quantitative because of the use of numbers.
  - Numbers allow the ranking of risk against each other, but do not in themselves represent an absolute level of risk
- Projects should use consistent and the same likelihood and severity categories for risks to be comparable.



How do Aviation DTs fit in?

- ADH owns the Rtl and assesses the Risk
- TAA supports this by defining and quantifying the **Equipment Contribution** to the RtL
- ASPIRE Process 17 developed to assist this approach.

AtkinsRéalis

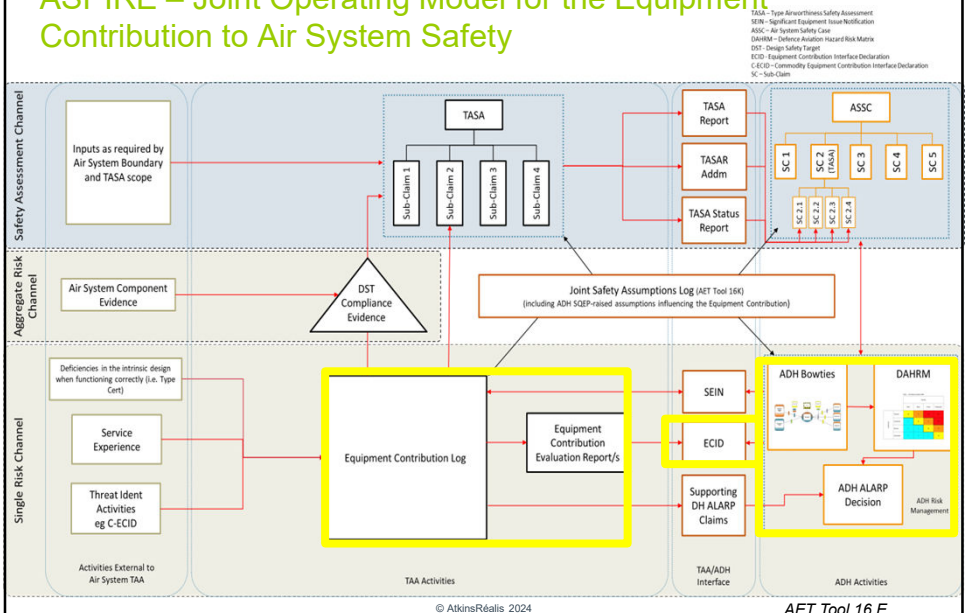
Equipment Contribution to Risk to Life (ECtRtL)

Plan Design Enable

19

AtkinsRéalis

ASPIRE – Joint Operating Model for the Equipment Contribution to Air System Safety



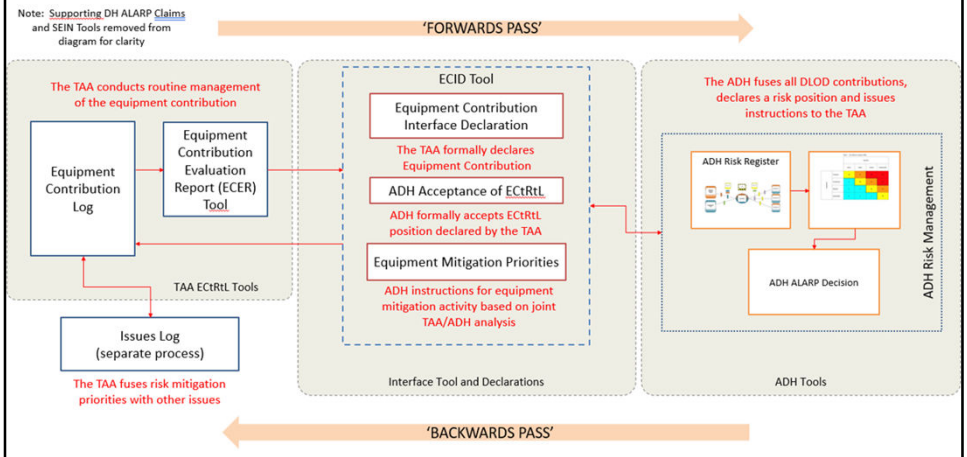
AET Tool 16.E

20

ASMT | Risk Assessment & ECtRtL

AtkinsRéalis

Reporting of ECtRtL



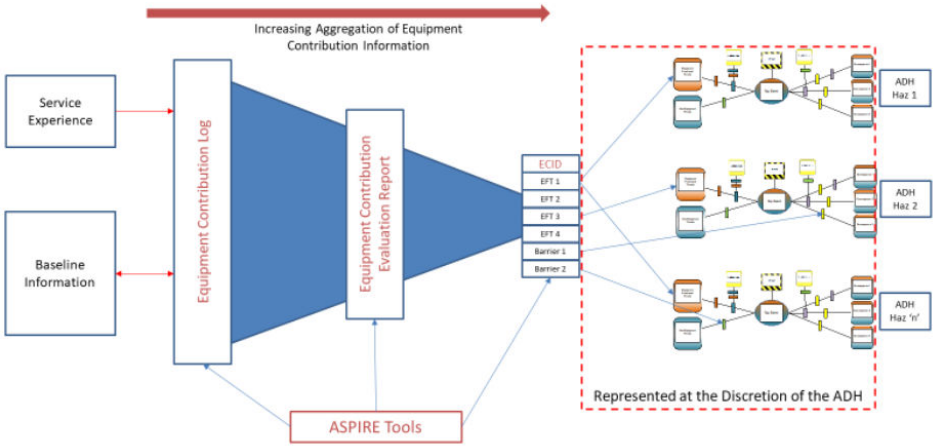
AET Tool 17.B

21

ASMT | Risk Assessment & ECtRtL

AtkinsRéalis

ECtRtL Artefacts



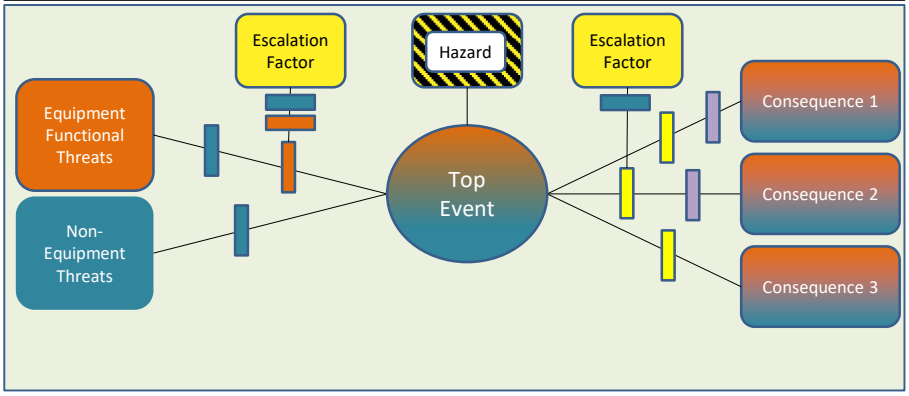
AET Tool 17.B

22

AtkinsRéalis

ASPIRE - Defining ECtRtL

This model focusses on an accident sequence with the centre of the Bow Tie representing an ADH managed hazard.



EQUIPMENT CONTRIBUTION TO ADH RtL MODEL

Equipment Functional Threats (LHS of bow tie only)	Non-Equipment Functional Threats (ADH bow tie only)	Proactive Equipment Barrier	Proactive Non-Equipment Barrier (TAA Advice)	Equipment Recovery Barrier	Non-Equipment Recovery Barrier (TAA Advice)

AtkinsRéalis

ASPIRE – ECtRtL Terminology

Term	ECL Foundation Description
Barrier	Any measure taken that acts against a threat or a TE becoming a consequence in order to reduce risk to life
Baseline information	Fundamental safety evidence that forms part of the approved Type Airworthiness Safety Assessment
Consequence	The undesirable events (usually accidents and safety related incidents) that may potentially result from the TE
Equipment Functional Threat (EFT)	A loss/failure of equipment function that is imperative for safe flight and which could directly lead to a TE
Equipment Threat (ET)	A degradation or loss of system/sub-system which could directly lead to an EFT
Escalation Factor (EF)	Conditions that can make a barrier fail or reduce the effectiveness of a barrier
Hazard	An intermediate state where potential for harm exists (MAA02)
Service experience	Information or data generated as a result of air system use that has a potential relationship to baseline information
Threat	Factors that could cause the TE
Top Event (TE)	The mechanism that describes the release or loss of control over a hazard

AET Tool 17.C

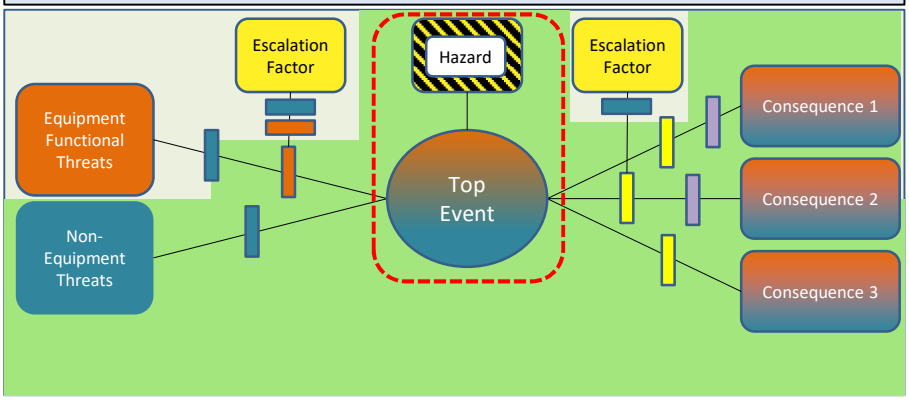
ASPIRE - Hazard Taxonomy

HAZARD	Top Event
Aircraft Operations (Airborne)	Loss of control in flight
	Loss of safe separation (terrain/obstacle)
	Loss of safe separation (airborne objects)
Aircraft Operations (Protected Manoeuvring Area)	Loss of control on ground
	Loss of safe separation (vehicle/personnel)
Aircraft Operations (General)	Uncontrolled ignition
	Loss of security of items fitted or loaded to aircraft
Ground Operations	Loss of safe separation (GE/Infra)
Individuals Carried Within or In Close Proximity to Aircraft	Individual exposed to personal hazard (not leading to loss of control)

AET Tool 17.C

ASPIRE - Defining ECtRtL

This model focusses on an accident sequence with the centre of the Bow Tie representing an ADH managed hazard.



EQUIPMENT CONTRIBUTION TO ADH RtL MODEL

Equipment Functional Threats (LHS of bow tie only)	Non-Equipment Functional Threats (ADH bow tie only)	Proactive Equipment Barrier	Proactive Non-Equipment Barrier (TAA Advice)	Equipment Recovery Barrier	Non-Equipment Recovery Barrier (TAA Advice)

ASPIRE - Equipment Functional Threat (EFT) Taxonomy

- Loss of / Failure of
- Malfunction of / Erroneous

1. Flight Control
- 1.1. Flying Control
- 1.2. Flight indications
- 1.3. CofG Control

2. Ground Steering
- 2.1. Landing Gear Extension
- 2.2. Ground Steering

3. Engine Control
- 3.1. Engine Thrust/Power Control
- 3.2. Sustained Engine Operation

4. Power (Torque) Distribution
- 4.1. Power (Torque) Distribution

5. Ground Deceleration
- 5.1. Ground Deceleration

6. Situational Awareness
- 6.1. Altitude Indication
- 6.2. Heading Indication
- 6.3. Aircrew Visibility
- 6.4. Location Information

7. Life Support
- 7.1. Protection from High G Acceleration
- 7.2. Cabin Conditioning
- 7.3. Cockpit Environment free from Health & Safety Risks
- 7.3. Cockpit Environment free from Substances Hazardous to Health

8. Retention and Release of Stores
- 8.1. Safe Loading of Stores
- 8.2. Safe Retention of Stores
- 8.3. Safe Release of Stores

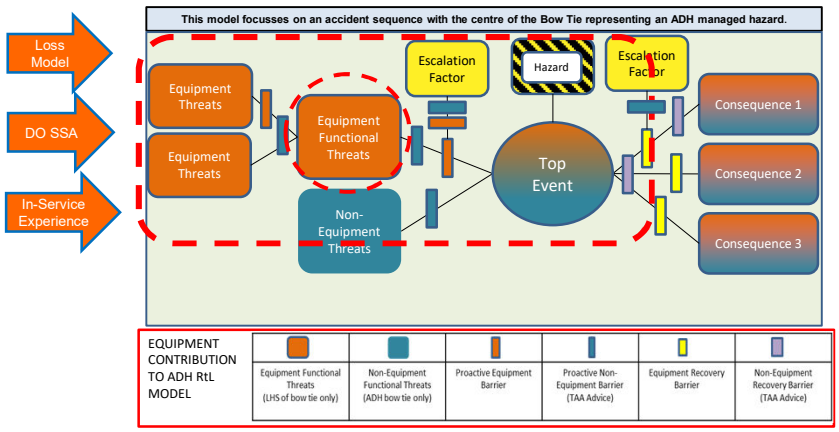
9. Damage Tolerance
- 9.1. Withstand Flight and Ground Loads
- 9.2. Retain Rotating Parts
- 9.3. Prevent Sources of Ignition

10. Cargo and Handling
- 8.1. Safe Loading of Cargo
- 8.2. Safe Retention of Cargo
- 8.3. Safe Release of Cargo

11. Launch / Recovery Systems
- 11.1. Air System Launch System
- 11.2. Air System Recovery System

AET Tool 17.C

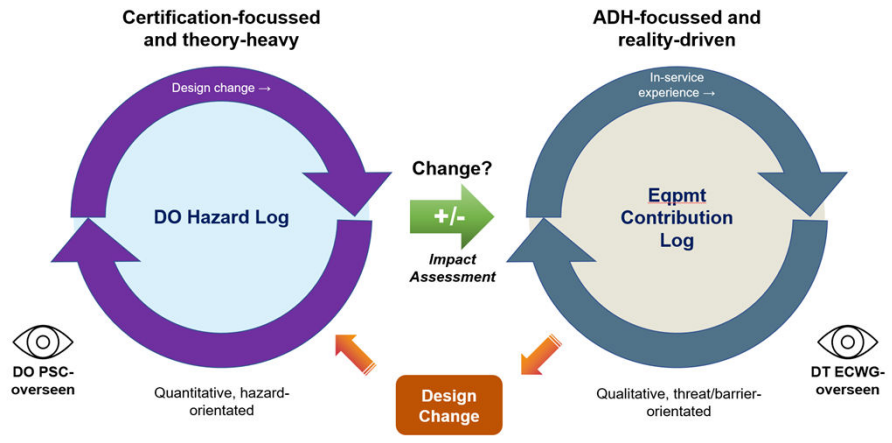
ASPIRE – DT Focus



Acceptance of prior Safety Scrutiny

- It is a fundamental principle of Process 17 to focus on “residual risk” from the accepted baseline position defined when establishing the Initial Type Airworthiness
  - Do not try and manage all associated hazards as defined by a Loss Model
  - Since the introduction of the Military Certification Regime, an Air System design now undergoes rigorous scrutiny before being certified by the MAA
  - This sets an “**acceptable baseline**” level safety with many hazards designed out based on the certification requirements

Acceptance of DO/TCH Responsibilities



AET Tool 17.B

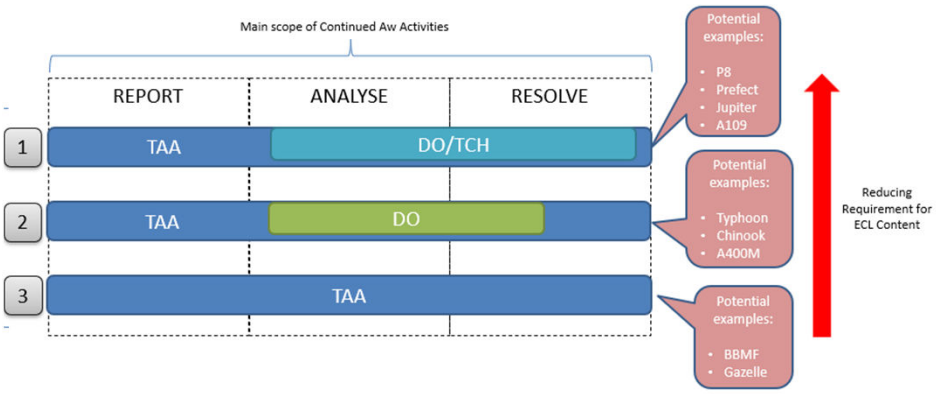
AtkinsRéalis

Reportable ECtRtL

- As such, focus should be on "**deviations**" from this certified position
  - MCRIs – capturing non-compliances with the Type Certification Basis
  - DO SSAs – residual risks identified by the DO where safety objectives have not been met
  - Service Experience – occurrences which undermine "Baseline" assumptions
  - Loss Model – drivers of risk identified within the Loss Model

AtkinsRéalis

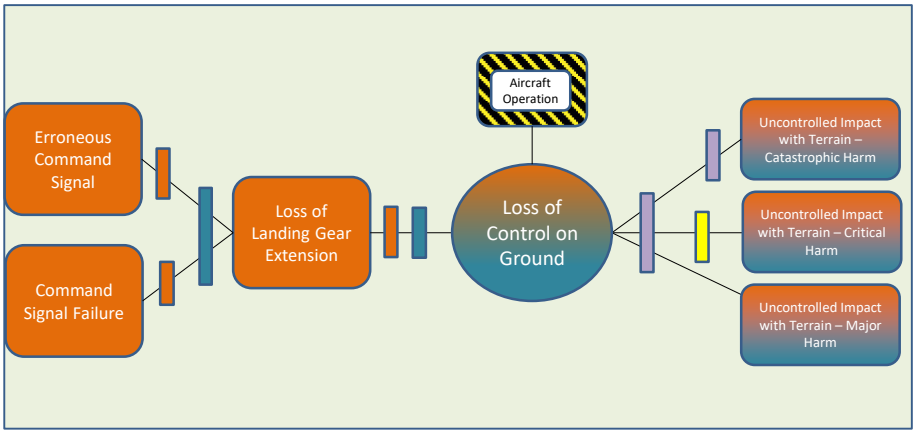
Scope of Equipment Contribution Log



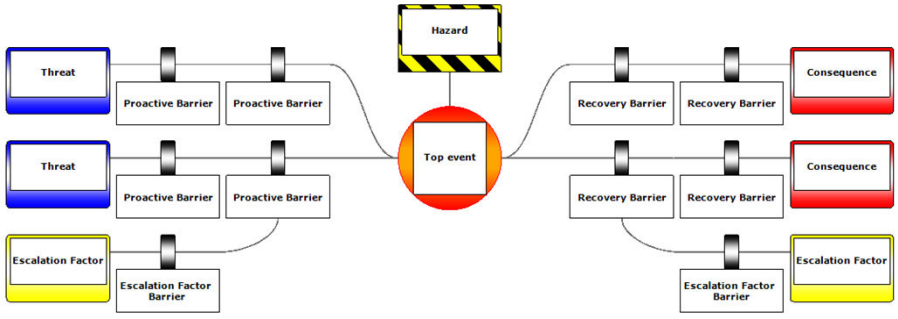
AET Tool 17.B

ASPIRE – Expand to Equipment Threats

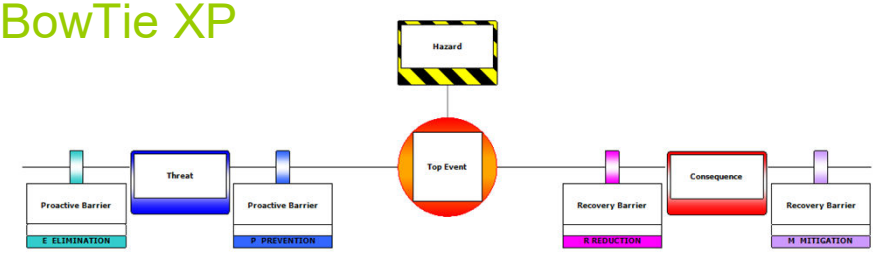
- Failure of undercarriage to lower



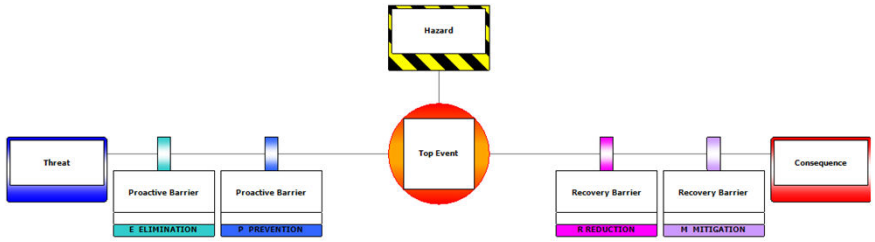
ASPIRE – Barriers Theory



BowTie XP



Displayed



ASPIRE – Barriers

- Two types of barriers in Process 17
  - Barriers providing assurance against Equipment Threats
  - Equipment Barriers that prevent/mitigate progression along the threat line

AtkinsRéalis

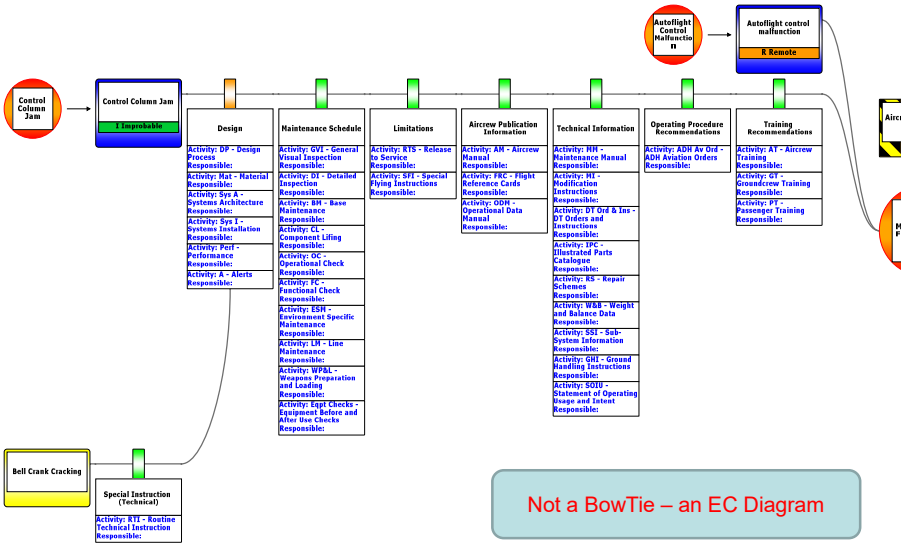
ASPIRE – Assurance Barrier Taxonomy

- Provides analysis of assurance of key factors that support the type airworthiness.
  - **Design**
    - Process, Materials, Architecture, Installation, Performance, Alerts
  - **Maintenance Schedule**
    - Inspections, Checks, Lifing, Line Maintenance
  - **Limitations**
    - RTS
  - **Aircrew Publication Information**
    - Aircrew Manual, FRCs, ODM
  - **Technical Information**
    - Maintenance Manual, Mod Instructions, Orders, IPC, SOIU
  - Operating Procedure Recommendations
  - Training Recommendations

AET Tool 17.C

AtkinsRéalis

ASPIRE – Applying Assurance Barriers



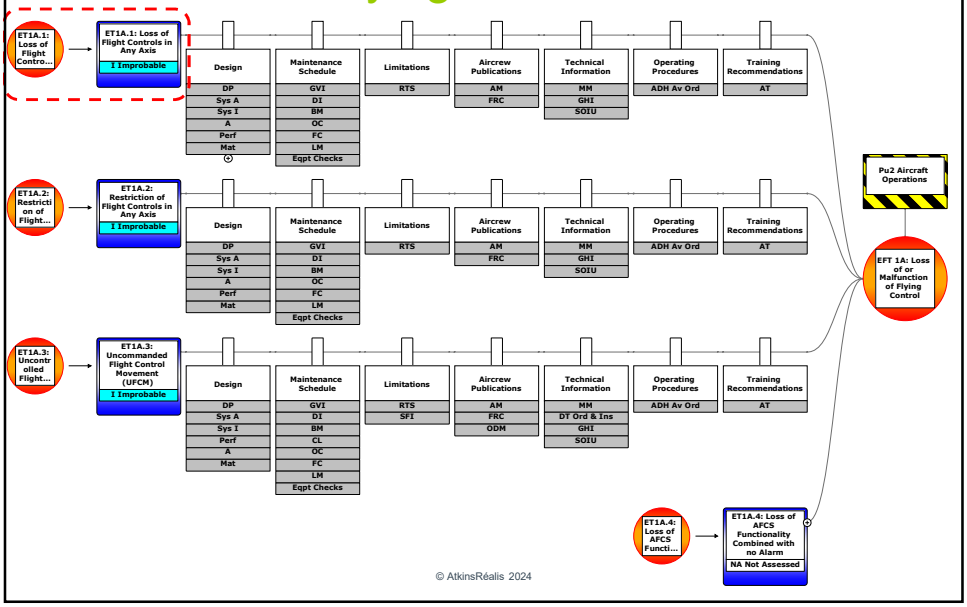
Not a BowTie – an EC Diagram

AET Tool 17.C

ASMT | Risk Assessment & ECtRtL

AtkinsRéalis

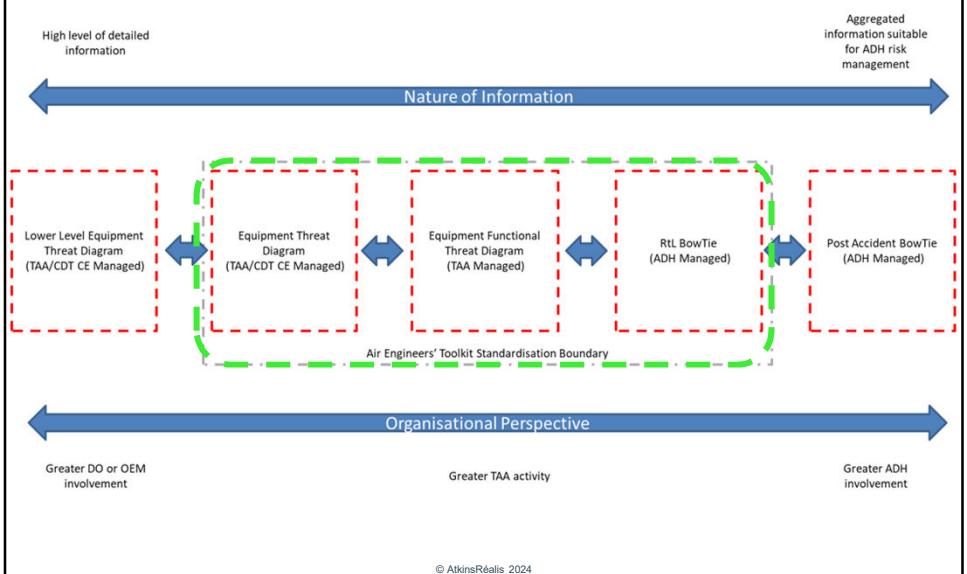
EFT: Loss of Flying Controls



ASMT | Risk Assessment & ECtRtL

AtkinsRéalis

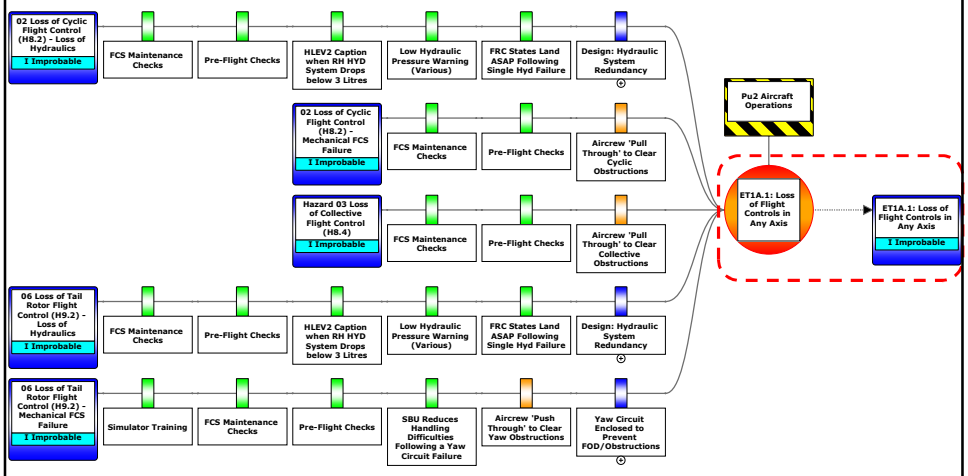
Chaining BowTies



ASMT | Risk Assessment & ECtRtL

AtkinsRéalis

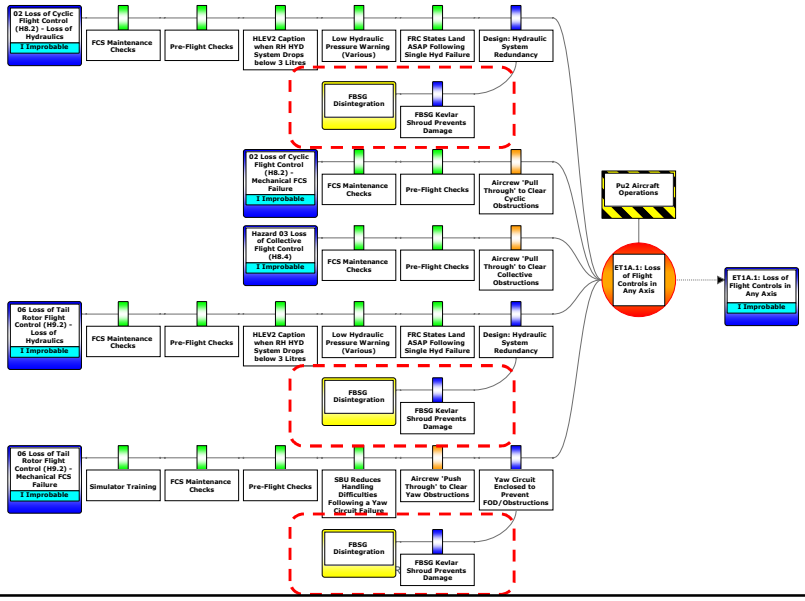
ET: Loss of Flight Controls (Any Axis)



ASMT | Risk Assessment & ECtRtL

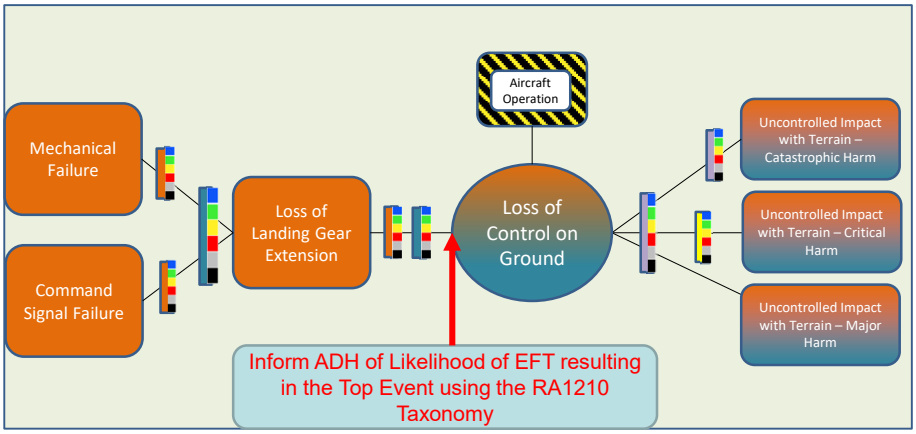
AtkinsRéalis

ET: Loss of Flight Controls (Any Axis)



ASPIRE – Determine the EFT Probability

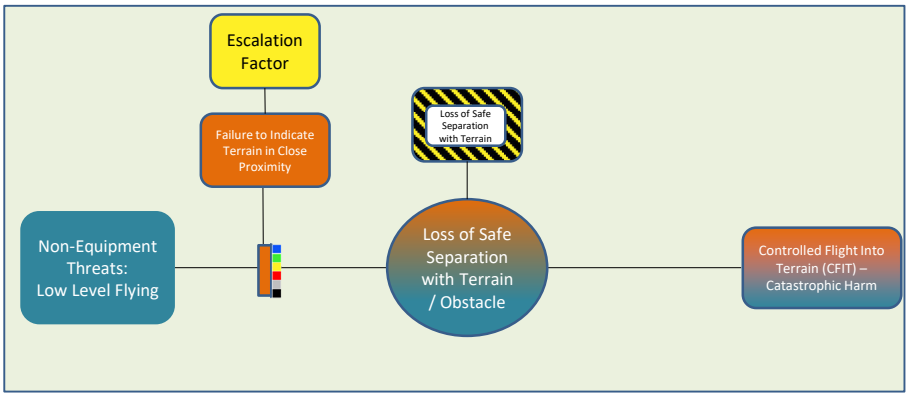
- Failure of undercarriage to lower



ASPIRE – Equipment Barriers

- Any measure taken that acts against a Threat or Top Event becoming a consequence
- Typically applied to the ADH BowTie but recorded in the TAA EC Log as they are provided as part of the equipment.
- Examples include:
  - RadAlt
  - Ice Protection
  - Collision Warning System
  - Ejection Systems
  - Wirecutters (Helicopters)

ASPIRE – Non Equipment Functional Threats



ASPIRE - Barrier Effectiveness

- Criticality
  - How much reliance is placed on a particular Barrier
- Type
  - Passive, Continuous, Hardware, Behavioural, Socio-Technical
- Adequacy
  - To what extent does the Barrier interrupt a particular scenario
- Reliability
  - How much certainty is there that the Barrier will function as expected when needed.

AtkinsRéalis

ASPIRE - Barrier Effectiveness Taxonomy

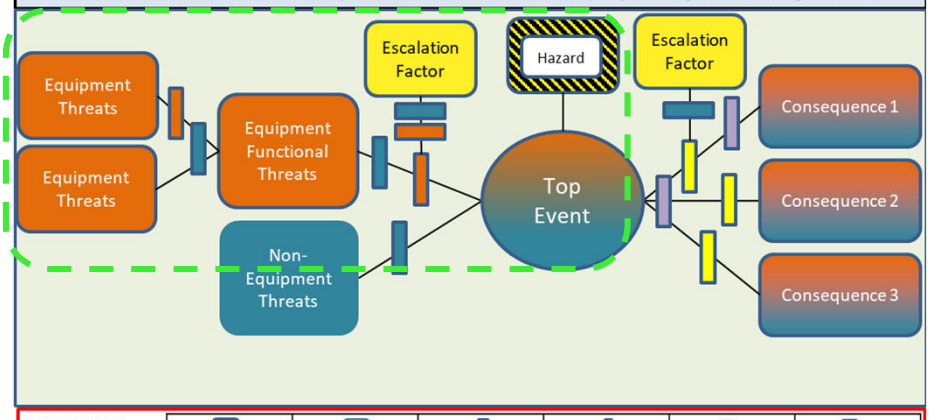
Barrier	Description
	• Barrier is suitable to eliminate/prevent the threat or lessen likelihood/reduce severity of the consequence. • Barrier has been tested and proven to work as expected. • Barrier owner informed of responsibilities and has provided feedback/ assurance on the status of the barrier. • Barrier is supported by documented evidence. • There are sufficient resources available to maintain the effectiveness of the barrier.
	• Barrier is suitable to eliminate/prevent the threat or lessen likelihood/reduce severity of the consequence. SME judgement suggests the barrier will work as expected, when needed but there might not be documentary evidence to support the assumption. • Description of effectiveness rating in place through SQEP assessment. • Barrier has an owner assigned through SQEP assessment. • Procedural barriers should always be Adequate at best.
	• The barrier is in place and offers some level of control over the threat, but the adequacy and/or ability of the barrier is considered to be sub-optimal. • Is the default assessment for purely HF related barriers (eg "Behavioural" barrier Type) unless there is clear evidence to the contrary.
	• A mitigation that is in place but does not operate reliably or as expected. • Applies especially to technical solutions that do not deliver the intended level of control.
	• The barrier has been included in the BowTie but has not been assessed by a SQEP panel for effectiveness.
	• Applies to any mitigation that is known to exist and is considered appropriate in the subject BowTie. Includes: Not present unfunded (purely aspirational) and Not Present funded (planed for future incorporation).

ASPIRE Tool 17.C

AtkinsRéalis

Workshop Time

This model focusses on an accident sequence with the centre of the Bow Tie representing an ADH managed hazard.



EQUIPMENT CONTRIBUTION TO ADH RtL MODEL	Equipment Functional Threats (LHS of bow tie only)	Non-Equipment Functional Threats (ADH bow tie only)	Proactive Equipment Barrier	Proactive Non-Equipment Barrier (TAA Advice)	Equipment Recovery Barrier	Non-Equipment Recovery Barrier (TAA Advice)

AtkinsRéalis

Workshop Wrap Up

- Do not be constrained by Taxonomy
  - Square Pegs, Round Holes
  - Taxonomy provides the framework
  - Key point is to interface with the DH's risk picture so start from the DH's BowTies if you can.
- Powerful Display Tool
  - Show what's important
  - Too much can hide the key message
  - Too much can give false sense of security
  - Barrier Effectiveness is a very important part
  - Escalation Factors are the key focus points for through life management

AtkinsRéalis

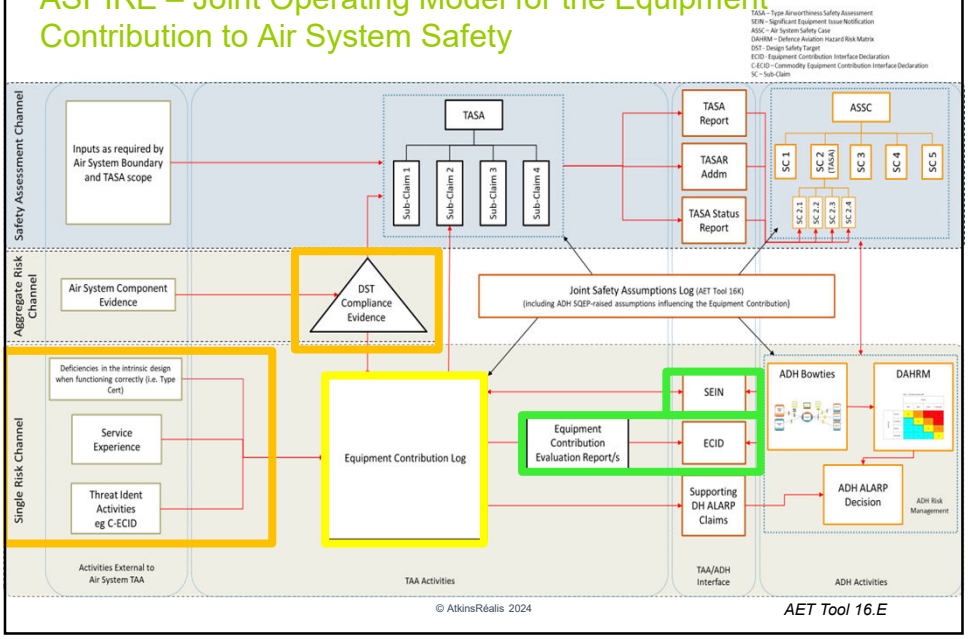
ECtRtL Top Tips

- Do
  - Draw a line under historical pre-ECtRtL approaches and archive
  - Link EFTs / Escalation Factors / Airworthiness Issues Management
  - ECL doesn't follow purist BowTies – diagrammatic representation
  - Be proportionate
  - Take up Facilitated Implementation (FI) sessions provided by the DAT
- Don't
  - Force ECLs into a scientific quantitative approach – ADH wants qualitative
  - Feel a need to sweep **all** the baseline analysis into the ECL
  - Rebuild historical issues within the ECL
  - Build a highly complex empty framework into the ECL for "when it is needed" – it is easy enough to build at the time

How do Aviation DTs fit in?

- TAA does not assess the risk, this is the ADH responsibility.
- TAA supports the ADH Risk Assessment by defining and quantifying the **Equipment Contribution** to the RtL
  - Identify Functional Threats from the Equipment (HAZID – FHA)
  - Identify Equipment Threats that impact the Functional Threats
  - Illustrate how the equipment impacts ADH risks (BowTie)
  - Identify Barriers associated with the Equipment
  - Identify escalation factors that could affect the barriers (HAZID – ZHA)
  - Assess effectiveness of the Barriers
  - Communicate Equipment Contribution analysis to the ADH

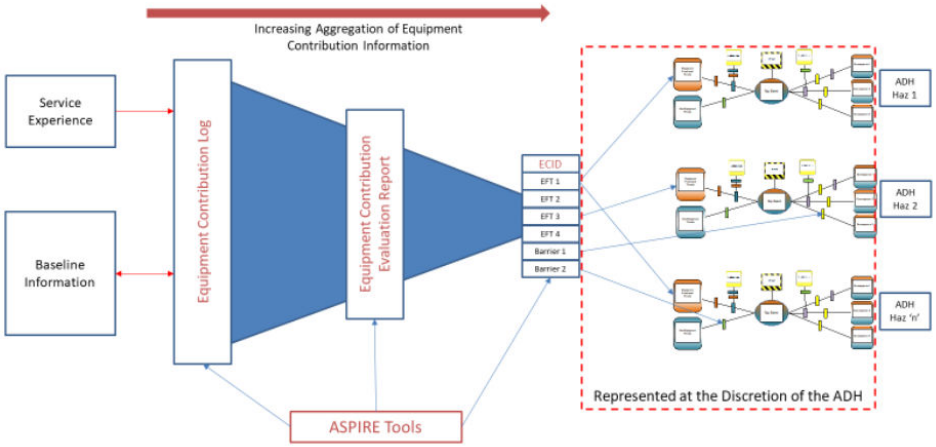
ASPIRE – Joint Operating Model for the Equipment Contribution to Air System Safety



AET Tool 16.E

AtkinsRéalis

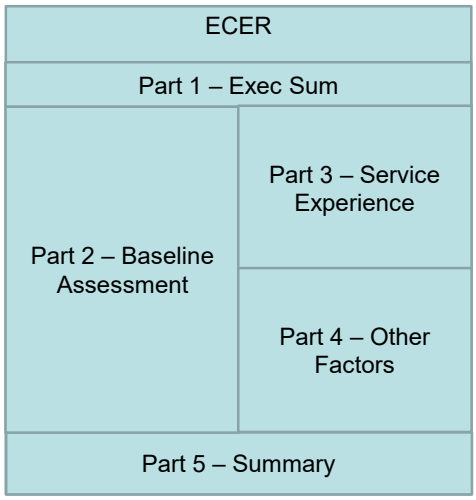
ECtRtL Artefacts



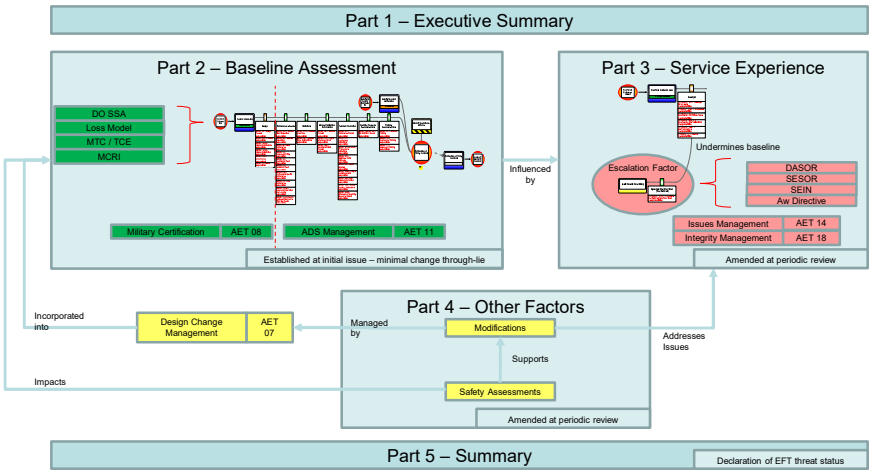
AET Tool 17.B

AtkinsRéalis

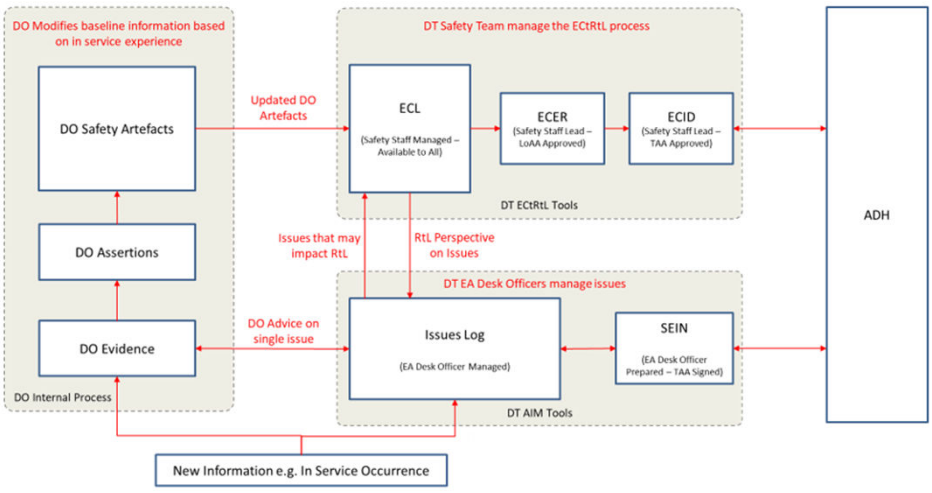
ECER Structure



ECER Structure



Issues Management



ECID - Joint Declaration

Part 2 – TAA declaration[xvii]

1. Taking into account the information presented in this ECID, and the evidence that supports it, the following declaration is made in respect of the [air system]:

It is considered that, based upon the evidence available and the assurance activity completed, and the implementation and sustainment of the recommended non-equipment barriers, the ECtRtL has been mitigated to an acceptable level of safety within the defined operating environment and application, and that the evidence exists for the ADH chain to make an ALARP judgement.

Type Airworthiness Authority/Commodity DT Leader Release

Name:

Signature:

Date:

Position: Title:

Telephone: Email:

Part 3 – ADH response to TAA declaration

Acknowledgement

1. As [enter role of individual] I acknowledge receipt of the information in this ECID (dated: [enter date of relevant ECID]) and confirm that the detailed information, and the implications of that information, have been considered. The [air system] risk picture, that I hold responsibility for, has been updated accordingly.

Response to recommendations

2. I have noted the assumptions highlighted in this document, and the recommendations for non-equipment barriers contained within Annex C. [I can confirm that all of these recommendations have been acted upon and are sustainable (where necessary), unless specifically mentioned in the Feedback and Direction section.]

Feedback and direction[xv]

3. As a result of considering the content of the ECID I would like to offer the following feedback/direction:

Table 3 – ADH feedback and direction

Ser No	Feedback/Direction	Related EC

Aviation Duty Holder[xvi]

Name:

Signature:

Date:

Position: Title:

Telephone: Email:

AET Tool 17.F

ECID – Summary of EFTs

Annex A – Status of equipment functional threats directly contributing to the ADH risk picture[xvii]

The following table is currently formatted for DTs using the full range of EFTs. For those who have elected to construct ECERs at EFT Group level, the appropriate lines may be aggregated to align accordingly (see AET Tool 17C – ECL Instructions, Section 2, Table 3).

ECL EFT Code	Equipment Functional Threat Description[xviii]	Related ADH Top Event	Likelihood[xix] of EFT				Key Drivers of EFT (Highlight systems or components that are a particular driver for the likelihood assessment)	Comments (any change between 'previous' and 'current' must be covered. Cross-refer to any related communication eg SEIN or items in Annex C)
			Previous Assessment	ECER Version Number	Current Assessment	ECER Version Number		
EFT1.1	Loss of flying control							
EFT1.2	Loss of flight indications							
EFT1.3	Loss of centre of gravity control							
EFT2.1	Loss of ability to extend landing gear							
EFT2.2	Loss of ground steering							
EFT3.1	Loss of engine power control							
EFT3.2	Loss of sustained engine operation							
EFT4.1	Loss of power (torque) distribution[8]							
EFT5.1	Loss of ground deceleration							
EFT6.1	Loss of altitude indication							
EFT6.2	Loss of heading indication							

AET Tool 17.F

AtkinsRéalis

ECID – Summary of Equipment Barriers

Annex B – Status of equipment barriers[xx]

Barrier Code	Equipment Barrier Description	Related Top Event and Threat or Consequence	Barrier Effectiveness[9] [xxi]				Key Escalation Factors (Highlight any factors leading to a barrier assessment below 'effective')	Comments (any change between 'previous' and 'current' must be covered. Highlight any drivers of degradation in effectiveness. Cross-refer to any related communication eg SEIN or items in Annex C)
			Previous Assessment	ECER Version Number	Current Assessment	ECER Version Number		
B23	TCAS	Loss of Safe Separation (airborne objects) and MAC	Effective		Effective			N/A
	Add further rows as required							

AET Tool 17.F

AtkinsRéalis

Have we Achieved the Learning Objectives?

- What are the parameters of risk?
- Who owns the risk?
- What is the purpose of risk assessment?
- How does DE&S determine the Equipment Contribution to RtL?

AtkinsRéalis

Questions?