Safety Case Development

For
Unmanned Aircraft Operations

Geraint Bermingham
Navigatus

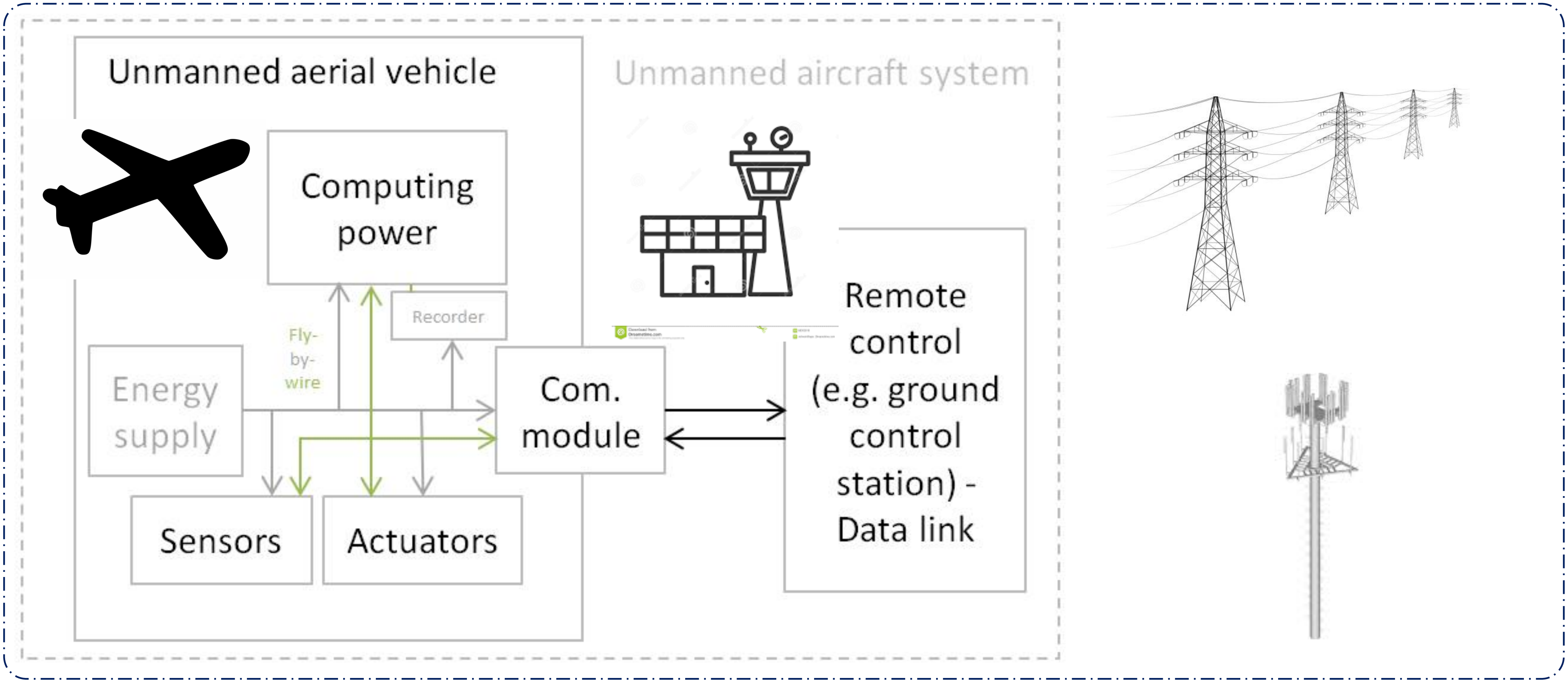
Risk NZ Conference Briefing

18 June 2019

NAVIGATUS CONSULTING

RISK NZ

Scope = system wide



On UA performance / failures

Off UA performance / failures

External interdependencies / interference

Problem Context

- The development and employment of small Unmanned Aerial Vehicle (UAV) has and continues to progress rapidly – but for the moment - operations are conducted within visual line of sight (VLOS)
- A common approach beyond that (BVLOS) has yet to be developed.
- The introduction of UA systems (UAS) - with their associated innovations and evolving technology - into established national aviation system is forcing the need to find new ways of ensuring successful and safe integration.
- The inability of the regulatory system to adapt will stifle innovation and the benefits that could be realised from a safe UA regime.
- The first country to find a viable regulatory solution stands to gain significant indirect value as well as the obvious direct benefits.
- A robust solution is required to ensure that the risks are acceptable.
- Without this assurance, large UAV operations cannot be considered viable or sustainable.

Safety Case Methodology

- A Safety Case approach offers a proven methodology for managing the risks of a given operation in non-routine situations or when the the existing rules regime is not suitable.
- A Safety Case allows the regulator to make evidenced risk-based decisions and ensure public safety on a case-by-case basis.
- With regard to UA BVLOS operations, many developers and operators will be on a development pathway that will mean the UA system will be continuously evolving. A Safety Case regime offers a flexible approach and allows on-going approvals as long as the operator can demonstrate to the regulator that defined criteria continue to be met.

Problem / Solution

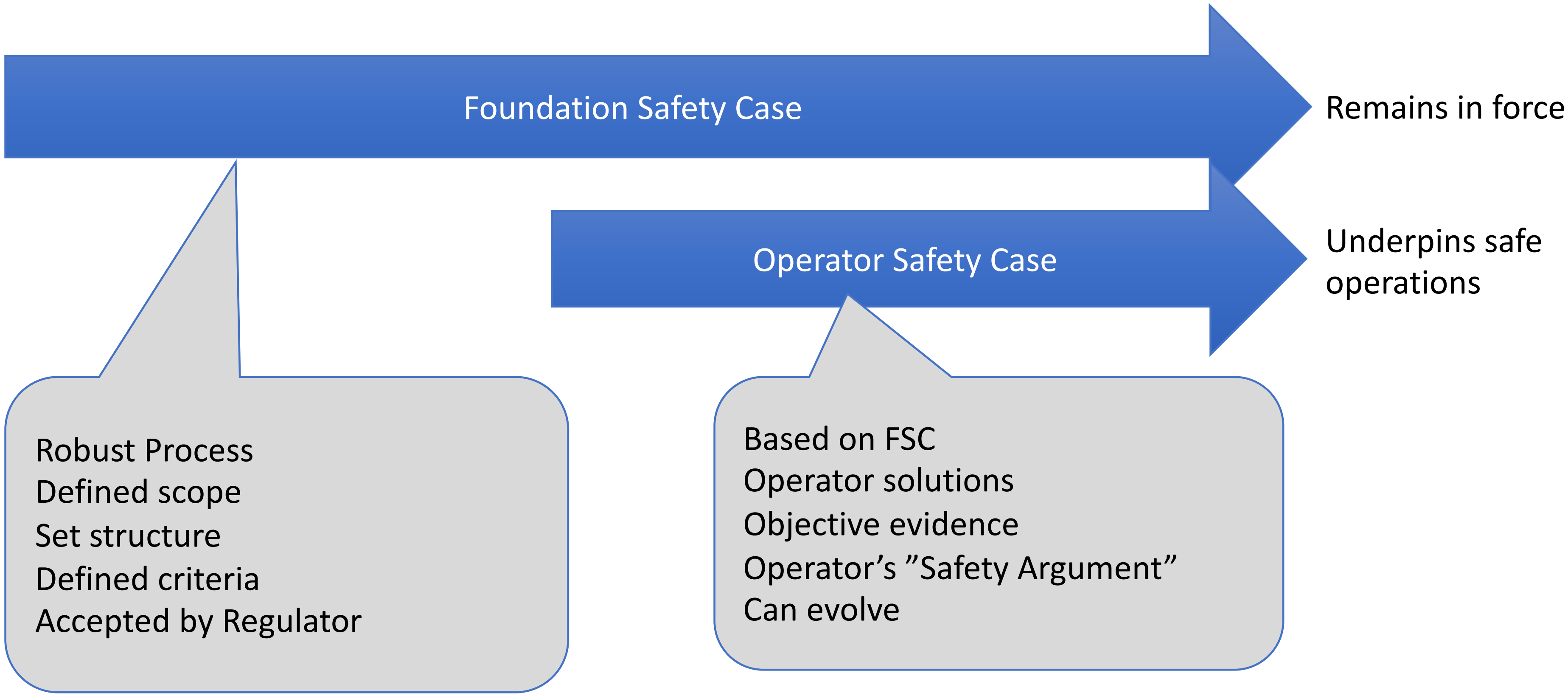
- Each applicant will probably be bring their own unique and usually innovative solution to the operational situation they are addressing.
- The existing regulatory framework does not have defined risk criteria – or the criteria are inadequately described.
- Significant burden on regulator as each operator seeks SC approval.

- A two-tier Safety Case structure has therefore been prepared:
  - Foundation Safety Case (FSC) – Setting the framework and criteria that must be met)
  - Operator Safety Case (OSC) - Showing how an operator will meet the requirements and criteria set out in the FSC

Solution

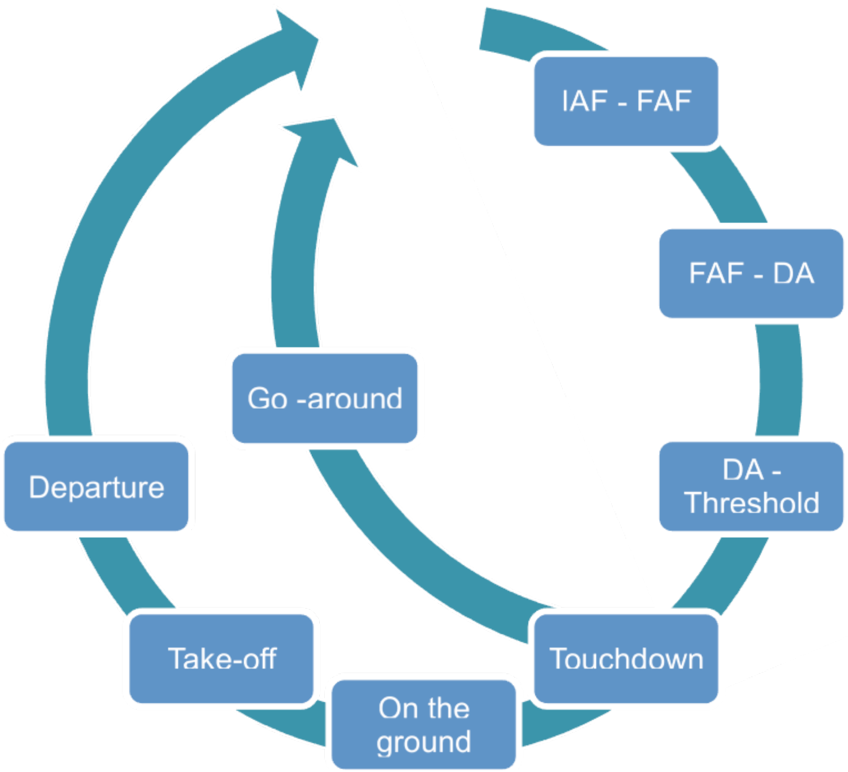
- The FSC consists of a structured framework with the required scope and an associated set of criterion to allow consideration of the functions and processes that an UAS must include and meet to enable safe and effective UAV operation.
- The aim is for the OSC to achieve a level of safety that will match or exceed the level of safety of established commercial GA operations. This will allow the societal, environmental and economic benefits of UAs to be achieved while also enabling ongoing innovation.
- If the an OSC shows that an operator can achieve the defined criteria of the FSC it should be acceptable by the CAA. *Subject to the usual F&PP, financial status tests etc.*

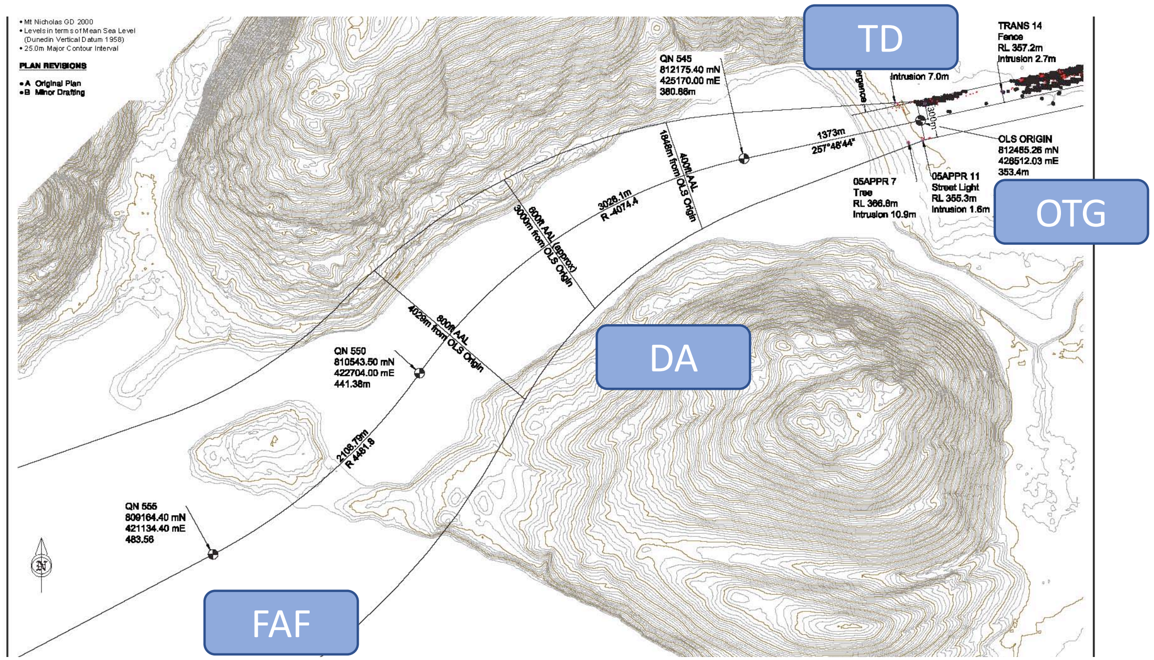
Two-tier Safety Case Concept



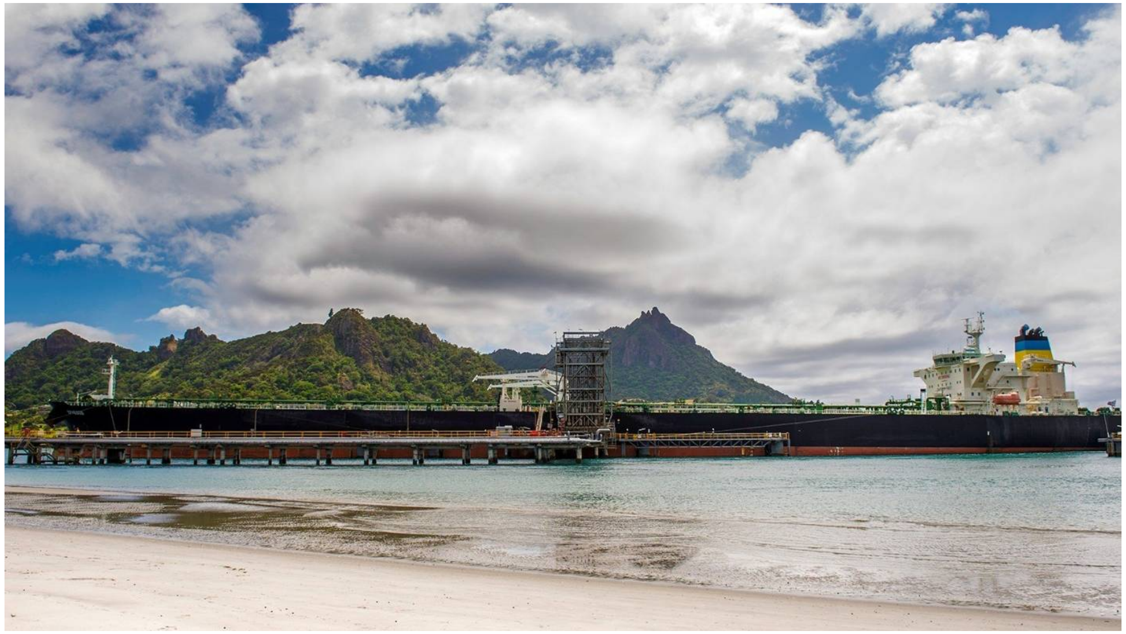
Process background: Break problem down

Aircraft phases of flight

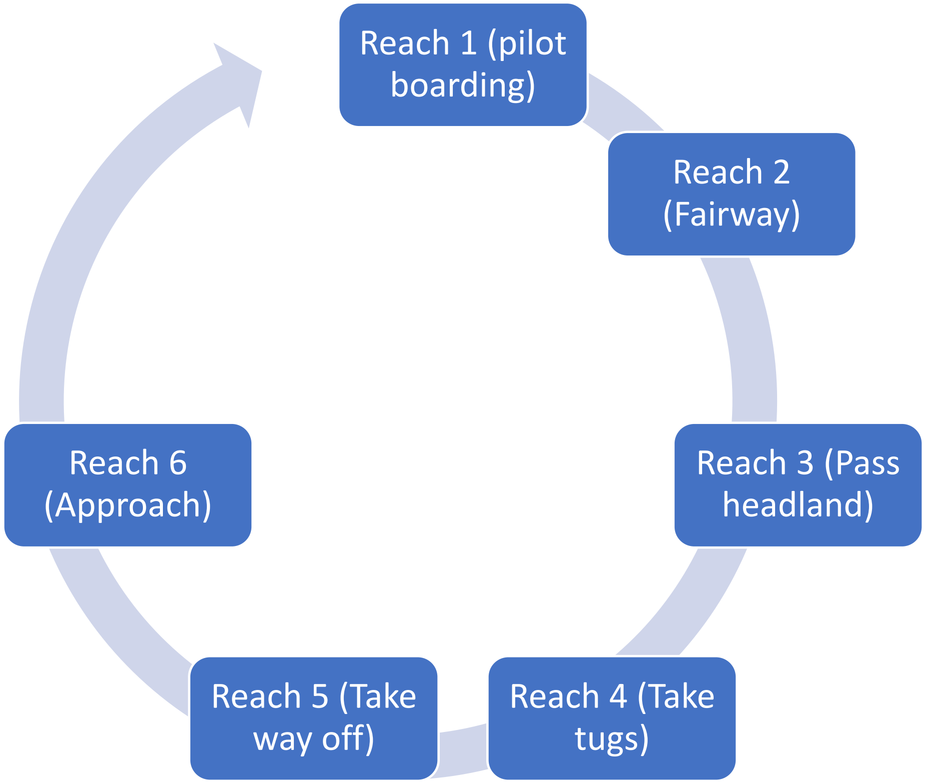




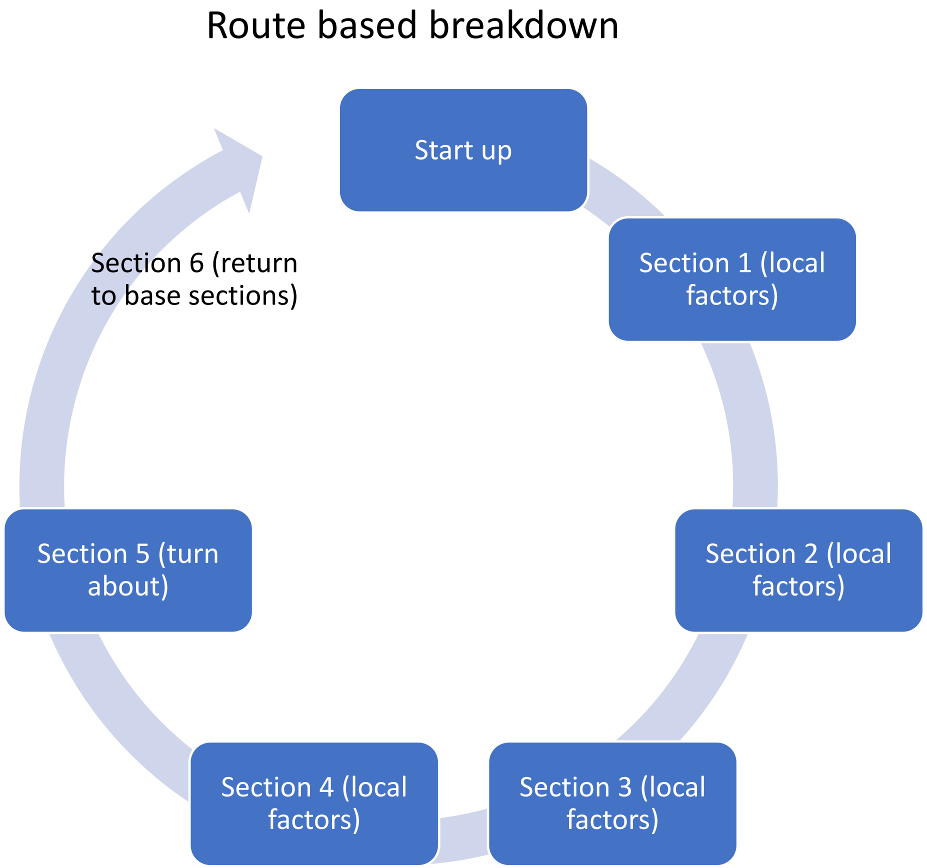
Break problem into manageable parts



Vessel approach reaches



Break problem into manageable parts



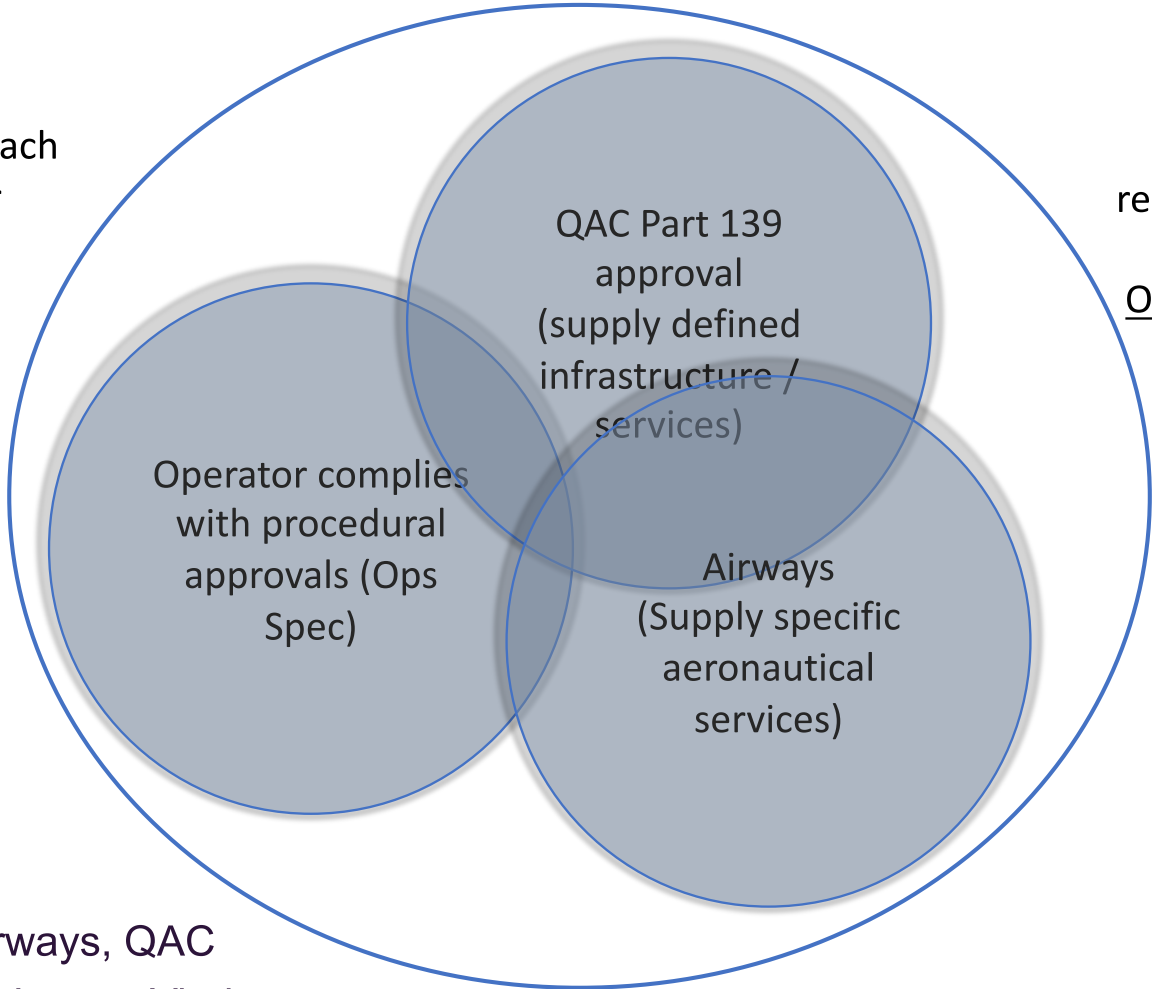
Example of use of two-tier Safety Case

- Queenstown Airport – Civil Regular Passenger Transport (RPT) Night Operations
- *Foundation Safety Case*
- *Operator Safety Cases*

  - *Air NZ: Airbus - A320 – with addition of Head Up Display and ROPS – Main line*
  - *Jetstar, Airbus - A320 – Existing equipment fit – Domestic and International*
  - *Virgin Australia) – Boeing 737-800 - Existing equipment fit – Limited application*

Multi-stakeholder context

<u>Foundation Safety Case</u> defines elements that each operational stakeholder supplies



Each stakeholder meets own responsibilities under own approved <u>Operator Safety Case</u>

CAA regulator for Air NZ, Airways, QAC

CASA regulator for Qantas, Jetstar, Virgin

Example - Operator Safety Case

Air NZ:

- *A320*
- *New technology equipage*
- *Main line*

Jetstar

- *A320*
- *Existing equipage*
- *Domestic and International*

Virgin Australia

- *Boeing 737-800*
- *Existing equipment fit*
- *Limited schedule*

67 controls in total

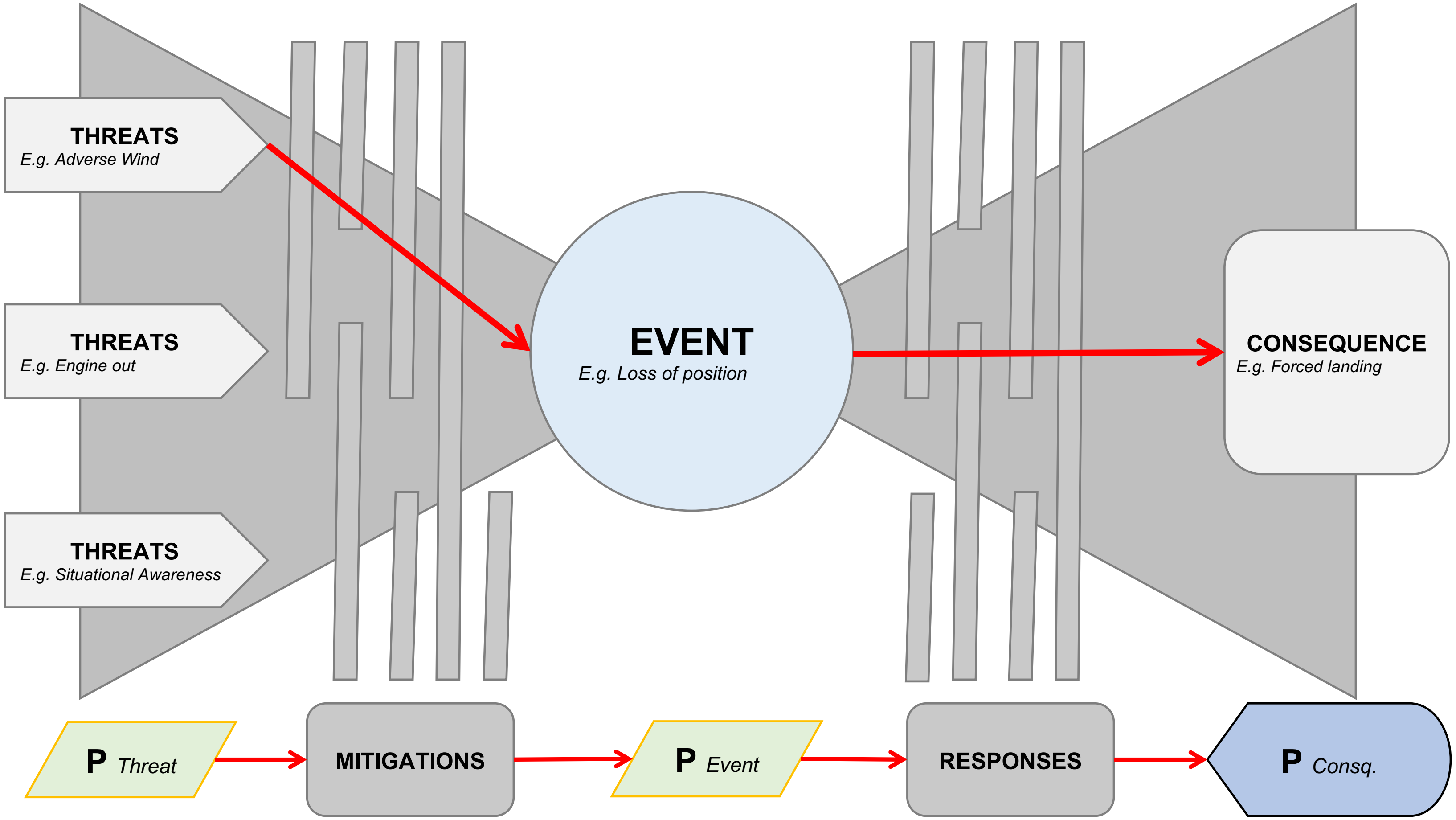
- Aerodrome operator:
  - E.g:
    - Infrastructure
    - Ground equipment
- Airlines
  - E.g:
    - Training
    - Procedures
- Airway NZ
  - Procedures

UAV Safety Case

- Development of Universal UAV Foundation Safety Case

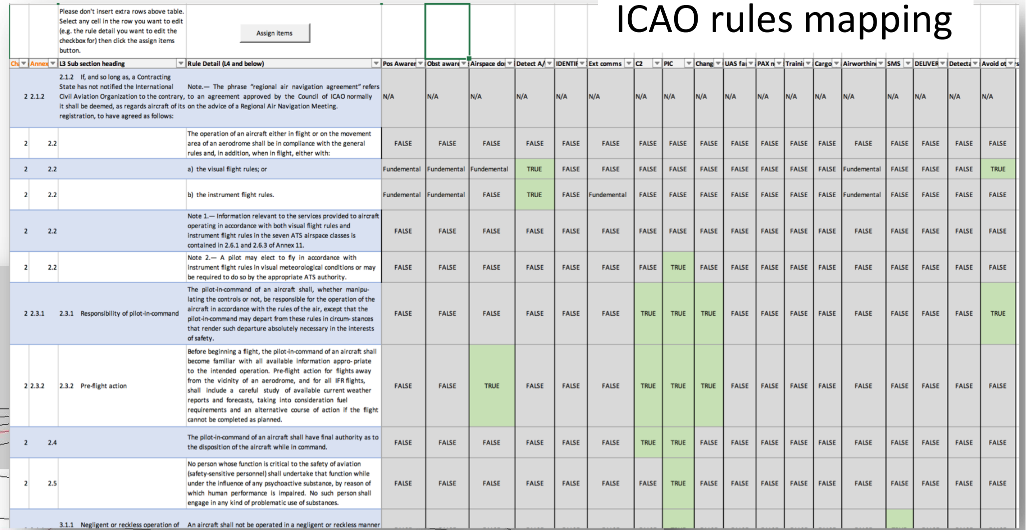
Analytical Concept

Contemporary best practice. Conforms to: ISO 31010 & AC139-15



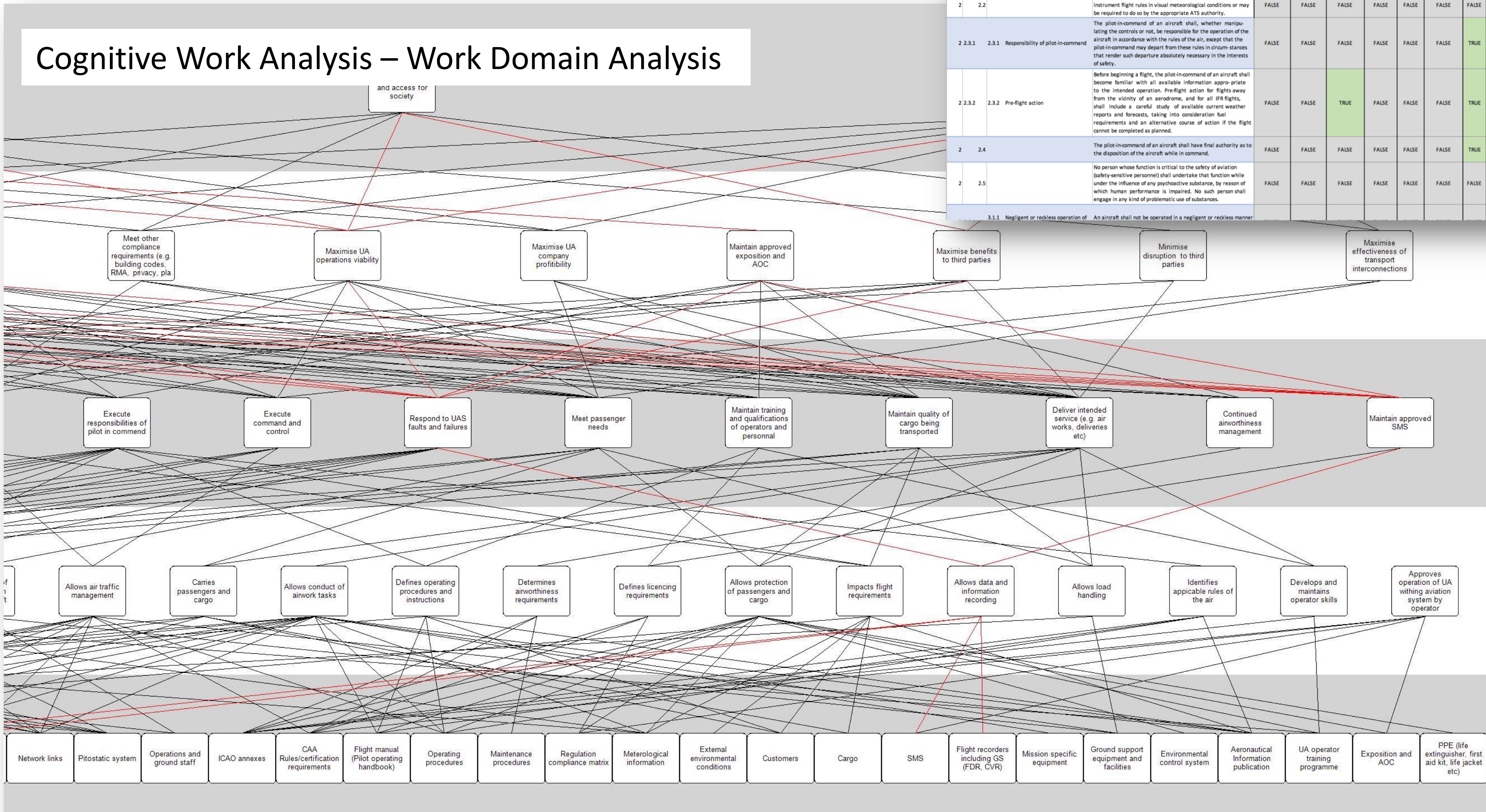
Foundation for SC

ICAO rules mapping

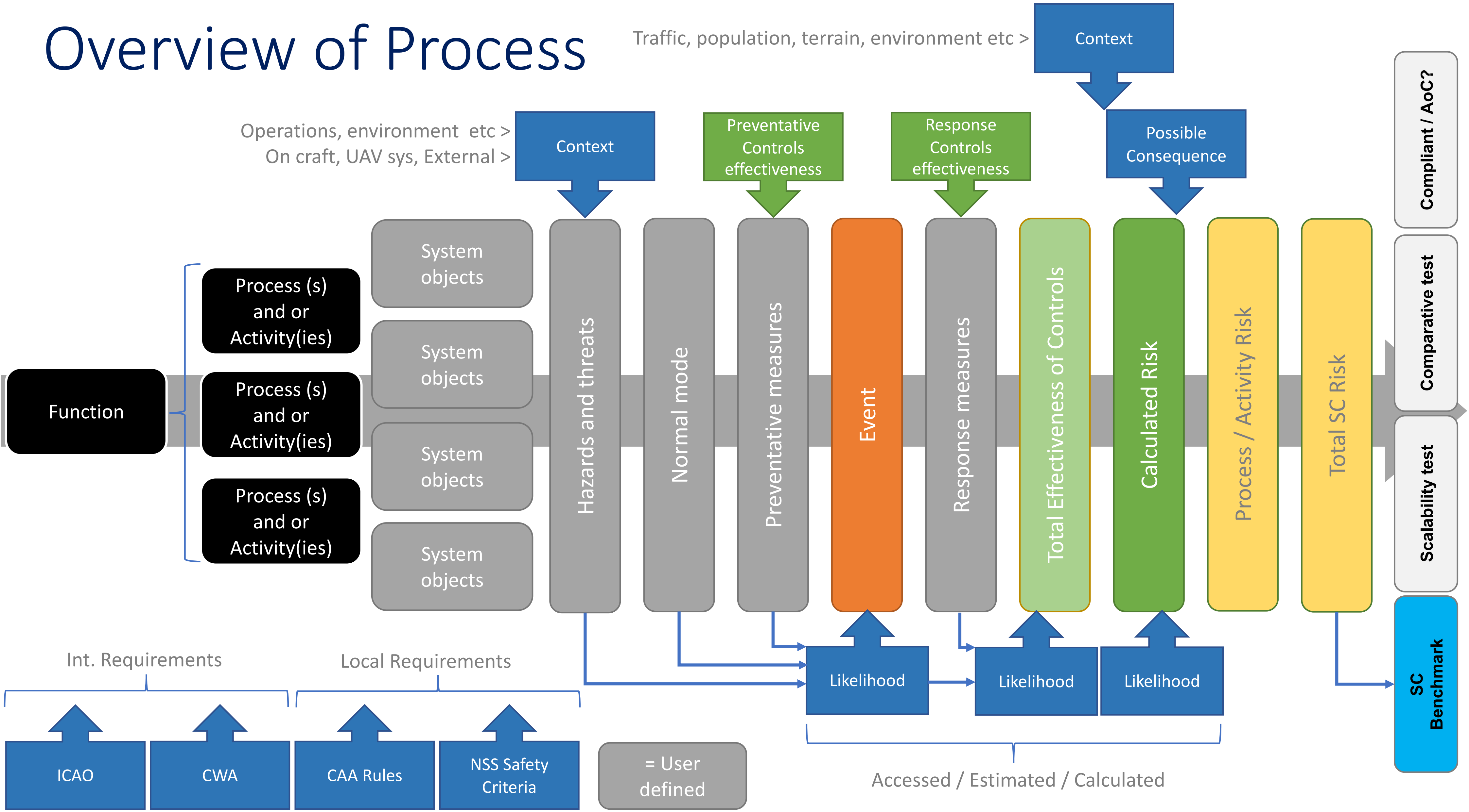


Ch	Annex	L3 Sub section heading	Rule Detail (L4 and below)	Pos Awarer	Obst aware	Airspace doi	Detect A/	IDENTIF	Ext comms	C2	PIC	Chang	UAS fai	PAX n	Trainii	Cargo	Airworthine	SMS	DELIVER	Detecta	Avoid ot
		Please don't insert extra rows above table. Select any cell in the row you want to edit (e.g. the rule detail you want to edit the checkbox for) then click the assign items button.	Assign items																		
2	2.1.2	2.1.2 If, and so long as, a Contracting State has not notified the International Civil Aviation Organization to the contrary, it shall be deemed, as regards aircraft of its registration, to have agreed as follows:	Note.— The phrase "regional air navigation agreement" refers to an agreement approved by the Council of ICAO normally on the advice of a Regional Air Navigation Meeting.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	2.2		The operation of an aircraft either in flight or on the movement area of an aerodrome shall be in compliance with the general rules and, in addition, when in flight, either with:	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	2.2		a) the visual flight rules; or	Fundemental	Fundemental	Fundemental	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Fundemental	FALSE	FALSE	FALSE	TRUE
2	2.2		b) the instrument flight rules.	Fundemental	Fundemental	FALSE	TRUE	FALSE	Fundemental	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Fundemental	FALSE	FALSE	FALSE	FALSE
2	2.2		Note 1.— Information relevant to the services provided to aircraft operating in accordance with both visual flight rules and instrument flight rules in the seven ATS airspace classes is contained in 2.6.1 and 2.6.3 of Annex 11.	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	2.2		Note 2.— A pilot may elect to fly in accordance with instrument flight rules in visual meteorological conditions or may be required to do so by the appropriate ATS authority.	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	2.3.1	2.3.1 Responsibility of pilot-in-command	The pilot-in-command of an aircraft shall, whether manipu-lating the controls or not, be responsible for the operation of the aircraft in accordance with the rules of the air, except that the pilot-in-command may depart from these rules in circum- stances that render such departure absolutely necessary in the interests of safety.	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
2	2.3.2	2.3.2 Pre-flight action	Before beginning a flight, the pilot-in-command of an aircraft shall become familiar with all available information appro- priate to the intended operation. Pre-flight action for flights away from the vicinity of an aerodrome, and for all IFR flights, shall include a careful study of available current weather reports and forecasts, taking into consideration fuel requirements and an alternative course of action if the flight cannot be completed as planned.	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	2.4		The pilot-in-command of an aircraft shall have final authority as to the disposition of the aircraft while in command.	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	2.5		No person whose function is critical to the safety of aviation (safety-sensitive personnel) shall undertake that function while under the influence of any psychoactive substance, by reason of which human performance is impaired. No such person shall engage in any kind of problematic use of substances.	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
		3.1.1 Negligent or reckless operation of	An aircraft shall not be operated in a negligent or reckless manner																		

Cognitive Work Analysis – Work Domain Analysis



Overview of Process



UAV Safety Criteria

- *When is 'safe' safe enough?*

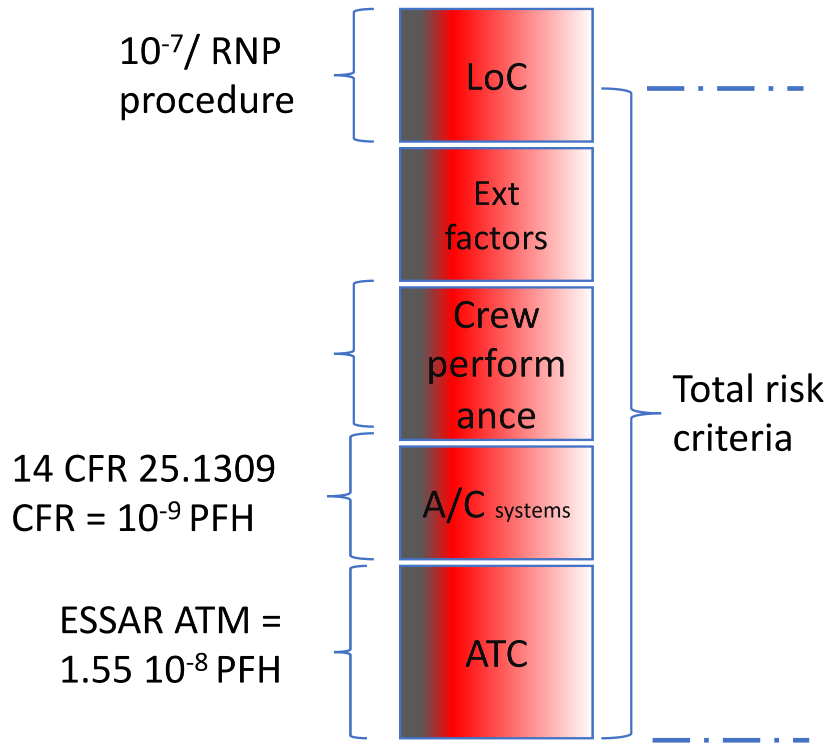
The Risk Criteria / Target Safety Level Problem

Quantitative

- Easy to “pick a number”
- Difficult to perceive actual meaning
- Very difficult (impossible?) to measure
- Differing units
- Unquantifiable factors

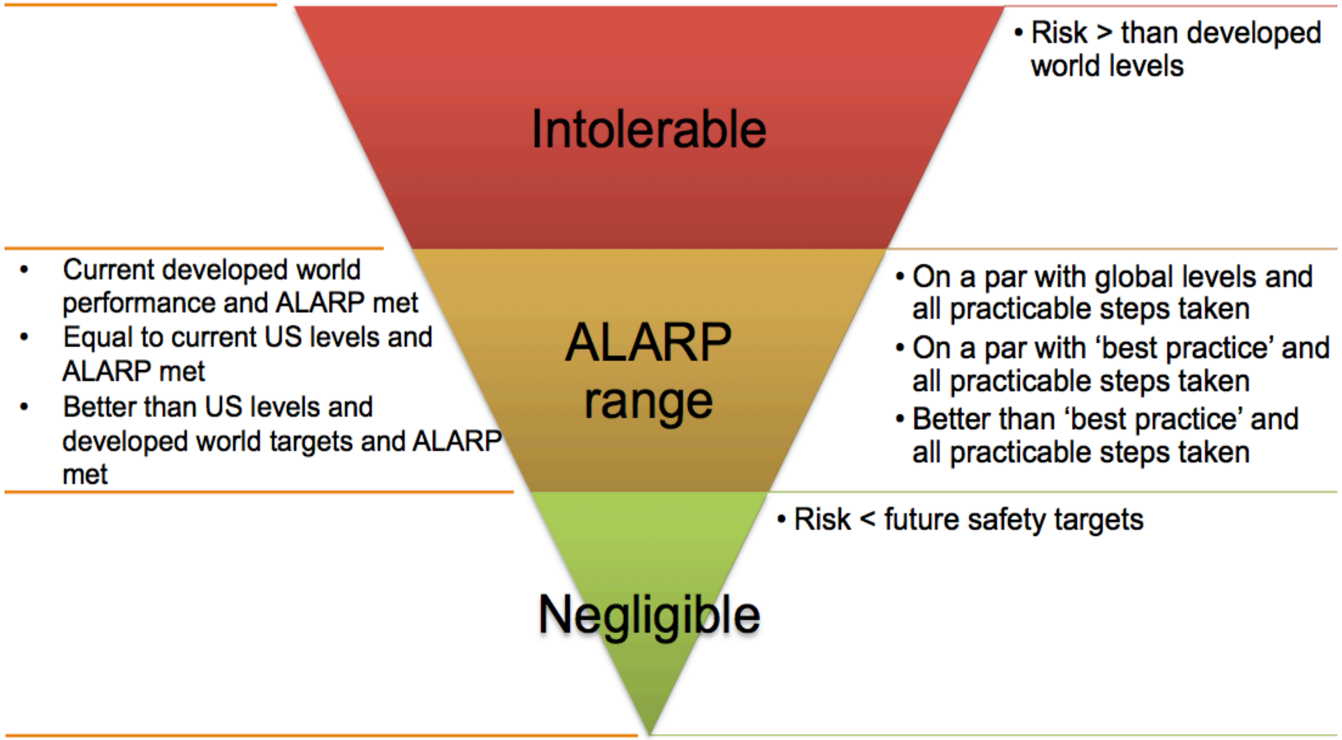
Qualitative

- Difficult to prove / justify
- Societal perceptions (new vs established activities)
- Imprecise

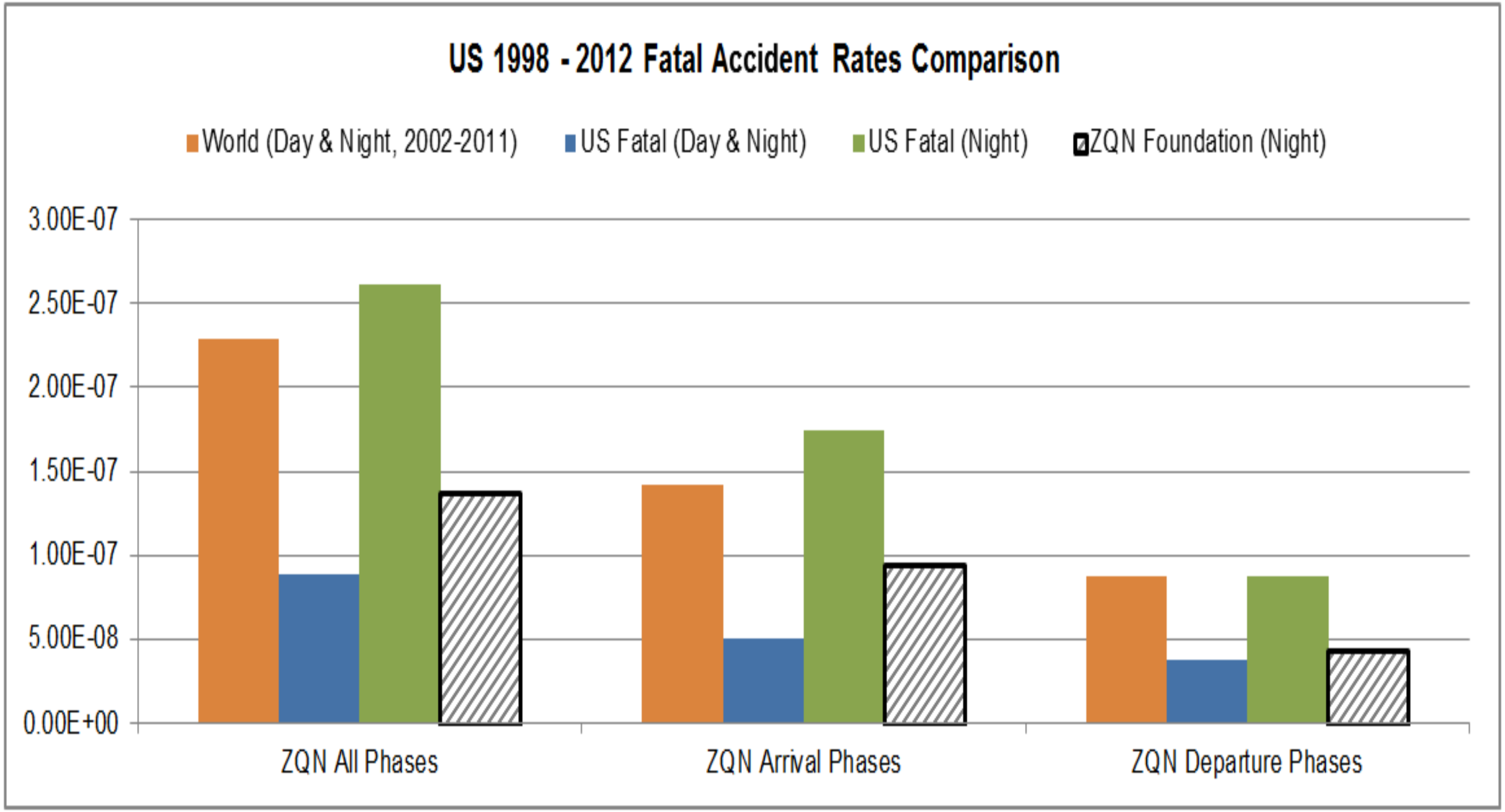


Units: PFH, per procedure, en-route FH/ATM, component failure PH, per phase of flight, etc

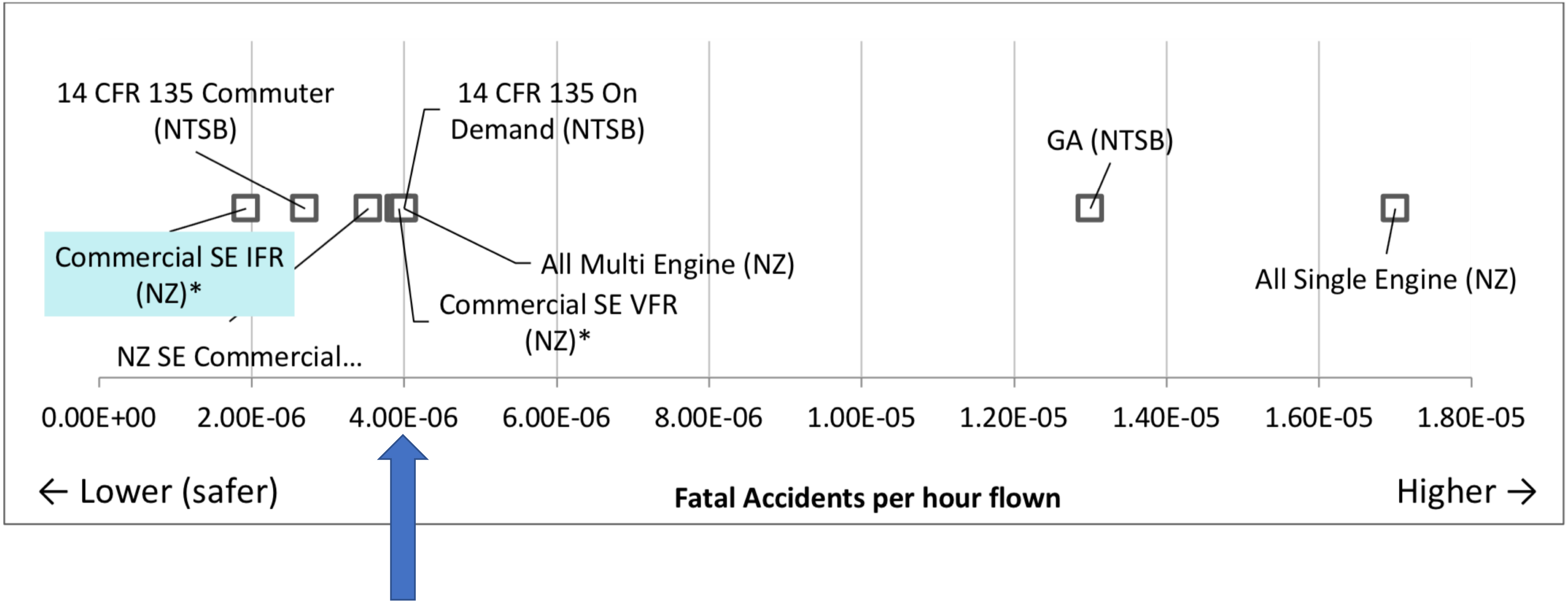
ALARP (concept)



Alternative - Bench marking (example)



Alternative - Bench marking (UAV example)



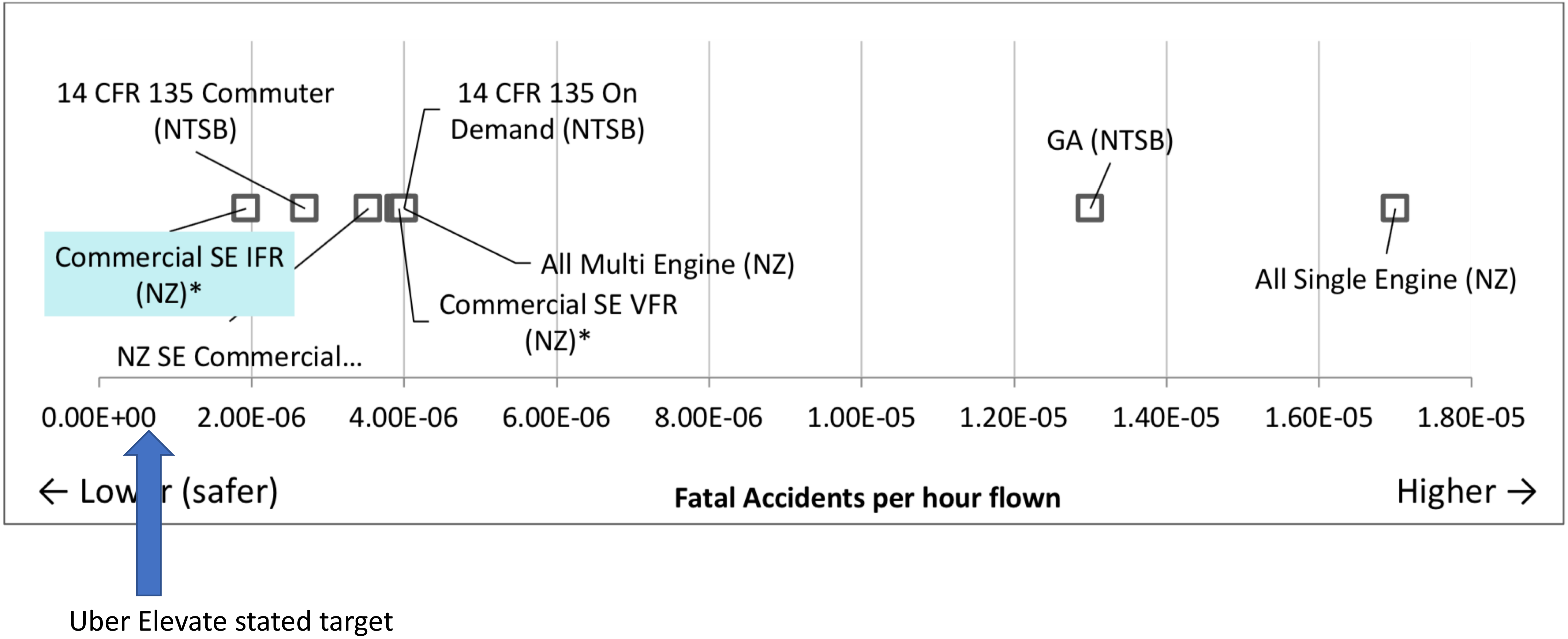
Similar operations – actual (socially accepted)

Uber Elevate White Paper 2019

“**Safety.** *We believe VTOL aircraft need to be safer than driving a car on a fatalities-per-passenger-mile basis. “*

“Federal Aviation Regulation (FAR) Part 135 operations (for commuter and on-demand flights) on average, have twice the fatality rate of privately operated cars, but we believe this rate can be lowered for VTOL aircraft at least to one-fourth of the average Part 135 rate, making VTOLs twice as safe as driving.”

Alternative - Bench marking (UAV example)

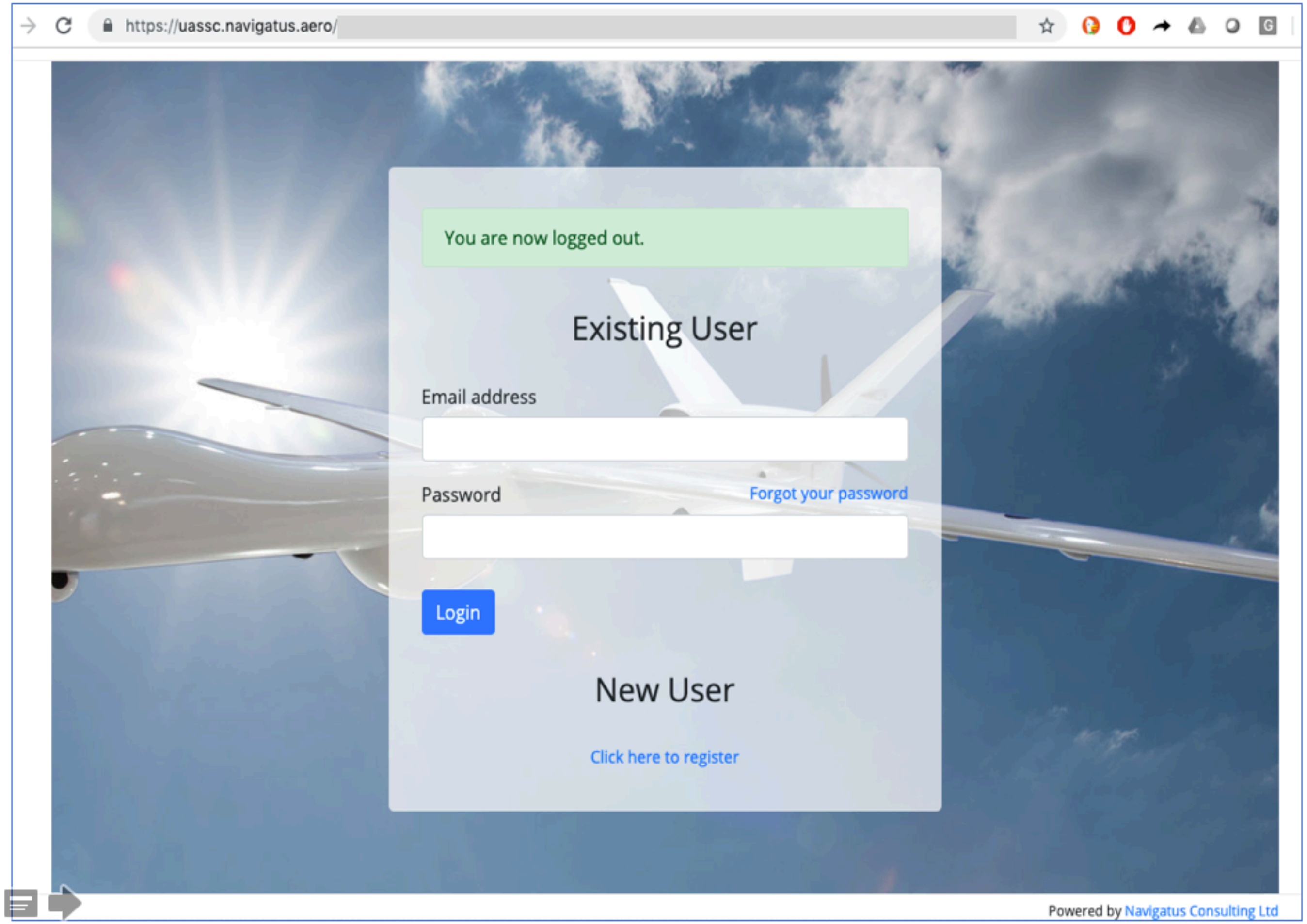


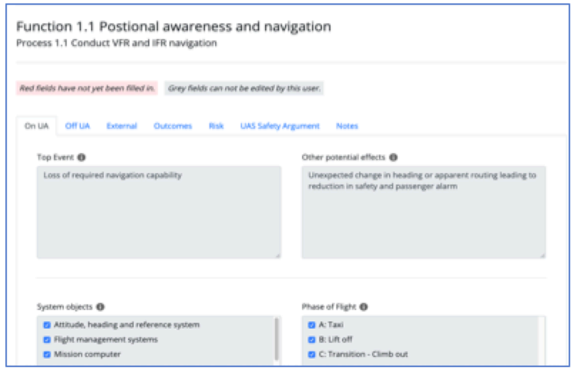
Proposed Criteria (Draft):

- Each process has an associated fatality risk faced by individual passengers and members of the public due to:
  - 'On Craft' hazards and threats (typically system or performance failures)
  - Hazards and threats that may impact the ''Off craft' elements of the UA system (typically system performance failures and human performance failures)
  - Risks created by external hazards and influences unrelated to the UA systems

- National Aviation Safety Criteria met
- That, for each given process, can be demonstrated that the risk is ALARP
- The Foundation Safety Case *Target Level of Safety* (TLS) = $<4 \times 10^{-6}$
- That the risk of not being able to carry out a given operational process is $<10^{-7}$ per flight hour (measured quantitatively were possible else qualitatively)
- That the collision risk is $<10^{-7}$ per flight hour (measured quantitatively)

On-line Interface / Safety Case Tool





Secure On-line Interface / SC Tool

https://uassc.navigatus.aero/

Welcome *OSC Test User* of *UAS Operator*. Not you?

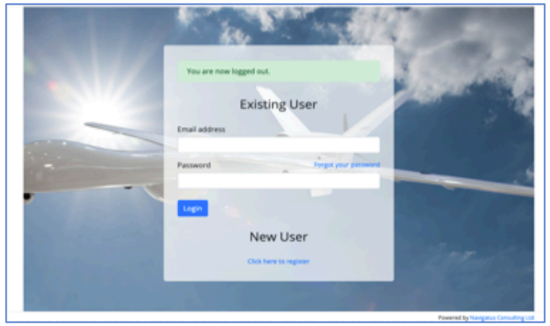
You have *Operator Safety Case (OSC) administrator* access rights.

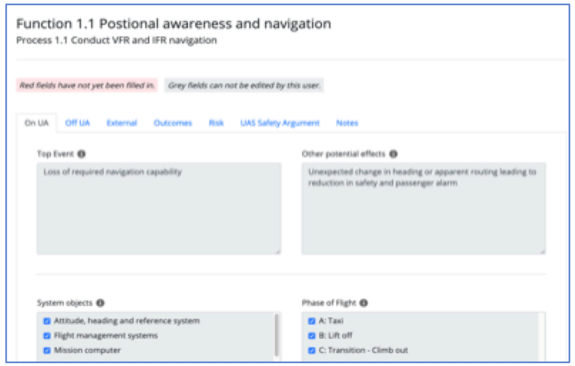
Currently viewing: **A2A EVLOS Safety Case**

To change safety case or set up a new safety case return to the Home page.

Threat-Event Sequence Analysis

ID	Function	Process	Operator Progress	Action
1.1	Postional awareness and navigation	Conduct VFR and IFR navigation	74%	Edit Summarise
2.1	Maintain airspace domain situational awareness	Maintain obstacle and terrain awareness and separation	70%	Edit Summarise
3.1	Maintain obstacle and terrain awareness and separation	Awareness of obstacles and fixed hazards	70%	Edit Summarise
3.2	Maintain obstacle and terrian awareness and separation	Awareness of terrain	100%	Edit Summarise
3.3	Maintain obstacle and terrian awareness and separation	Manourver and respond	100%	Edit Summarise
4.1	Other aircraft	Obtain air traffic information	100%	Edit Summarise
4.2	Other aircraft	2-way communications and info flow	100%	Edit Summarise





Practical Example:

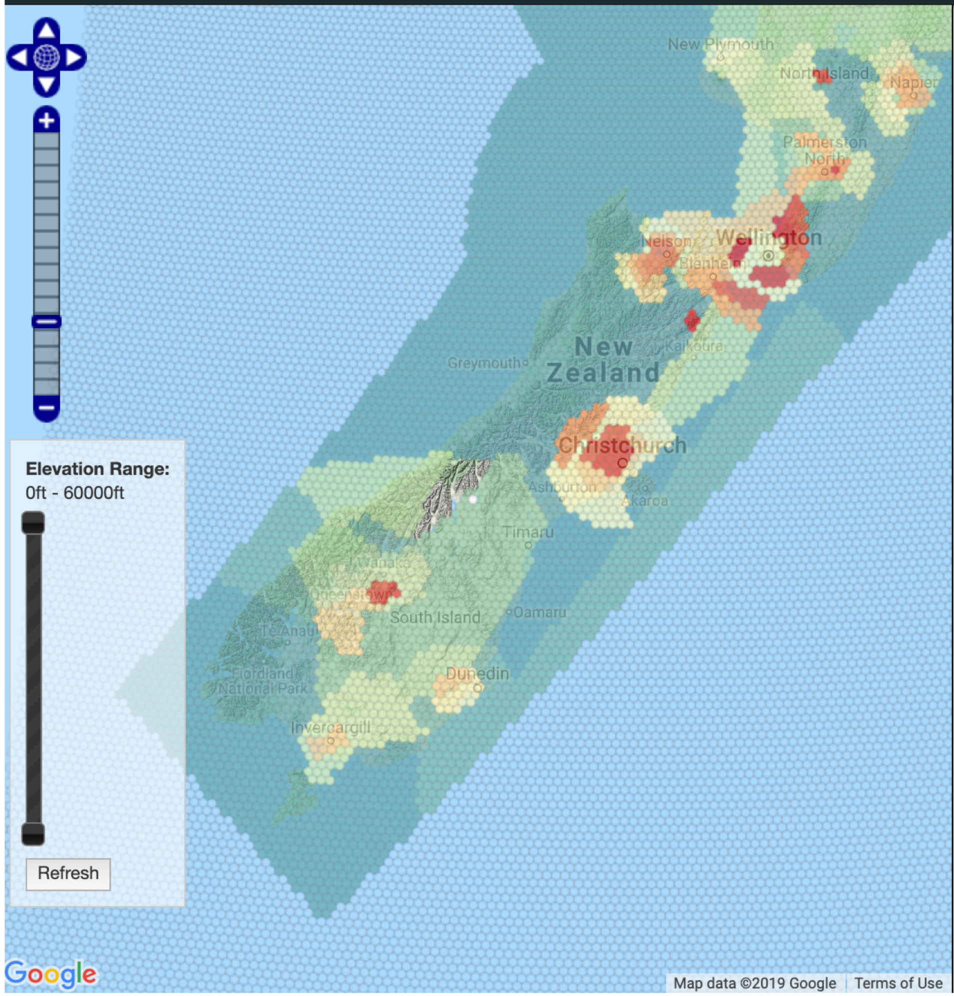
for Unmanned Aircraft and General Aviation Aircraft in Uncontrolled Airspace

Linking airspace collision model with Safety Case

National Airspace Risk Reference System

Not Secure | asrp.navigatusconsulting.com/map/index/26902

Show: Exposure   Logged in as   Logout



AirSpace Risk Profile - Sample Data

Note: Mock data for Complexity and a/c movements.

Cell ID	Ref X	Ref Y
26902	51	150

Sample Complexity Factors

Aircraft Count

Aircraft Proximity

Aircraft Mixture

Proportion Climbing

Proportion Descending

Heading, Speed and Altitude Changes

Variance of All Aircraft Headings

Conversion of Traffic Flows

Separation Standards

Overall Inherent Complexity Rating

Sample Aircraft Movements

IFR - Large	947
IFR - Medium	214
IFR - Small	329
VFR	324
Fixed Wing	1965

Safety Case Linked to Airspace Risk Model

Link to the Operational Base

Open Airspace Risk Tool

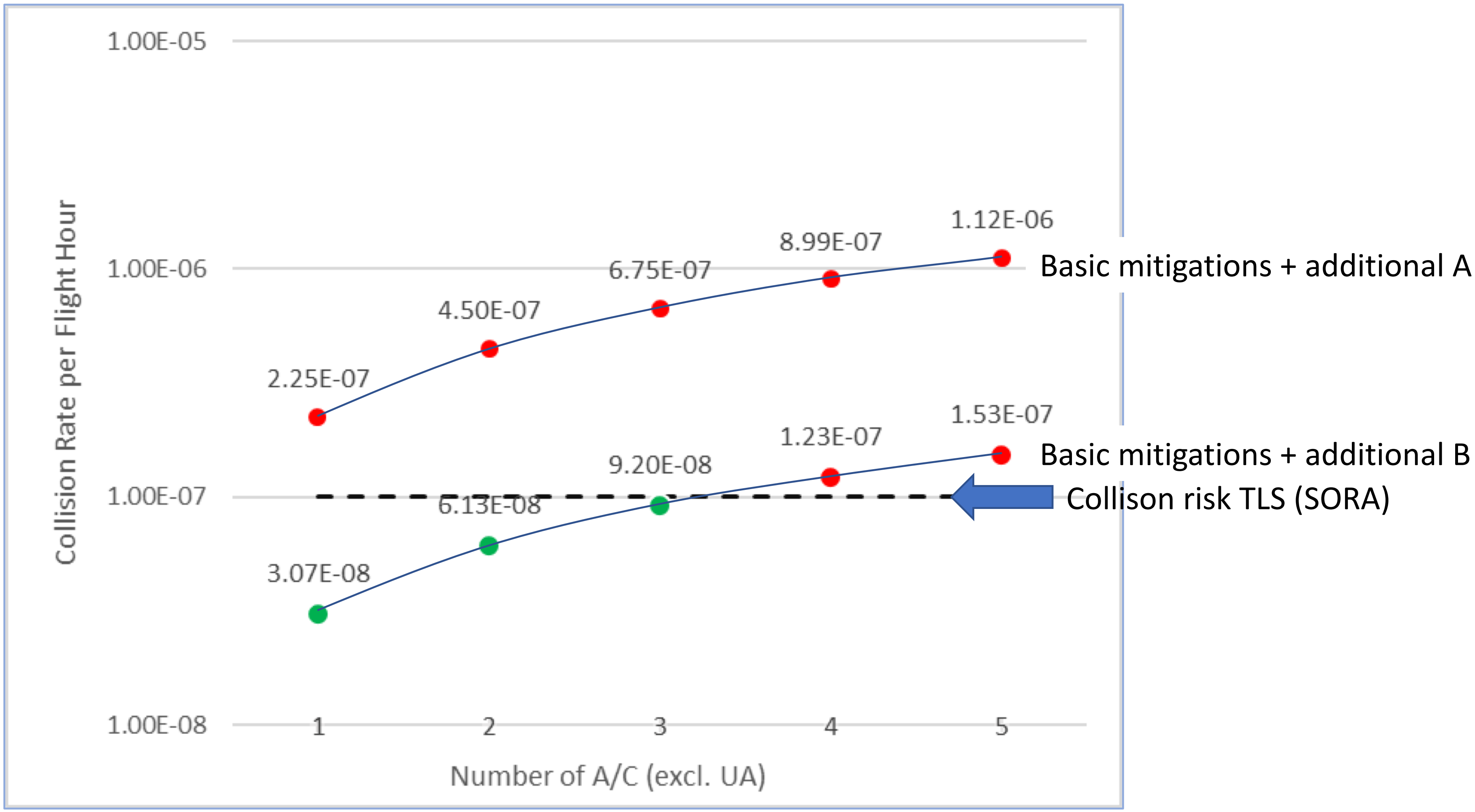
Show selected cell on the Airspace Risk Tool

Operational Area

26902

Select a cell from the Airspace Risk Tool grid below

Example results – Applied Collision Risk Model



Take aways (1) ……….

A: Until:

- Technology matures
- Rule system catches up with technology

Safety Case approach offers near term regulatory solution to managing risk while enabling innovation.

B: Process model enables objective of existing system

C: Establishing criteria is not straight forward

Take aways (2) ……….

D: While Safety Case solution potentially huge burden on regulator

E: Practical Safety Case framework can be developed that:

- Enables efficient oversight and monitoring
- Flexible – allowing ongoing innovation

F: For UAV; a practical quantitative / universal collision model can be developed

G: The proposed safety criteria (a step up from the current ‘accepted’ risk) are probably achievable

Thank you

Geraint Bermingham
Navigatus

www.navigatusconsulting.com
g.bermingham@navigatusconsulting.com

+64 21884425