SQEP

Safeguarding Mission-readiness

Helen Summers, MSc, CEng, MRAeS, Principal Safety Consultant at SQEP Ltd

Delivering Safety Safely
Proportionality and Pragmatism

The Gerhard Sedlmayr Lecture
RAeS Hamburg Branch
11 November 2025

https://doi.org/10.5281/zenodo.18404322

Deutsche Gesellschaft für Luft- und Raumfahrt Lilienthal-Oberth e.V. Bezirksgruppe Hamburg

ROYAL AERONAUTICAL SOCIETY HAMBURG BRANCH e.V.

ZAL

VDI Verein Deutscher Ingenieure Hamburger Bezirksverein e.V. Arbeitskreis Luft- und Raumfahrt

HAW HAMBURG

Hamburg Aerospace Lecture Series
Hamburger Luft- und Raumfahrtvorträge

RAeS Hamburg in cooperation with the DGLR, VDI, ZAL & HAW invites you to a lecture

Annual Gerhard Sedlmayr Lecture

Delivering Safety Safely: Proportionality and Pragmatism

Helen Summers, MSc, CEng, MRAeS, Principal Safety Consultant at SQEP Ltd

Date: Tuesday 11 November 2025, 18:30 *(light refreshments available from 18.00 and there will be a get-together with refreshments after the lecture)*
Location: Goldene Zeiten, Harvestehuder Weg 48, 20149 Hamburg
(in-person only – not online!)

(If you wish to attend, please register online or send a mail to Susanne Altstaedt,

What is safe? Most programmes nowadays are multi-national and sometimes the design is not conducted in accordance with recognised standards. In the modern (post Haddon-Cave) era of Type Certification and regulation, how do we deliver a safe FMS programme for a new, but 60-year-old capability, accommodating new technology and systems without asking everyone to start from scratch ?
In this lecture, as well as considering the philosophy of safety delivery, I will look at how we are developing the equipment contribution to the Air System Safety Case for the new Chinook H47 (Extended Range) helicopter for the RAF to enable our Chief Engineer to understand and transfer risk to the ultimate risk taker. The presentation will look at the drive for proportionality and pragmatism whilst retaining appropriate levels of rigour, and why that matters.

A Royal Air Force Chinook Mark 6 helicopter takes its first flight at RAF Odiham. © Crown copyright https://www.defenceimagery.mod.uk

Helen is currently a Principal Consultant at a small, specialist consultancy firm, SQEP Ltd, where she is the Head of Area for Safety, Environmental and Human Factors disciplines. A former RAF Engineer Officer, she spent nearly 25 years in the RAF and Civil Service, working in both engineering and programme management, on multiple equipment types (Tristar, Hercules, Nimrod, Eurofighter, Communications and Complex Weapons) as well as having been responsible at a departmental level for Safety, Environment and Quality Assurance.

DGLR / HAW — Prof. Dr. Dieter Scholz, FRAeS — Tel.: (040) 42875 8825 — info@ProfScholz.de
RAeS — Richard Sanderson — Tel.: (04167) 92012 — events@raes-hamburg.de

DGLR Bezirksgruppe Hamburg — http://hamburg.dglr.de
RAeS Hamburg Branch — http://www.raes-hamburg.de
VDI, Arbeitskreis L&R Hamburg — http://www.vdi.de/
ZAL TechCenter — http://www.zal.aero

Hamburg Aerospace Lecture Series
DGLR HAW Hamburg RAeS VDI ZAL

Experience – Helen Summers

SQEP

Training – Helen Summers

SQEP

ENGINEERING & LEADERSHIP

MANCHESTER 1824
The University of Manchester

Cranfield University

Engineering Council

ROYAL AERONAUTICAL SOCIETY

ASHRIDGE

PROGRAMME MANAGEMENT & TRAINING

association for project management
apm

PRINCE2

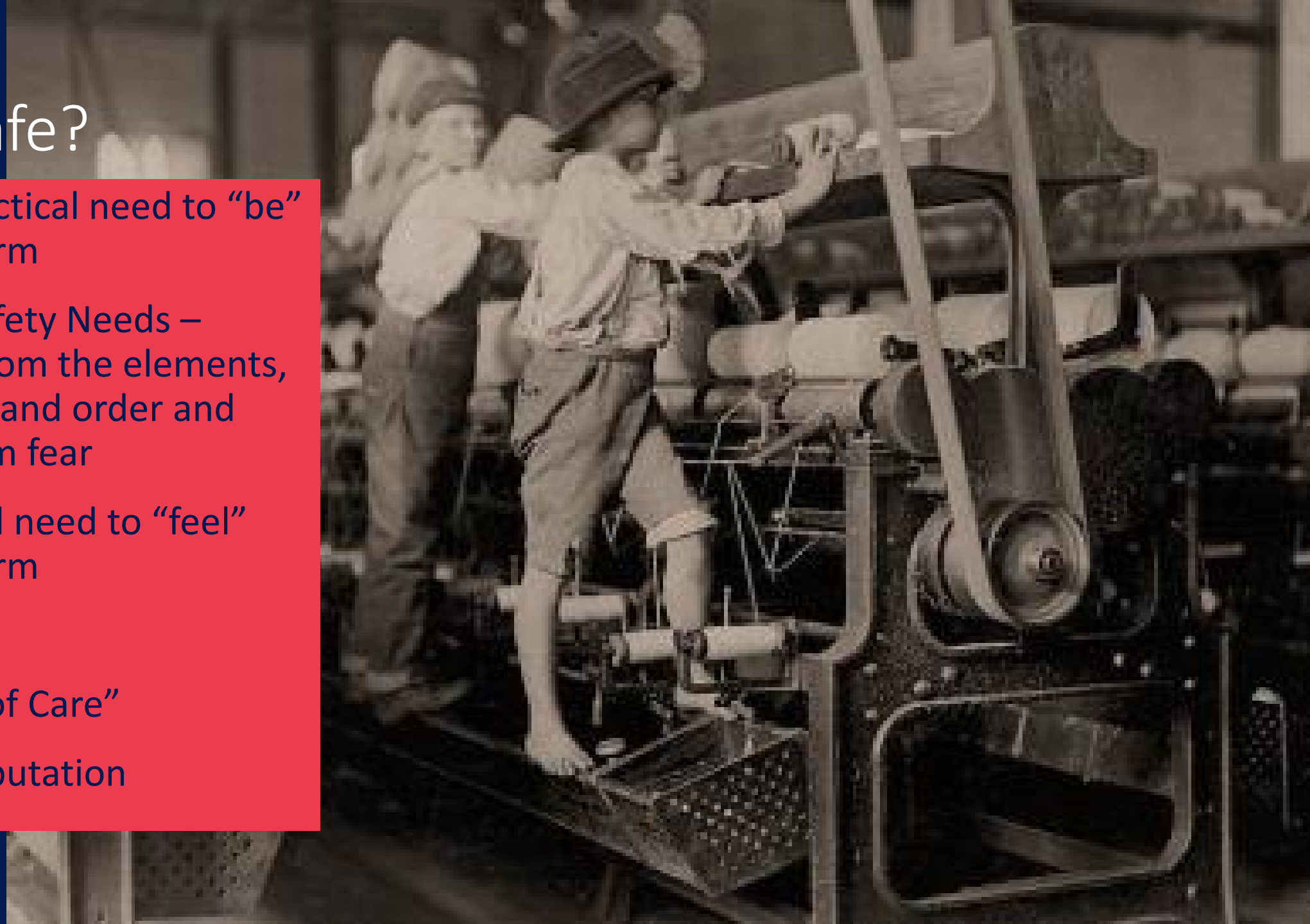
UNIVERSITY of CAMBRIDGE
CELTA

ITIL®

CONTROL
DEFINE
MEASURE
ANALYZE
IMPROVE
6σ

What is Safe?

- Human's Practical need to "be" free from harm
- Maslow – Safety Needs – protection from the elements, security, law and order and freedom from fear
- Psychological need to "feel" free from harm
- Societal
- Legal "Duty of Care"
- Company reputation



SAFETY ASPECTS - Occupational Health and Safety

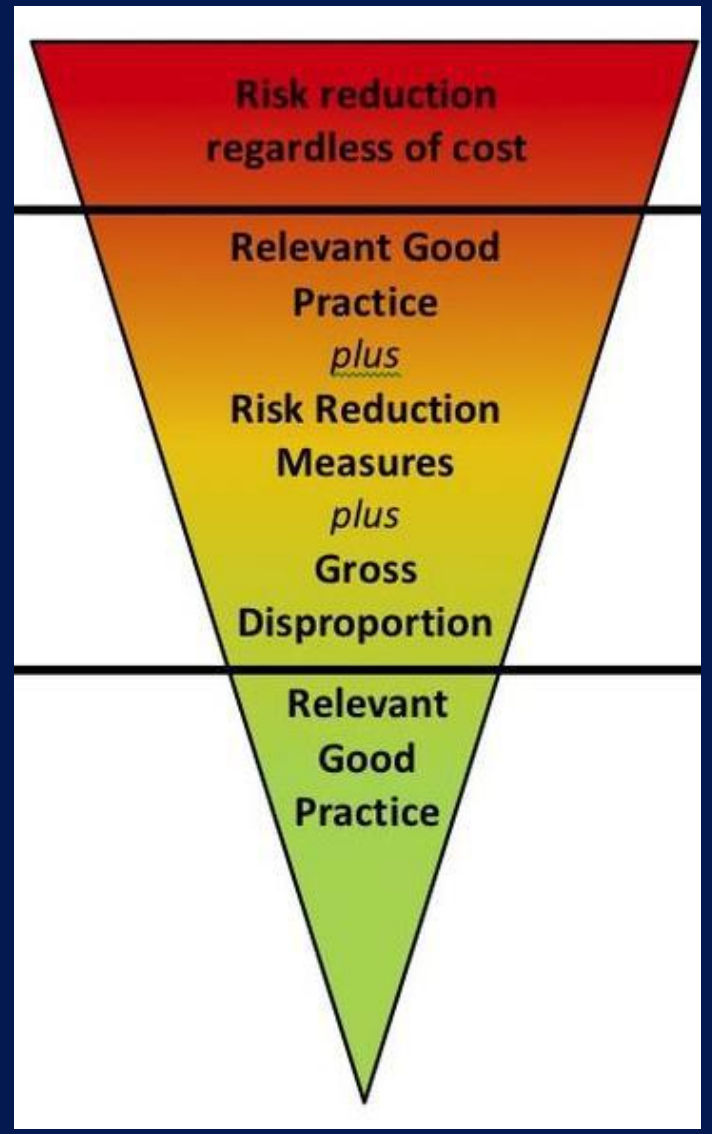
Associated with how work and the work environment can impact the health, welfare and wellbeing of people in that environment (Health & Safety at Work)

SAFETY ASPECTS – SYSTEM SAFETY (REGULATOR)

SQEP

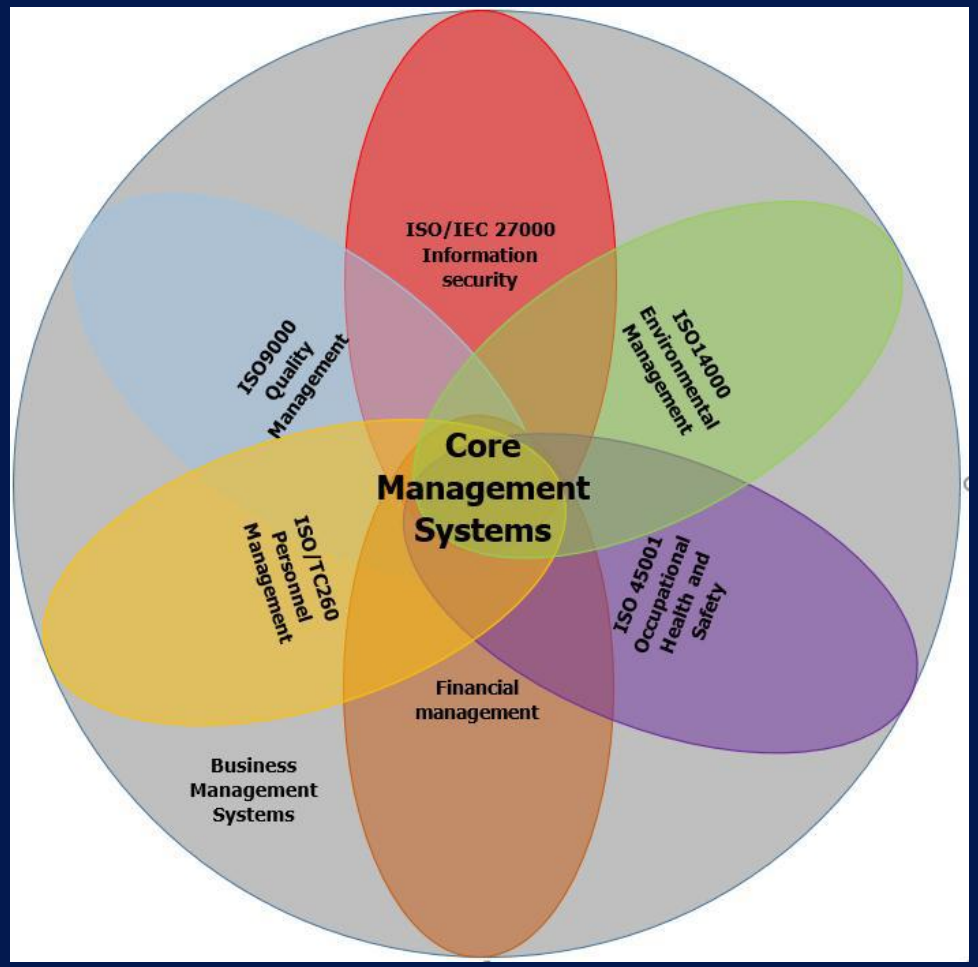
The practice of using engineering and management techniques to reduce the impact of risk associated with systems and equipment:

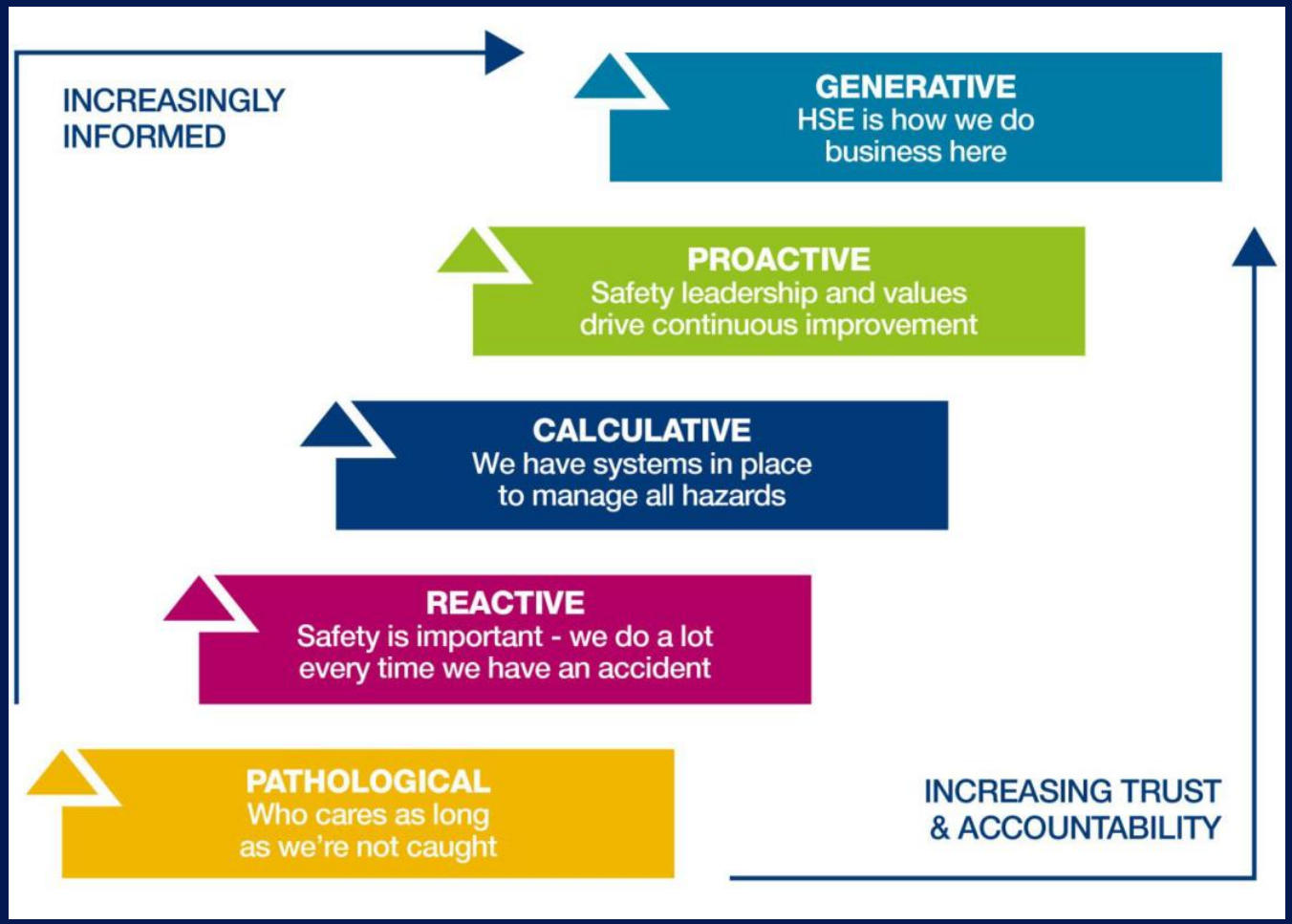
- Hazard Identification
- Risk Management
- Risk appetite and tolerability



SAFETY ASPECTS - ORGANISATIONAL

SQEP





The culture and activities associated with an organisation which seek to manage the safety risks associated with its business

1961 – 2024 - DOESN'T LOOK THAT DIFFERENT – WHY ASSESS ?

SQEP

VIVE LA DIFFERENCE !

SQEP

WHAT DO WE HAVE?

Proven design - in service since 1961 – still flying

Existing / legacy systems

Competent operators

Competent contractors

Accident history - multiple losses

Service / fault / reliability history

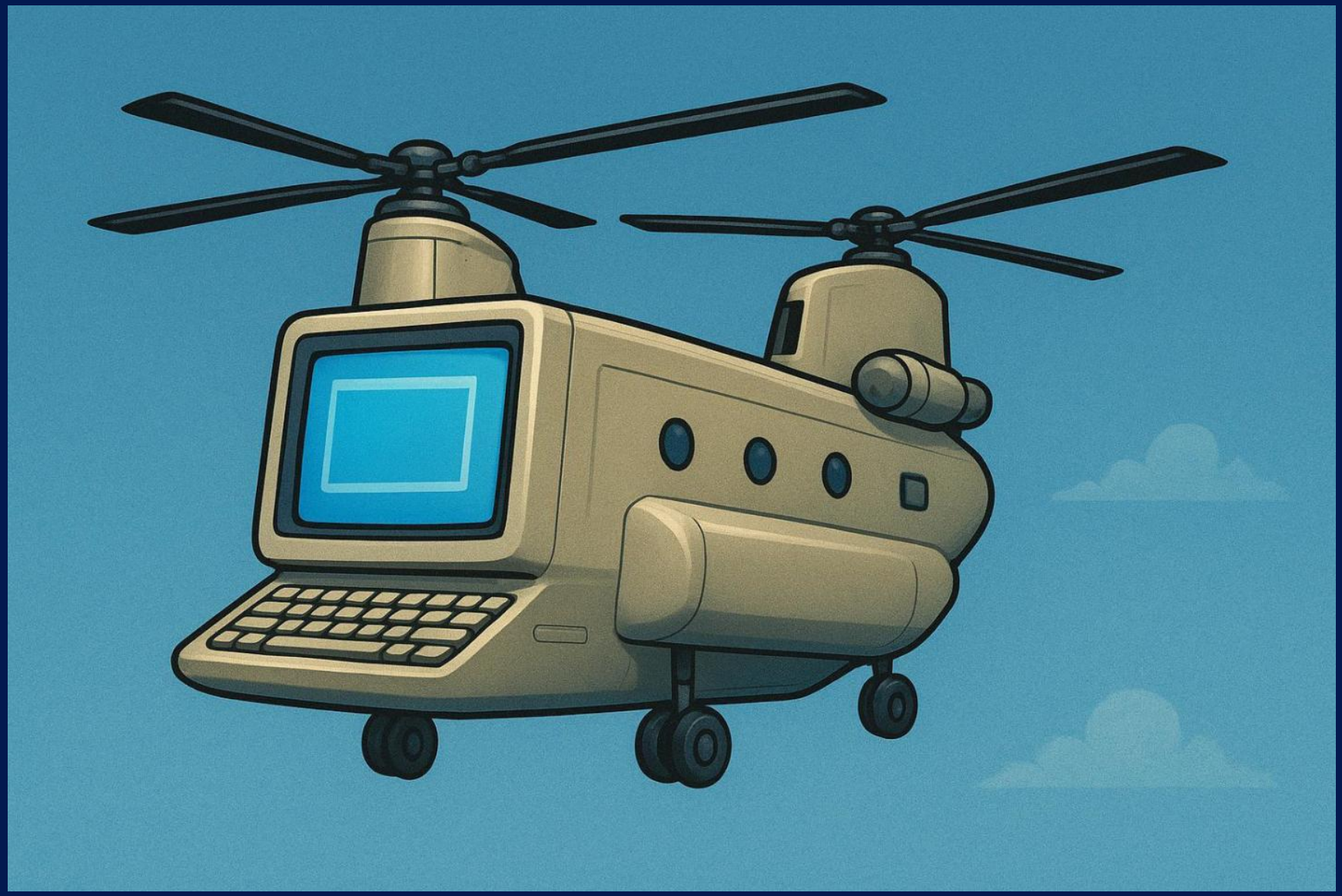
Design changes

- New systems & support
- Obsolescence & upgrade
- Greater complexity
- UK-only modification

Different standards / regulations / requirements:

- Now and then
- USA and UK

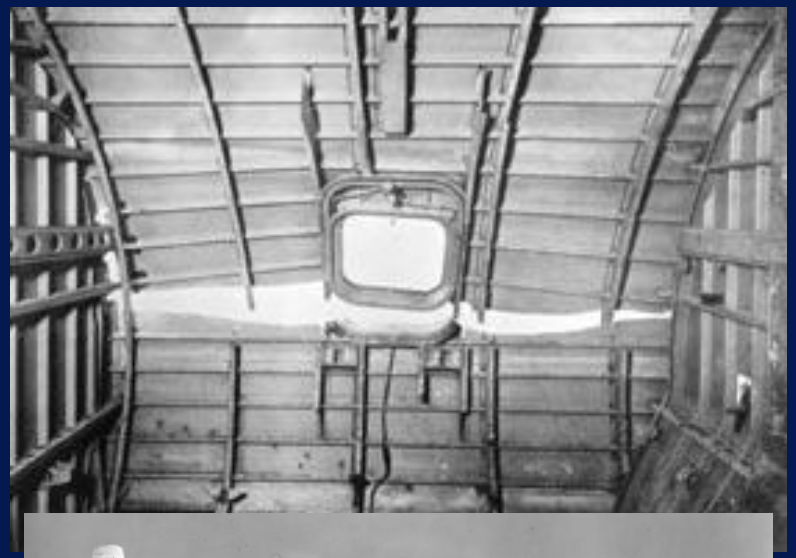
HOW THE CYBER FOR AIRWORTHNESS / SECURE BY DESIGN TEAM SEES CHINOOK



ACCIDENTS THAT CHANGED HOW WE CERTIFY AIRCRAFT – FROM FAILURE

SQEP

De Havilland Comet (1950s) – Stress Concentration factors for square apertures



The resulting debris field …

DC 10 (1974) – Cargo Door design / seal / lock

Boeing 737 - Aloha Flight 243 (1988) – fatigue, damage tolerance, inspection, repair & maintenance

ACCIDENTS THAT CHANGED HOW WE CERTIFY AIRCRAFT – FROM FIRE

SQEP

Boeing 737 - British Airtours Flight 28M (1985) - Cabin safety: fire-proofing, emergency lighting, briefing

Boeing 747 – TWA Flight 800 (1996) – fuel tank design, inert fuel vapour, fire protection

Nimrod Crash (2006) – MOD organisational change – independent regulator & investigator

ACCIDENTS THAT CHANGED HOW WE CERTIFY AIRCRAFT – FROM SYSTEMS & PEOPLE

SQEP

Airbus A330 - Air France Flight 447 (2009) – pitot tubes; crew training & CRM

Boeing 737 Max - Lion Air Flight 610 (2018) & Ethiopian Airlines 302 (2019) – redundancy, anomaly detection and manual override

And because you can't control everything …

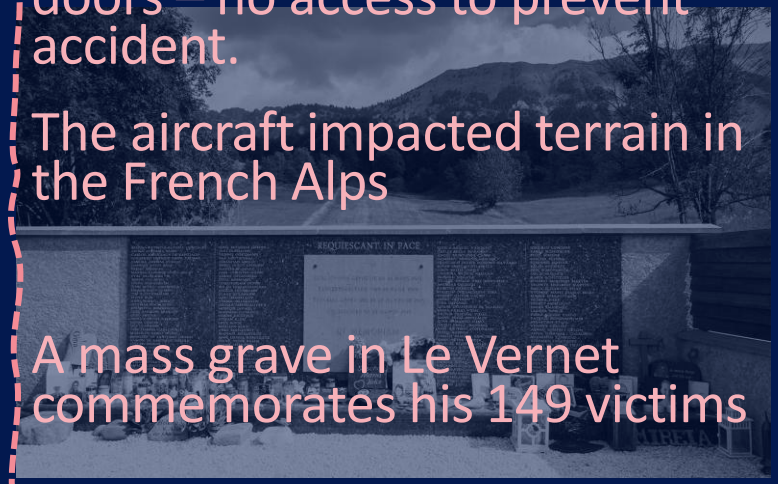
Germanwings Flight 9525 (2015) ….

Neither human error nor technical failure

Deliberate CFIT by pilot

Security requirements following 9/11 strengthened cockpit doors – no access to prevent accident.

The aircraft impacted terrain in the French Alps



A mass grave in Le Vernet commemorates his 149 victims

Accident – Chinook – Mull of Kintyre 1994

- Human error?
- Equipment & Environment:
  - Design, integration and testing
  - Reliability
  - Weather / conditions
- Individual:
  - Health
  - Stress
  - Capability
  - Capacity and Workload
- Organisation:
  - Resource & pressure
  - Working culture & environment
  - Training & supervision

Accident – Nimrod XV230 - 2006

SQEP

Accident - Hawk TMk1 – Sean Cunningham

SQEP

Technical Cause:

- Ejection seat component failure

Major Contributing Factors:

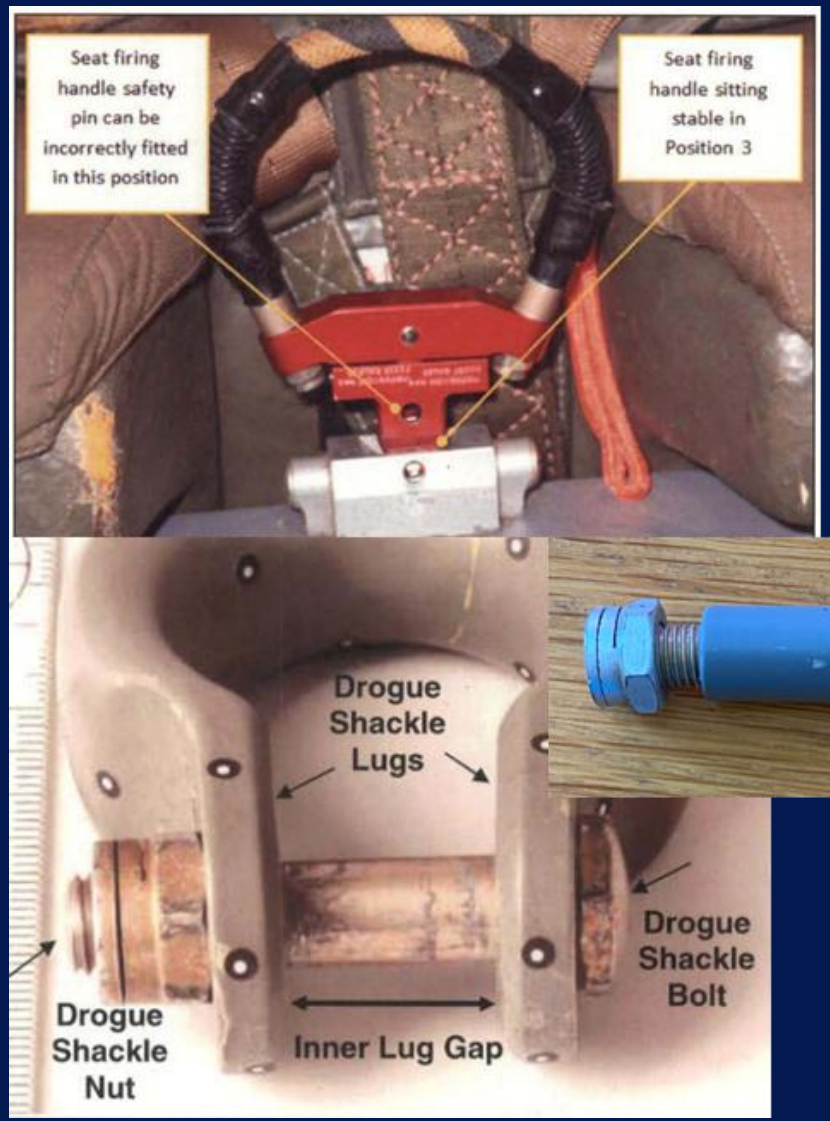
- Communication
- Culture
- Procedure
- Design of components
- Risk assessment

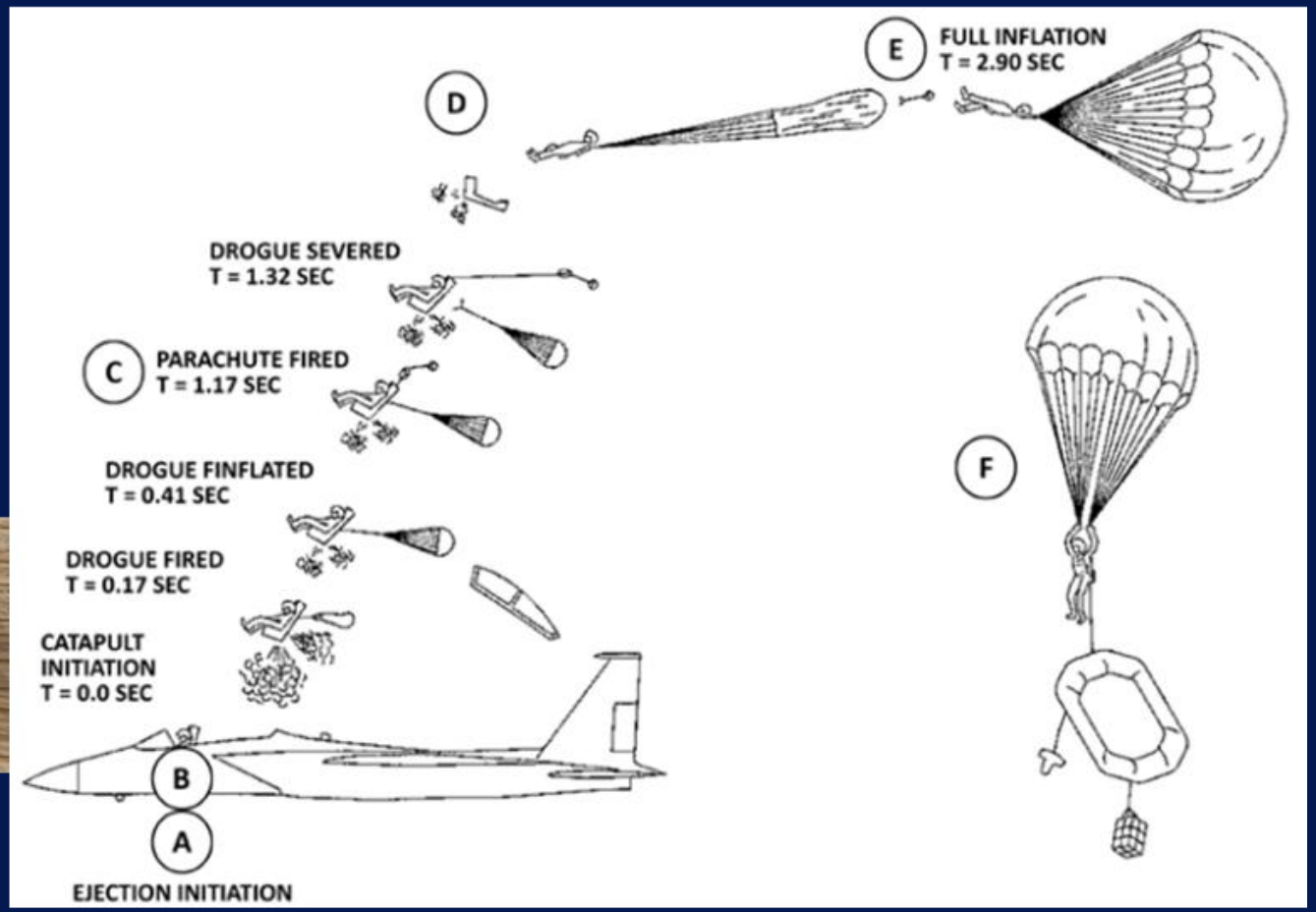
Ejector seat maker fined £1.1m over death of Red Arrows pilot

Sean Cunningham was ejected while performing pre-flight checks at RAF Scampton in 2011

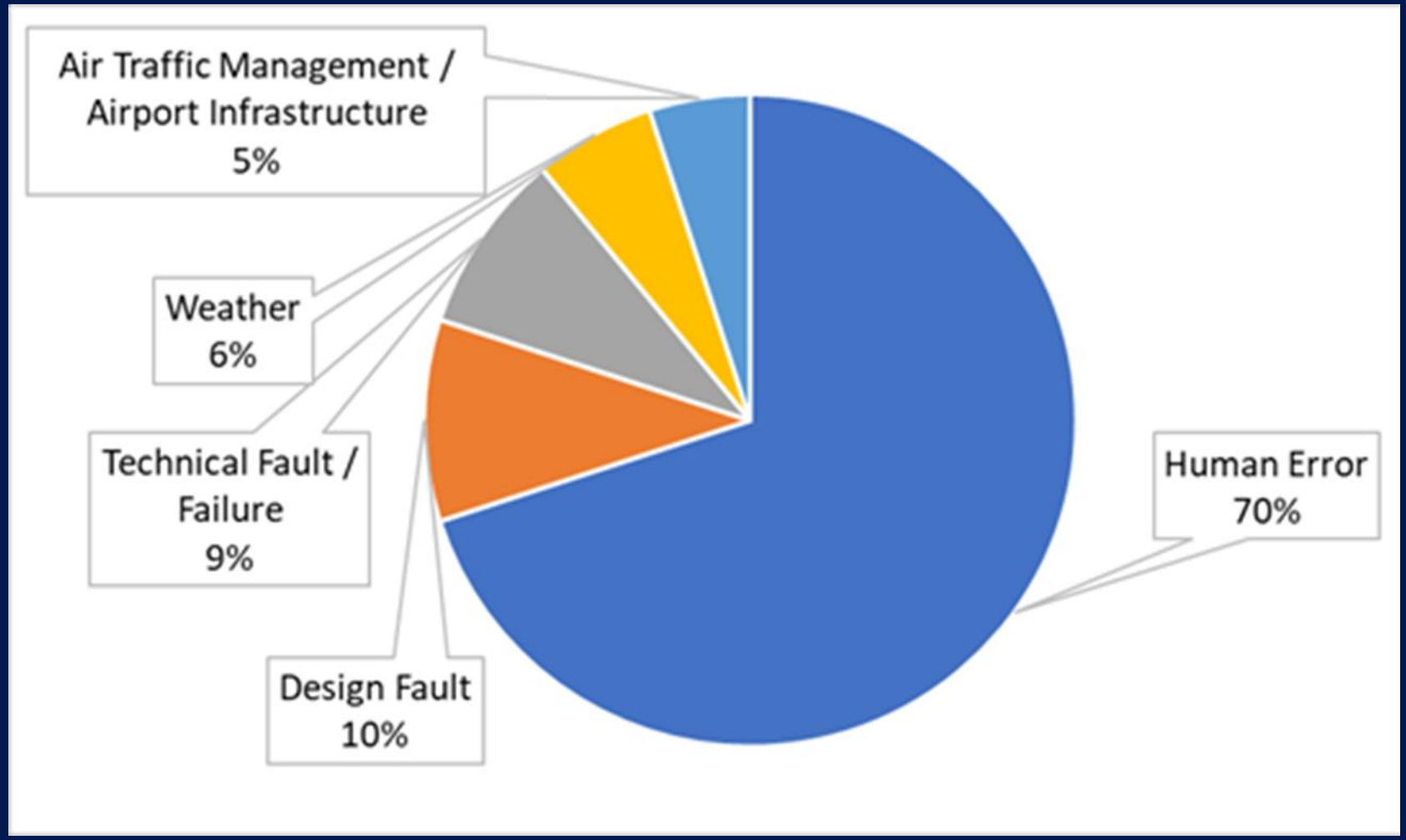
"Sean's death was not an accident. It was a preventable death waiting to happen and we don't believe it was an isolated incident. We acknowledge the fine issued to Martin-Baker today, a tiny percentage of its profits. No amount of money will bring our son back or relieve our pain."

The technical problem – but





Accident Causes



Human error was cited as a causal or contributory factor in 70% of aviation accidents, where the consequences of that error were severe. *(Gilbert, 2007)*

So what can we do … ?

SQEP

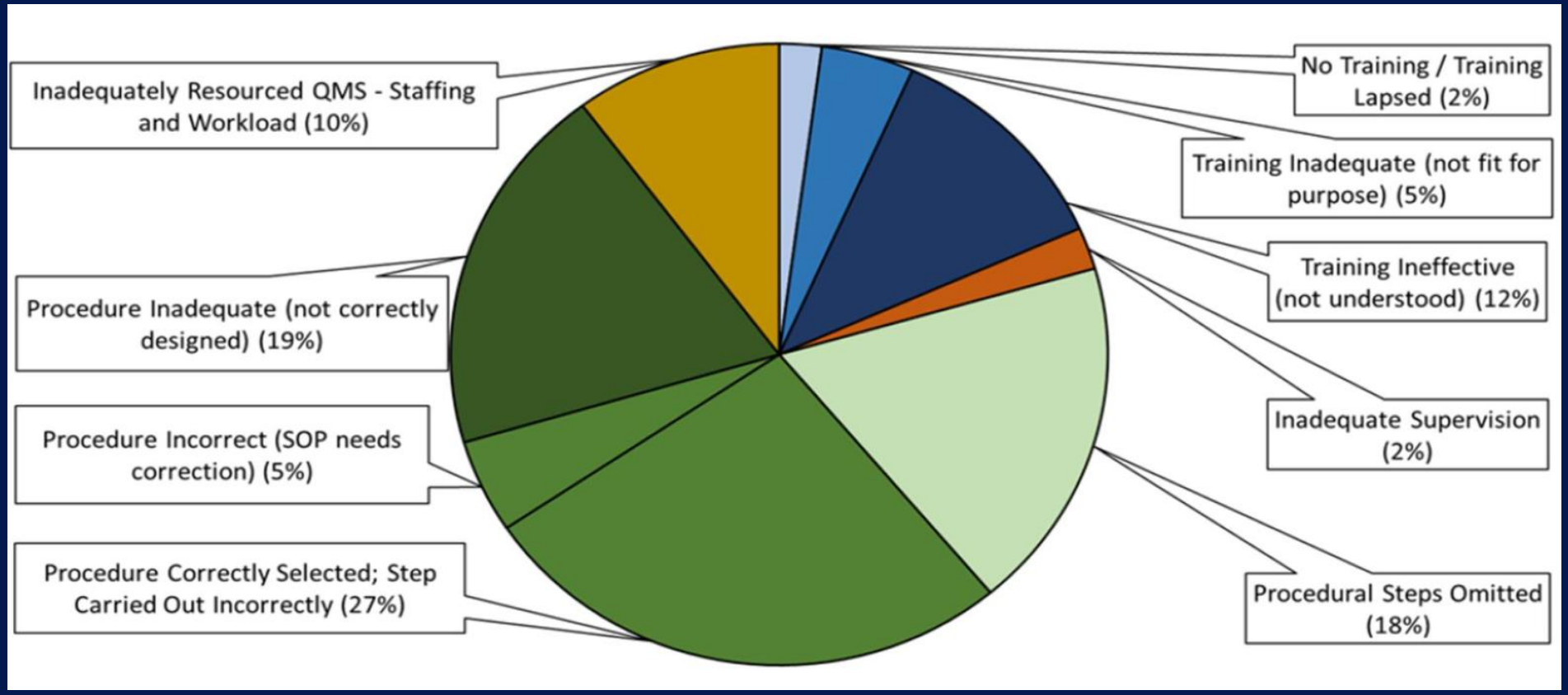
AWARENESS

PROCESSES

TRAINING

RESOURCE &

REWARD



MAKE IT EASIER TO:

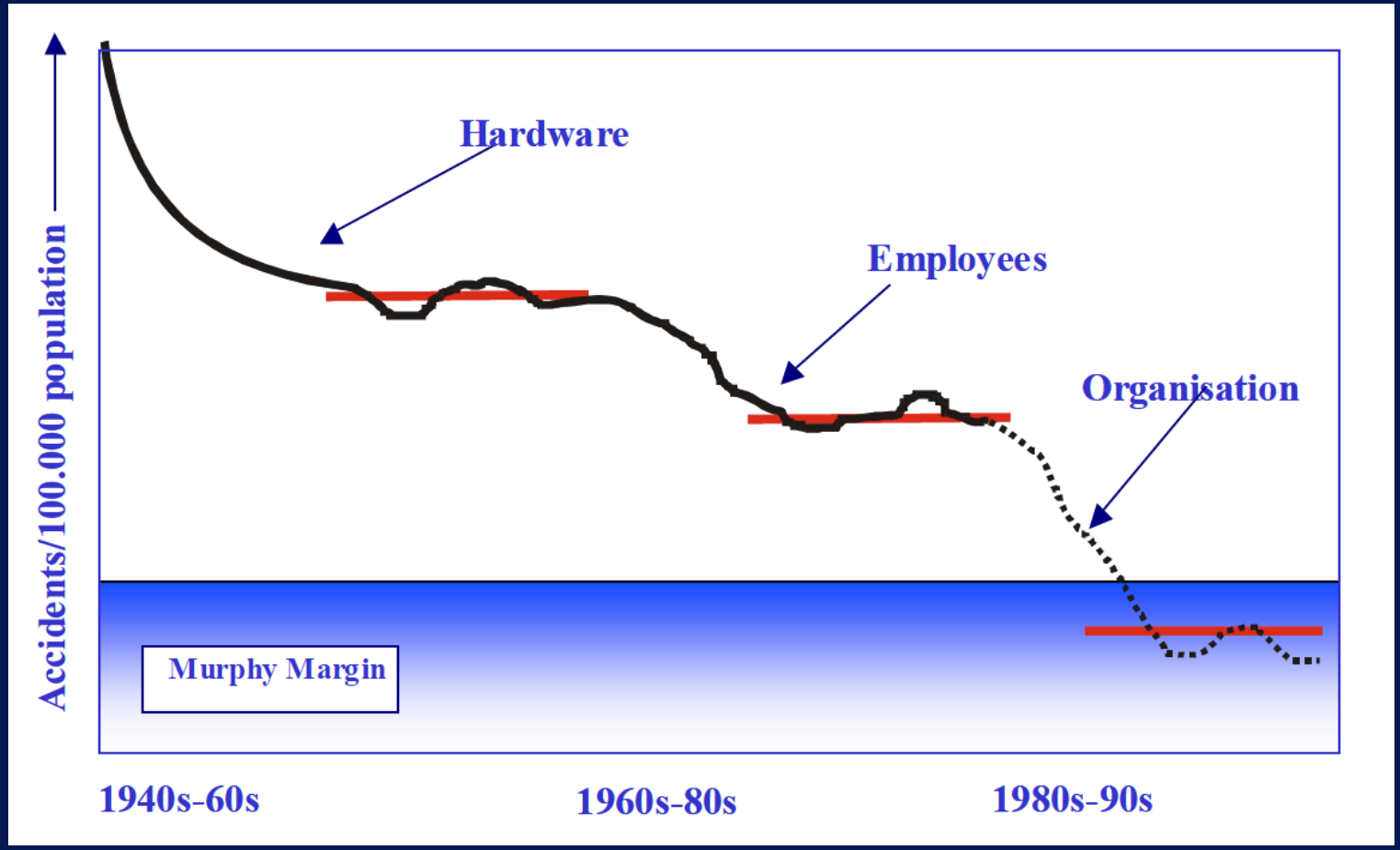
DO THE RIGHT THING – AND DO THINGS RIGHT

Accident Rate Reduction

SQEP

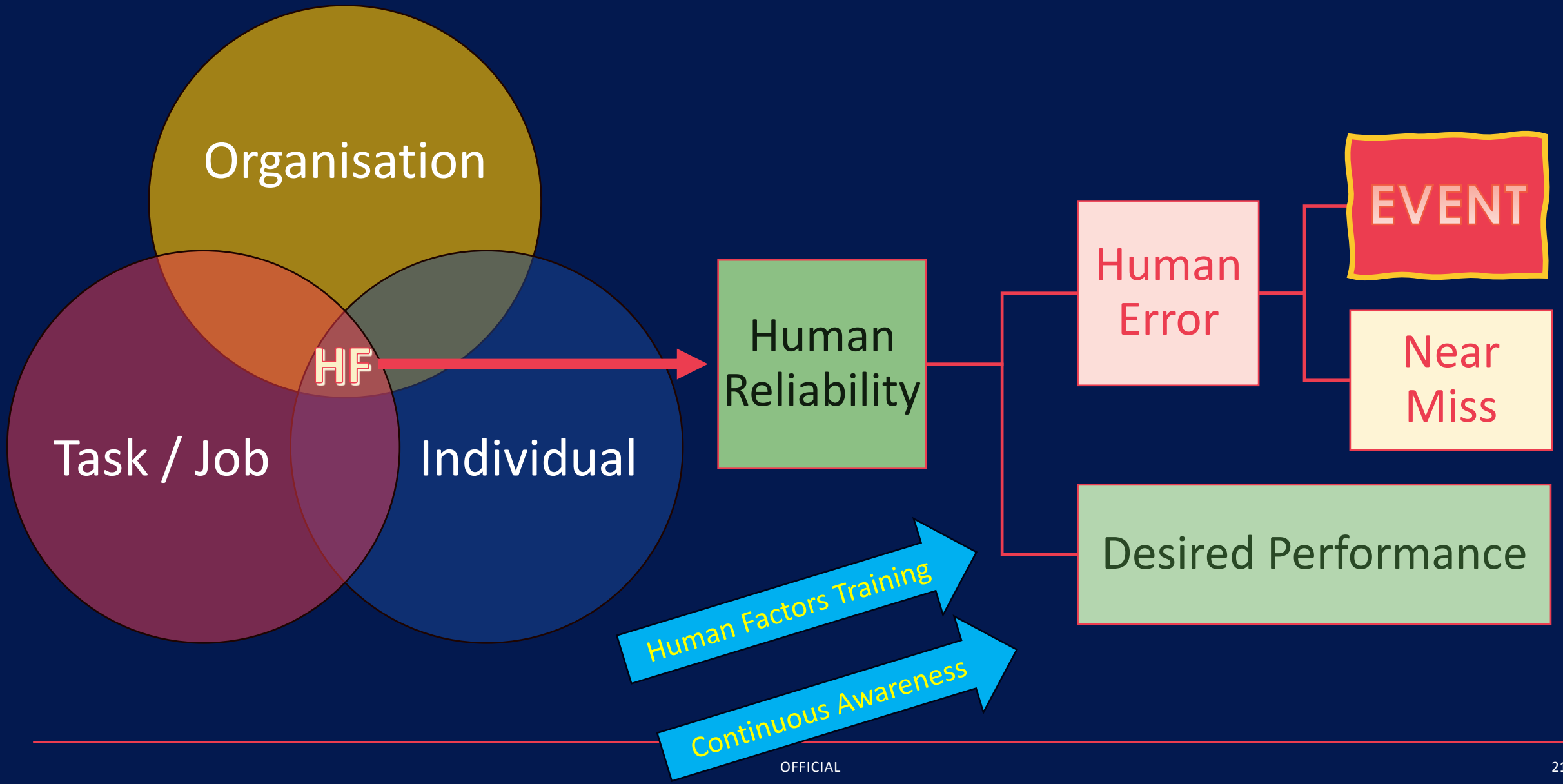
Investigation now focuses on organisational causes as well as technical faults and human error to prevent reoccurrence.

(UK HSE, 2002)

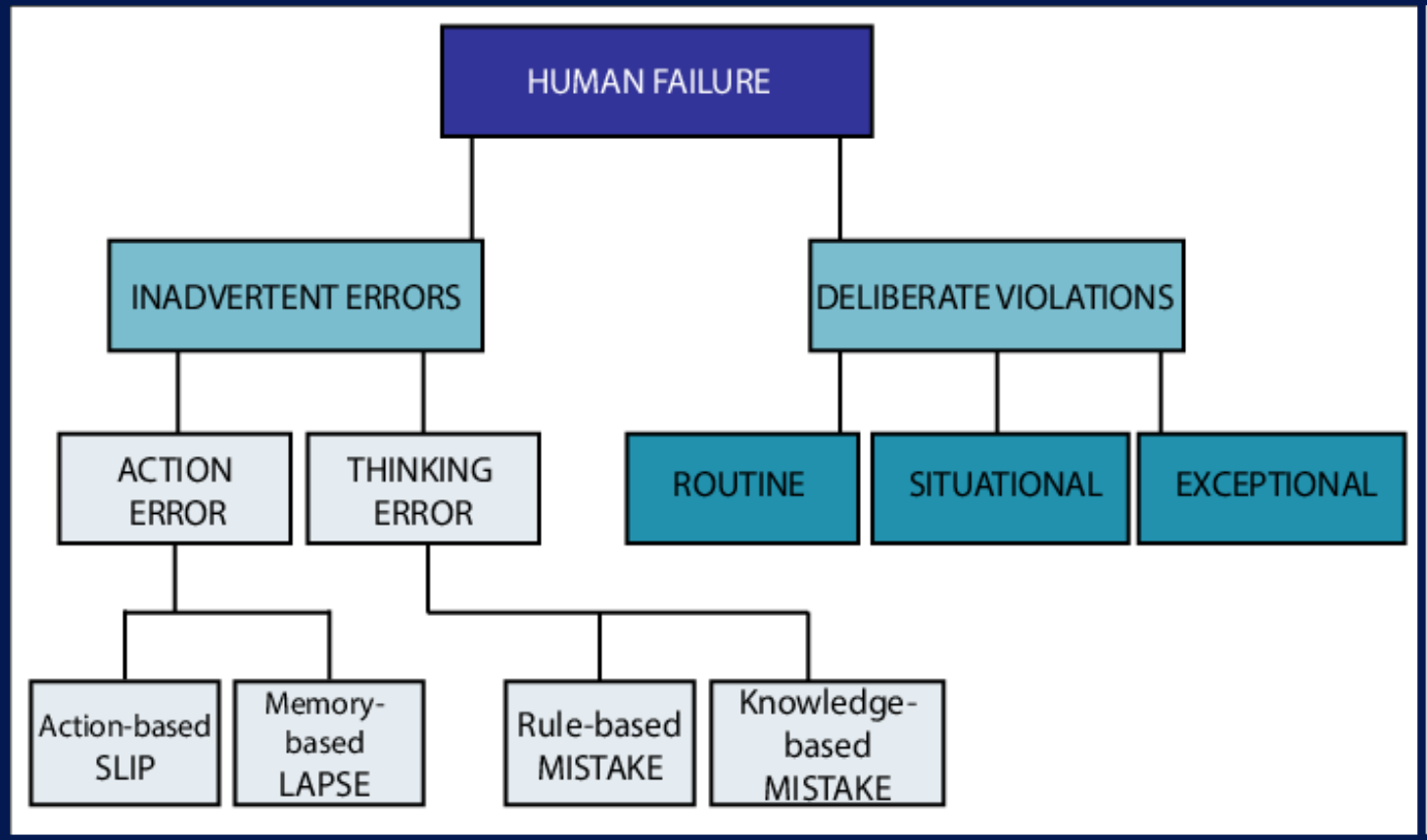


Human Performance

SQEP

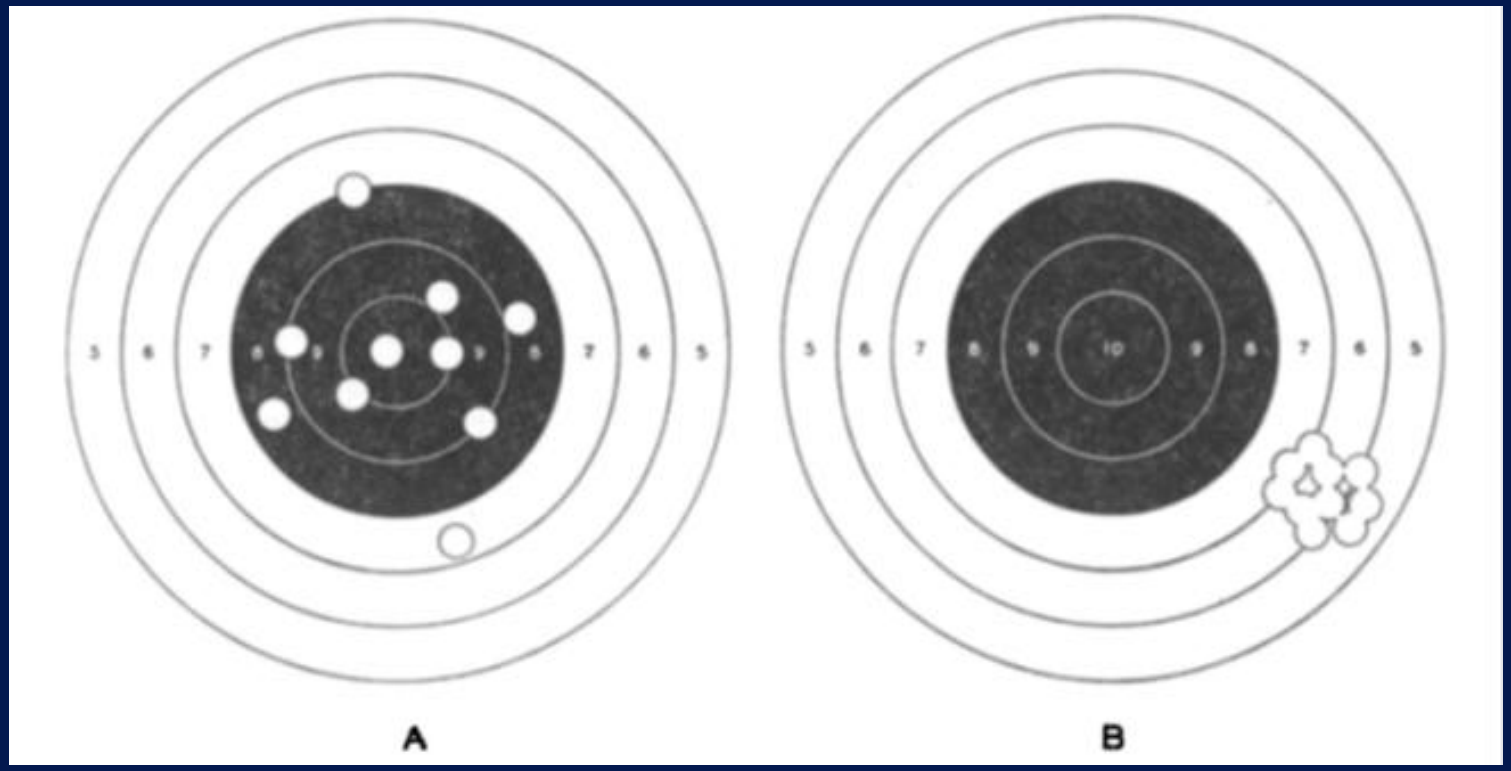


Human Failure Types



SLIP (comission)	Skill-based, familiar tasks that may occur if attention is diverted momentarily
LAPSE (omission)	Resulting action is not intended: 'not doing what you were meant to do'
RULE-BASED MISTAKE	Errors of judgement: mental processes linked to planning, information gathering, communication, etc.
KNOWLEDGE-BASED MISTAKE	Action as planned, but 'doing the wrong thing believing it to be right'
ROUTINE	Deliberate deviations from rules (violations)
SITUATIONAL	Knowingly fail to follow procedures, to save time or effort
EXCEPTIONAL	Well-meaning but misguided action to 'get the job done'

Who is the Best Shot?



The Trouble With Humans…

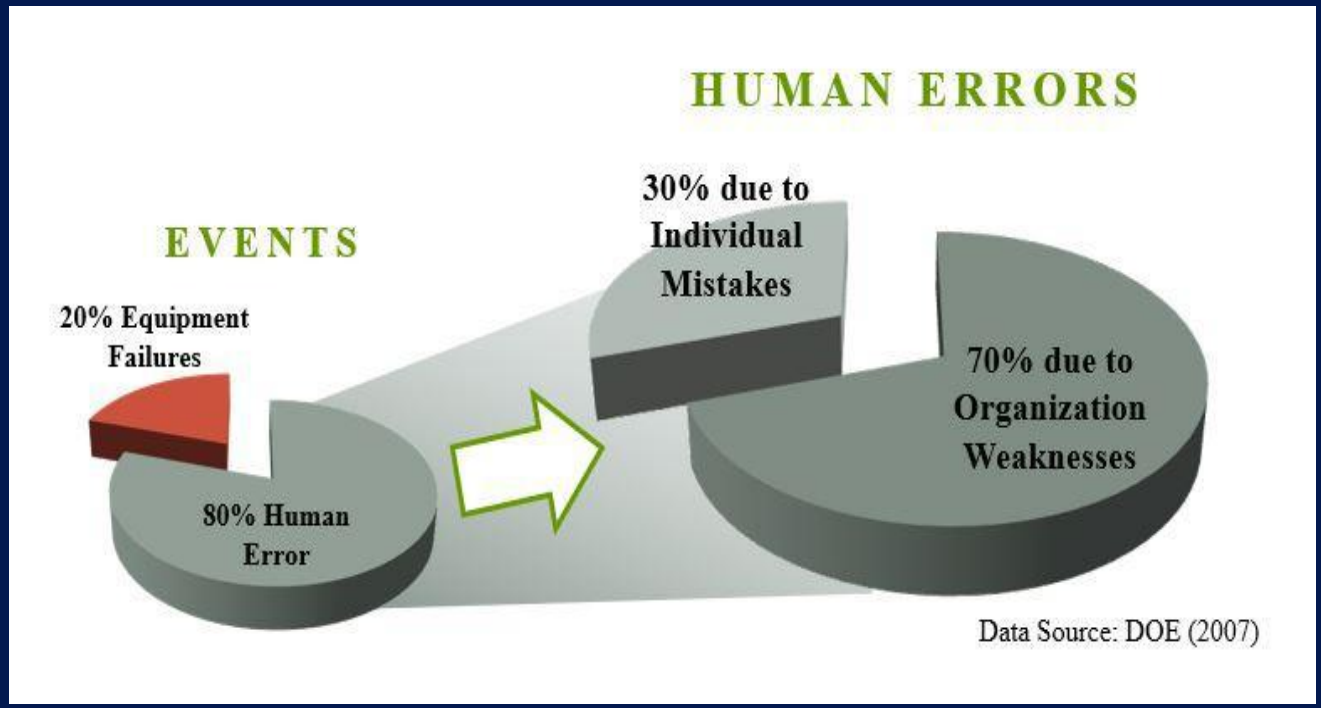
SQEP

What could possibly go wrong?

So, What Do We Know?

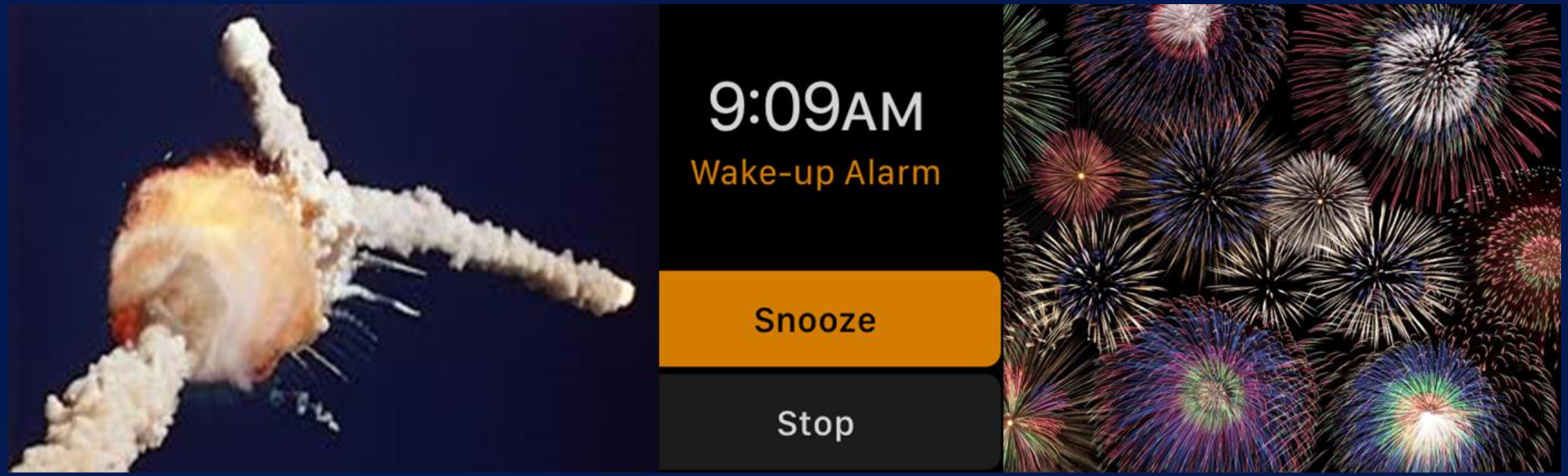
SQEP

- Not all human errors are a problem
- Human behaviour ranges between heroic saves and massive stupidity
- Most people go to work intending to do a good job
- Human error has been cited as the cause of accidents in every industry and has been shown to cost millions



Consequences of Error – Learn To Tell The Difference

SQEP



DISASTER TRIVIAL FABULOUS

Human Error Rate

SQEP

Cognitive: $1 \times 10^{-1} \rightarrow 1 \times 10^{-5}$

Procedural: $1 \times 10^{-2} \rightarrow 1 \times 10^{-6}$

EXPERIENCE · FREQUENCY

COMPLEXITY · CORRECTION

ENVIRONMENT · STRESS

SIMPLIFY · PRACTICE

INFORM · CHECK

Image: Steigler & Tung 2014

Looking for the Real Causes

Maybe you're not incompetent or lazy, but you're missing deadlines because:

- You agree to actions regardless of your workload (pressure / can-do)
- You're having trouble concentrating (illness / stress / distraction)

The secret to efficiency might be having the courage to say, "No"

Results of poor design choices …

Conventions - issues

It’s not enough to have a good design; equipment within an industry has to be consistent to prevent error.

Here is an example from anaesthesia – spot the difference!

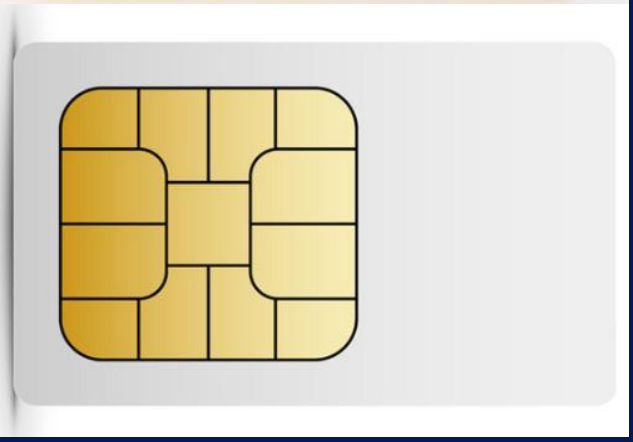
- O2 instead of air – oxygen toxicity - damage
- Air instead of O2 – hypoxia - death

IT COULD BE WORSE …

The N2O is in the same place – so you should at least get the planned level of anaesthesia – but you would not get the right amount of oxygen if air was selected (50:50)

Poor product design

SQEP

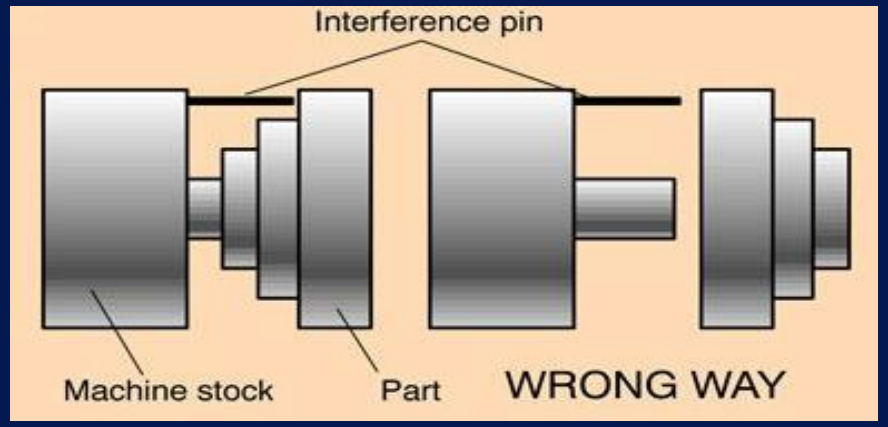


Human-Centred Design – the HUD

- Critical information is provided to operators while preserving their Situational Awareness
- Green is used for the display because it's easy for humans to see
- The human retina has a peak sensitivity around 555 nanometers – yellowish green – easiest seen!

Human-Centred Design – Poka Yoke in action

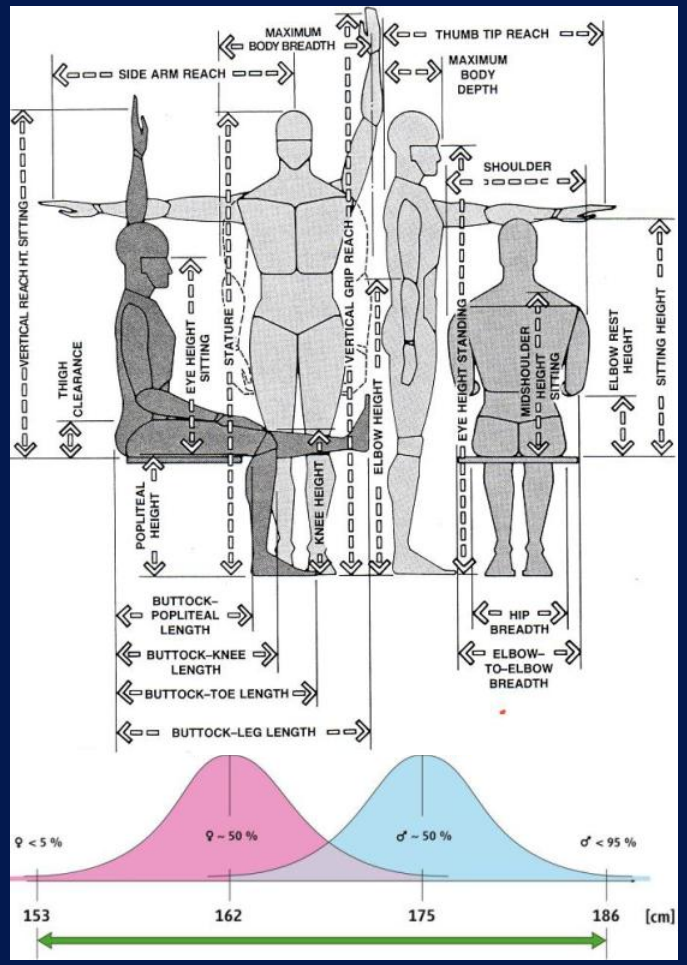
SQEP



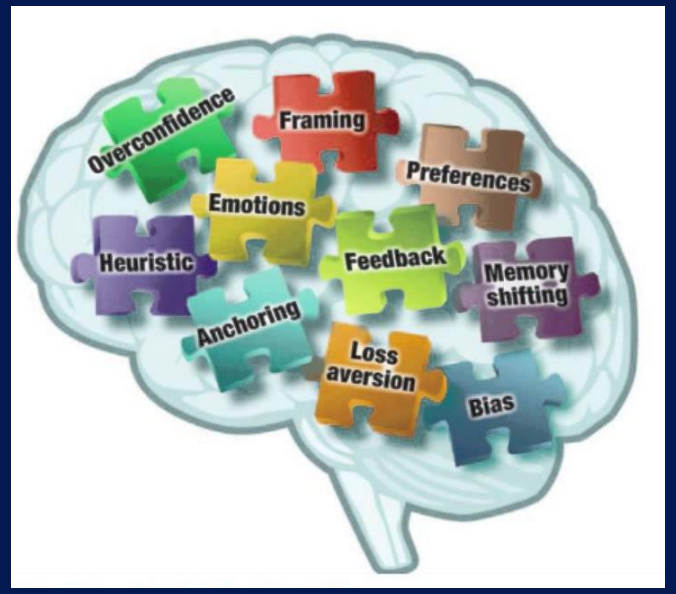
Requirements

SQEP

ERGONOMIC - PHYSICAL



HUMAN - PSYCHOLOGICAL



- Sensory - colour / sound / position
- Capacity – workload / automation / alerts / communication

ORGANISATION

Including: IMS / Governance / KPIs

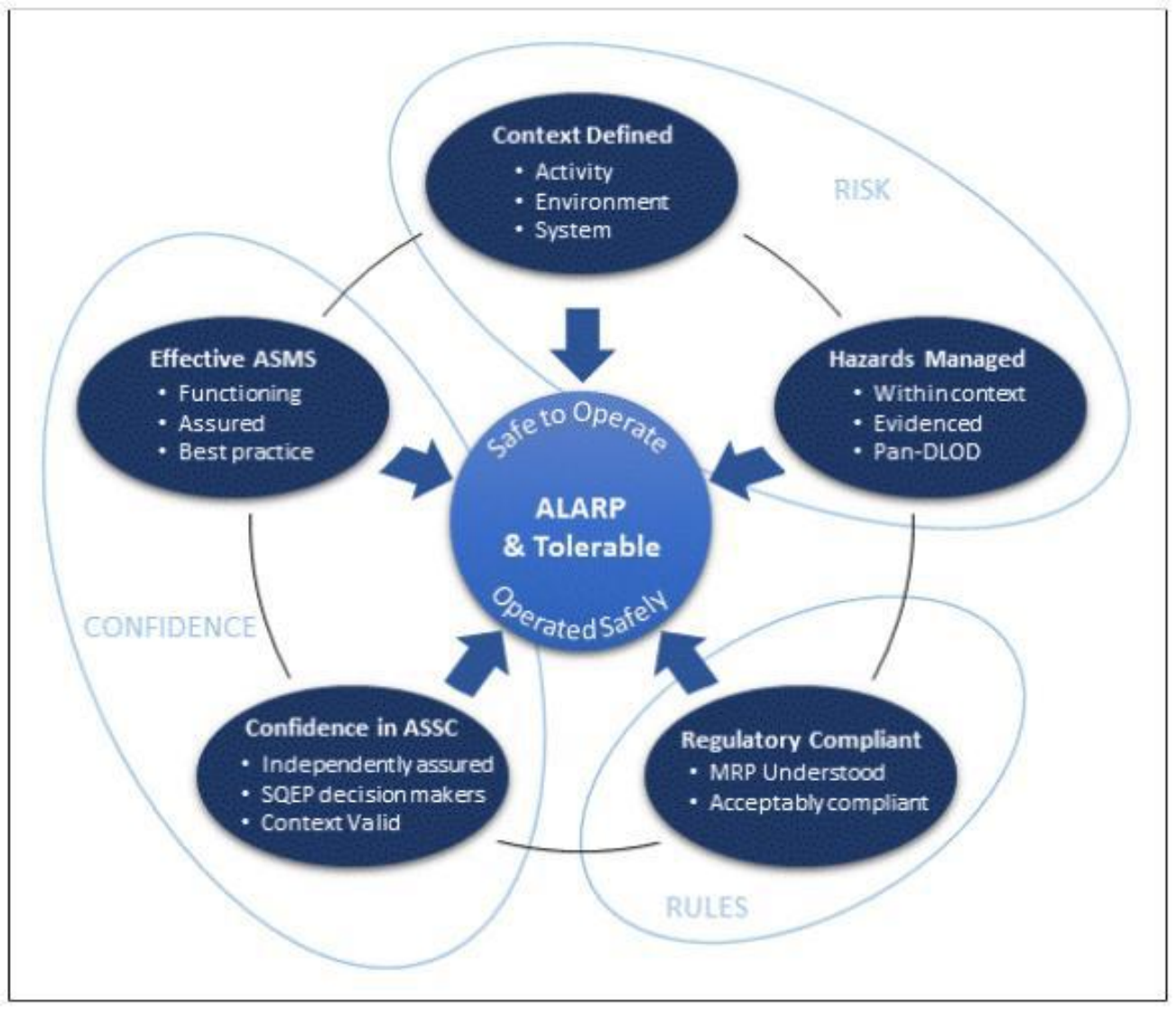
Sufficient & suitable …

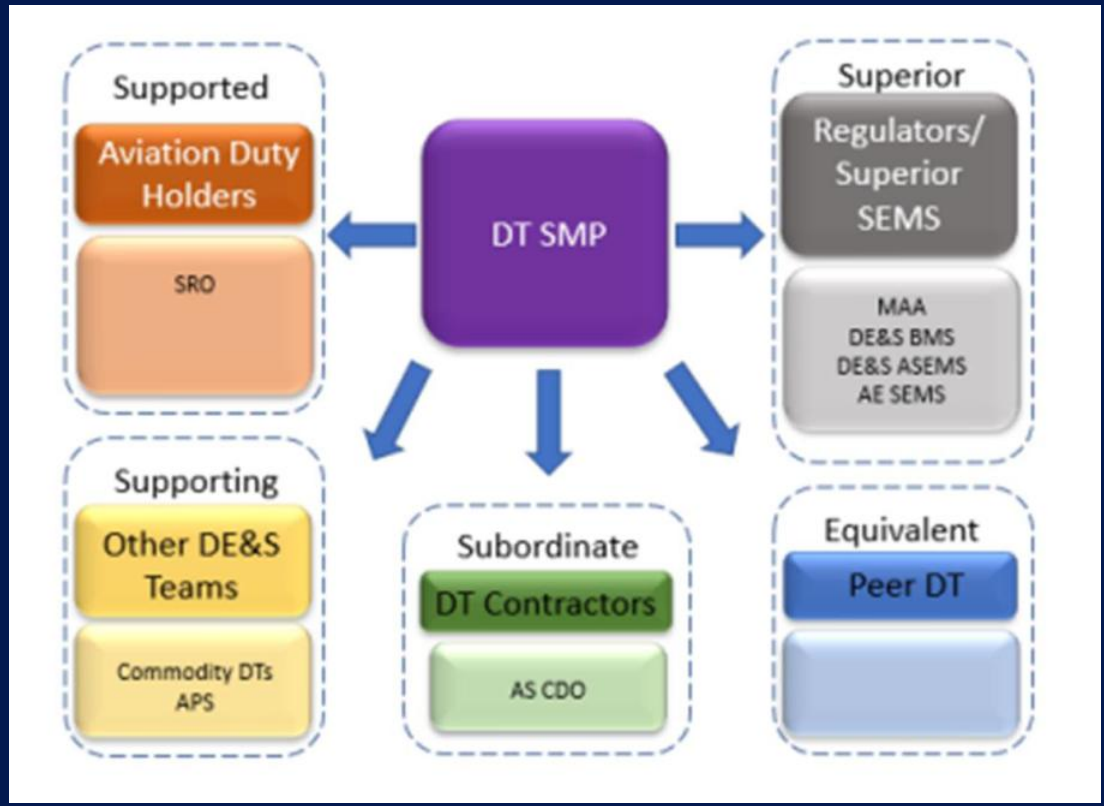
- People
- Accommodation & Equipment
- Tools & Spares

MEANWHILE, BACK AT THE AIRCRAFT ….

Safety Overview – the Air System Safety Case Model and Safety Management Plan

SQEP





What is a Safety Case and What's it for ?

SQEP

The primary purpose of a Safety Case is to present the argument that a system can be considered acceptably safe (in a given context).

It can also be used to support mitigation strategies/tolerability assessment by demonstrating that the appropriate level of Hazard and Risk Assessment (HARA) has been undertaken.

A Safety Case generally consists of two interdependent parts:

1. An argument
2. A body of supporting evidence

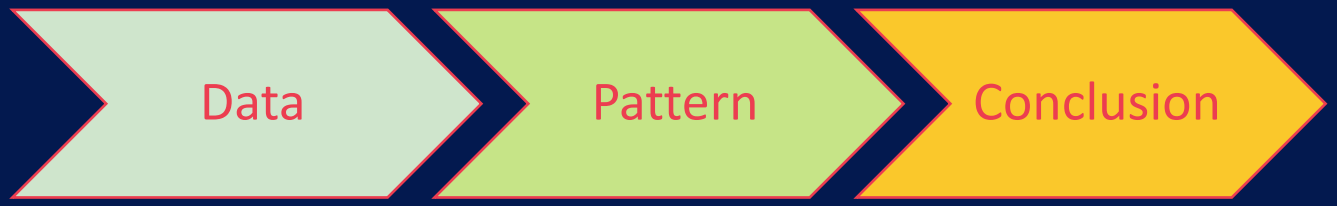
"...A structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment."

THE ARGUMENT

SQEP

An inductive argument is one where we cannot state categorically that a premise is true, and we therefore have to talk about the *likelihood* of the premise being true.

Inductive arguments are generally formed this way:



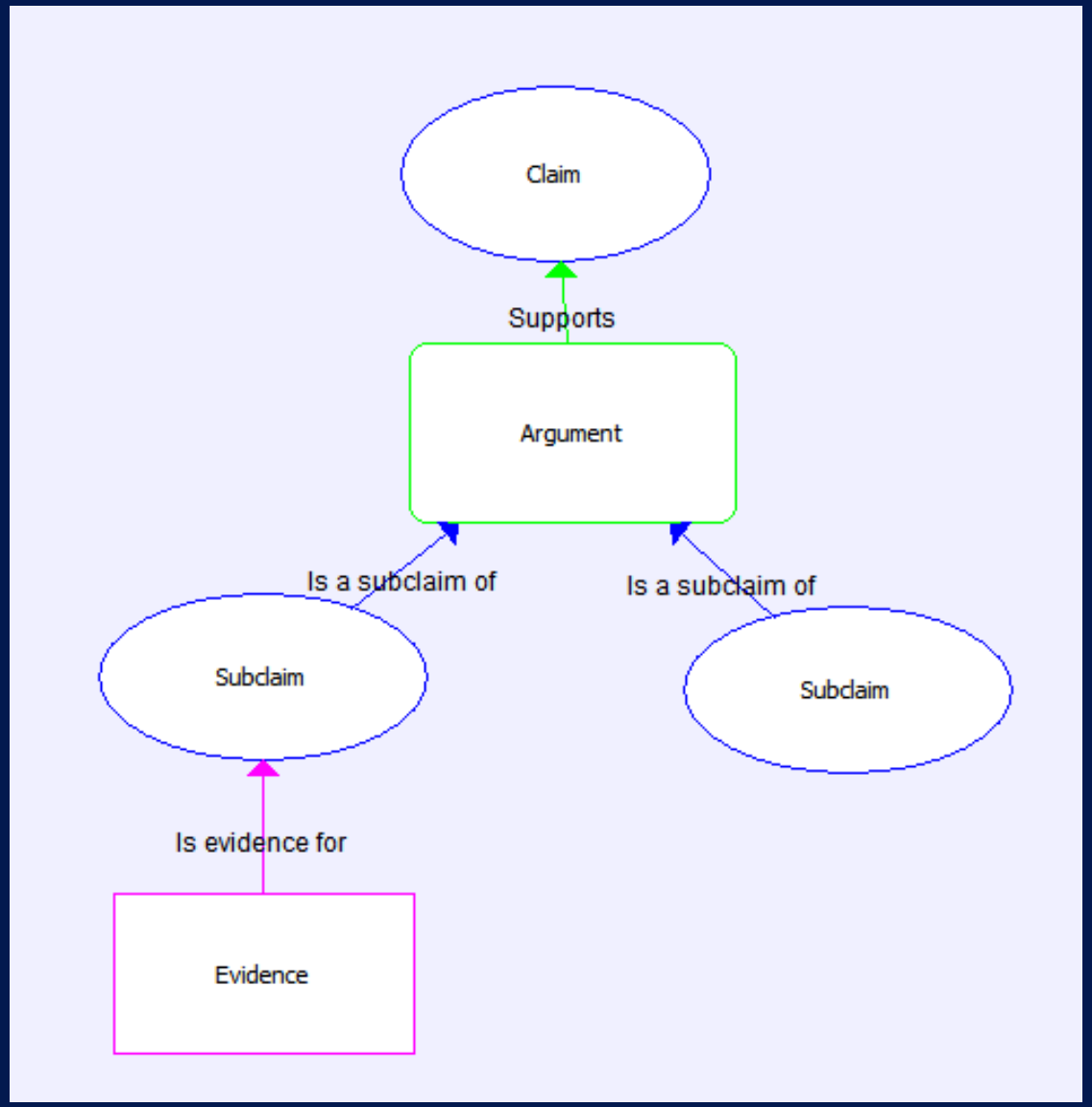
An example might be:

“Most dogs have four legs. Winston is a dog, therefore Winston is likely to have four legs”

THE LANGUAGE USED IN SAFETY ARGUMENTS IS ALMOST NEVER ABSOLUTE

SAFETY CASE – GRAPHICAL REPRESENTATION - CLAIMS ARGUMENT EVIDENCE

SQEP



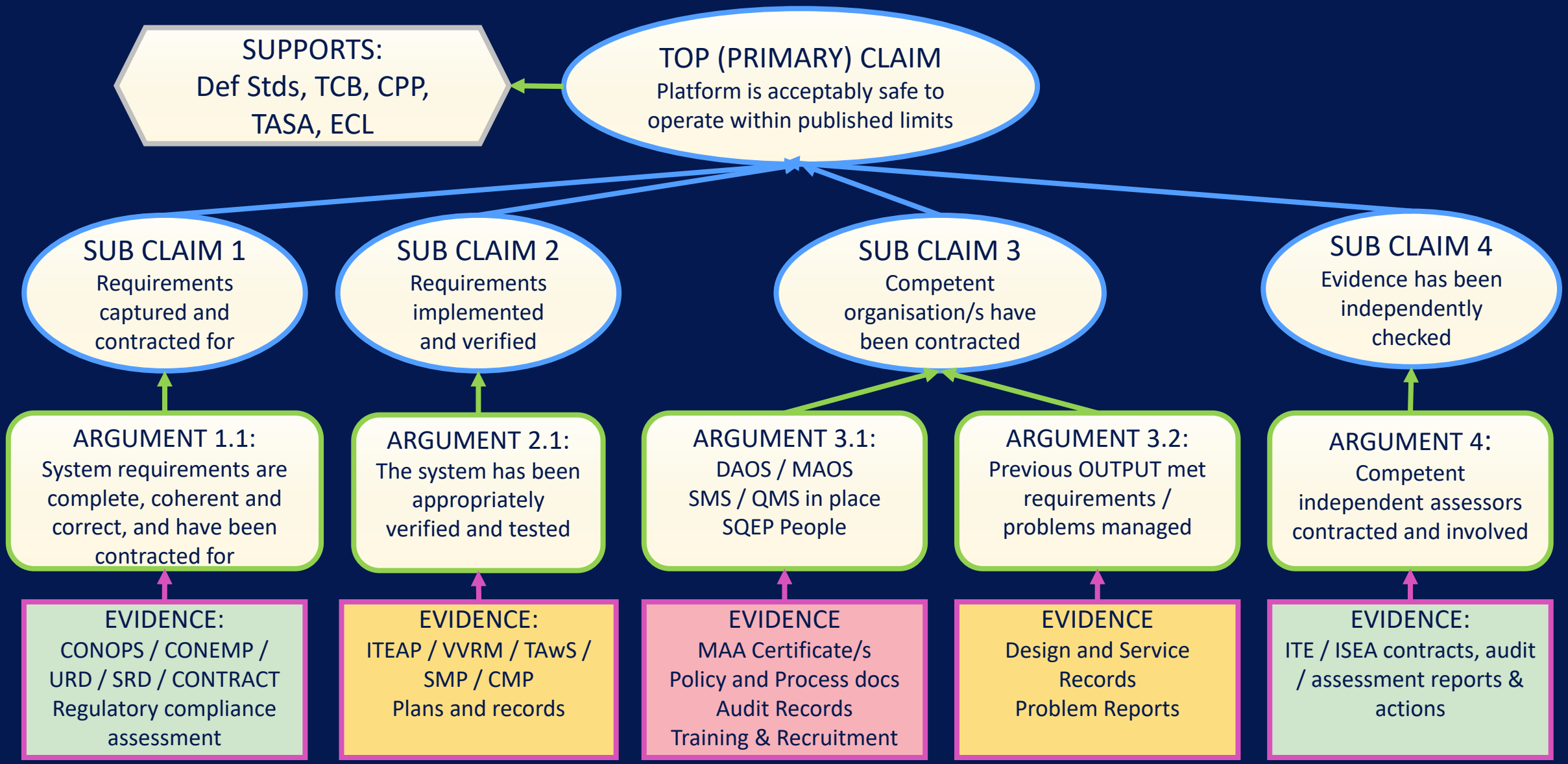
Claim – A true or false statement about a property of an object (e.g. '…is acceptably safe'

Argument – a rule that provides the link between what we know to be true (evidence) and the claim being investigated

Evidence – an artefact which establishes facts that can be trusted. Leads directly to the claim

SAFETY CASE EXAMPLE

SQEP



COMMON SAFETY CASE ISSUES

SQEP

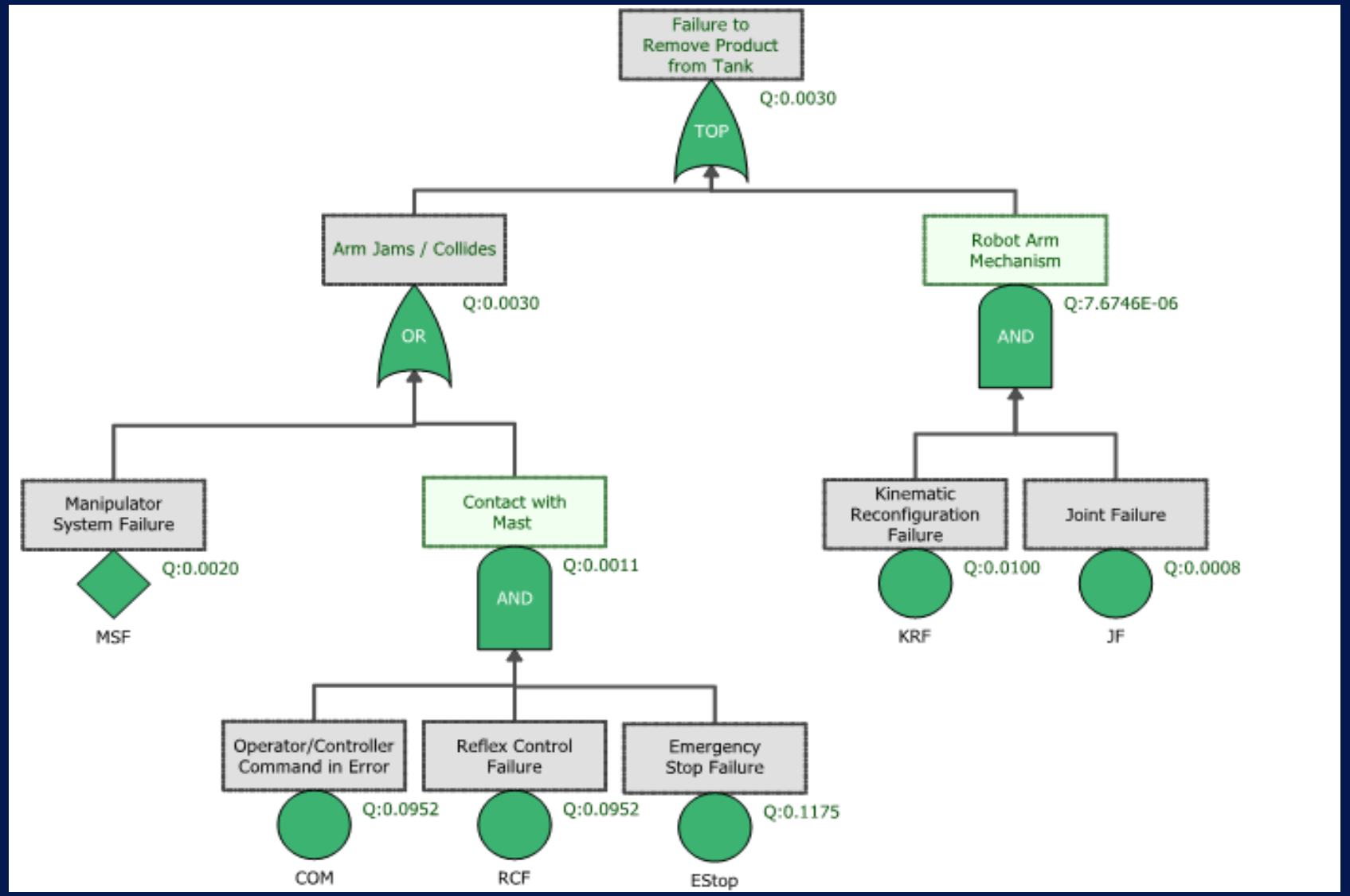
Not all Safety Cases are good. Problems include:

- They contain assertions rather than reasoned argument.
- There are unjustified and implicit assumptions
- Some major Hazards have not been identified and are therefore never studied
- There is a poor treatment of data with uncertain pedigree, and the effect this uncertainty has on subsequent assessments
- They don't deal well with Human Factors
- They don't deal well with software
- There is inadequate involvement of senior management
- Ownership of the Safety Case is not always clear

The work we do aims to avoid these issues – getting to a good ASSC is a significant body of work

Fault Tree Analysis

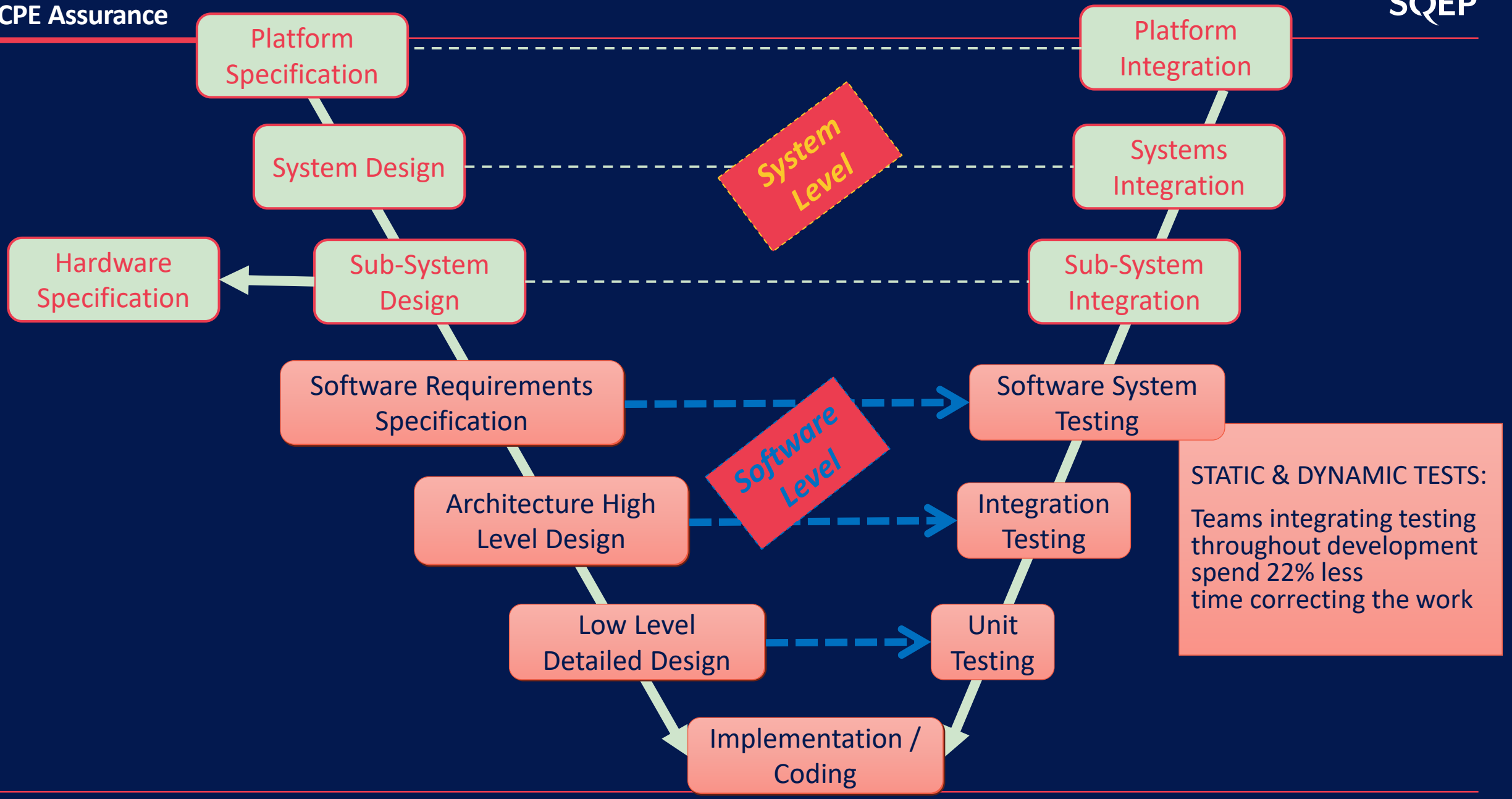
SQEP



- FTA is used to predict critical failures and verify their prevention / mitigation of
- Breaks down a top event (incident / accident) into contributing factors
- Can pinpoint root causes to identify effective mitigations

CPE Assurance

SQEP



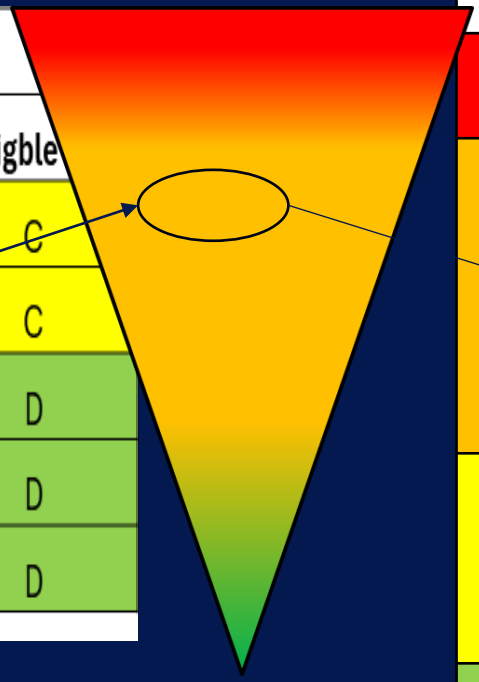
STATIC & DYNAMIC TESTS:

Teams integrating testing throughout development spend 22% less time correcting the work

RISK CRITERIA

SQEP

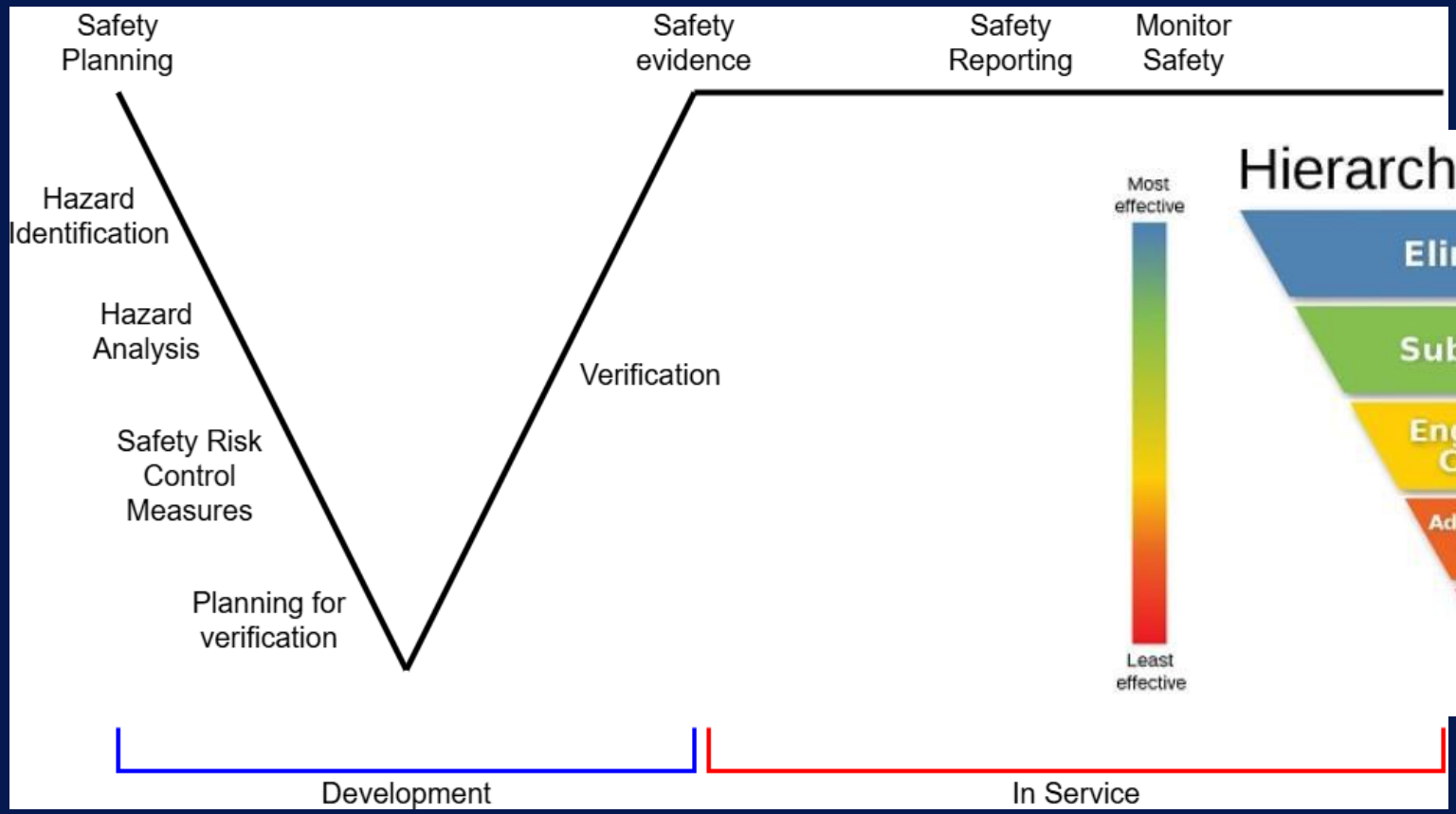
Likelihood	Severity: Catastrophic	Critical	Major	Minor	Negligble
Frequent	A	A	A	B	C
Probable	A	A	B	B	C
Occasional	A	B	B	C	D
Remote	B	C	C	D	D
Improbable	C	D	D	D	D

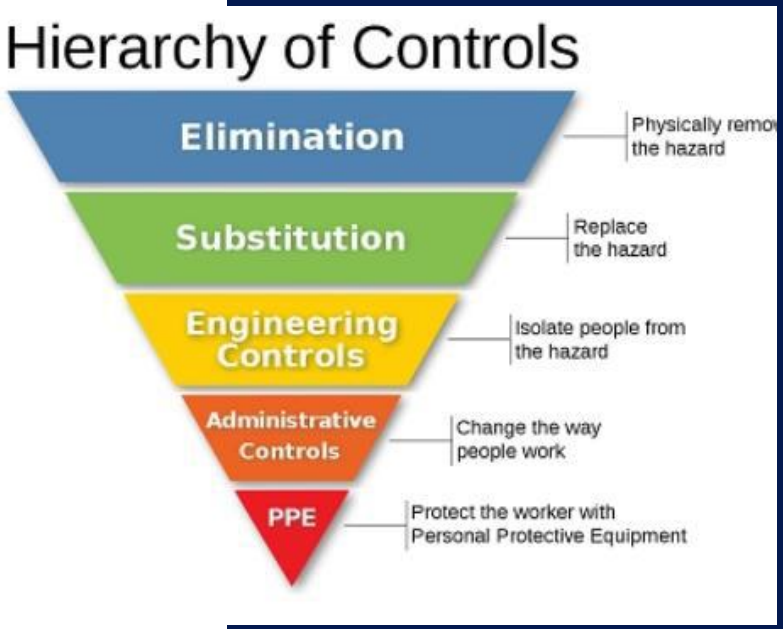


Risk Assessment Definition	
A	Work shall not proceed or facility shall not be used
B	Shall only be accepted when risk reduction is impracticable and with the agreement of the Authority as appropriate
C	Acceptable with adequate control and with the agreement of the Authority
D	Acceptable with agreement of the Authority

HAZARD MANAGEMENT

SQEP





Identification → Analysis → Mitigation Planning → Tracking & Monitoring → Closure

BOWTIE - ECL Format – Functional Level

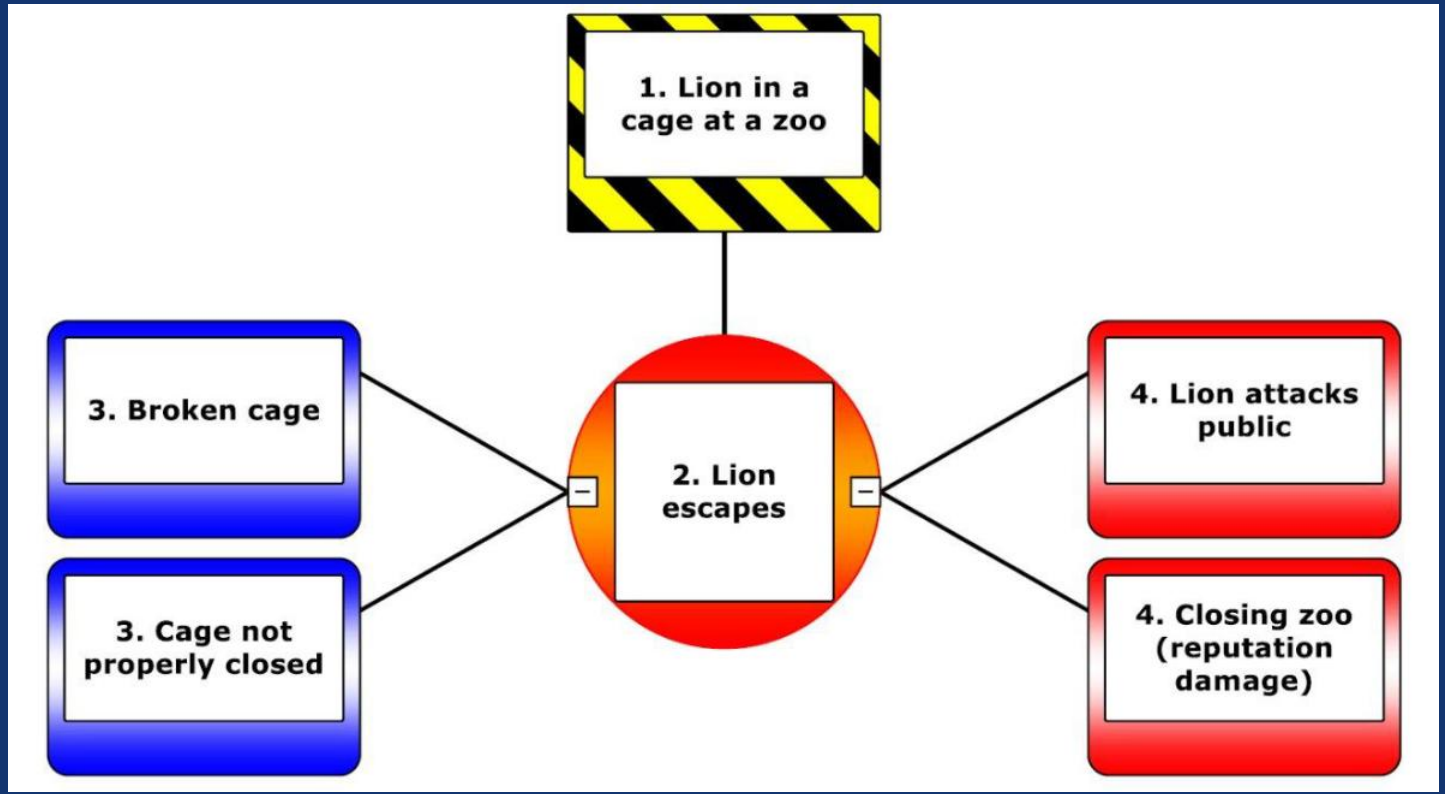
SQEP

- ✓ Visual risk management tool
- ✓ Based on barrier thinking

So … easy to understand if done right

BUT …

- ➢ Must pitch at right level
- ➢ Needs consistent taxonomy
- ➢ Linear causation model limits complexity
- ➢ Does not address Haz ID

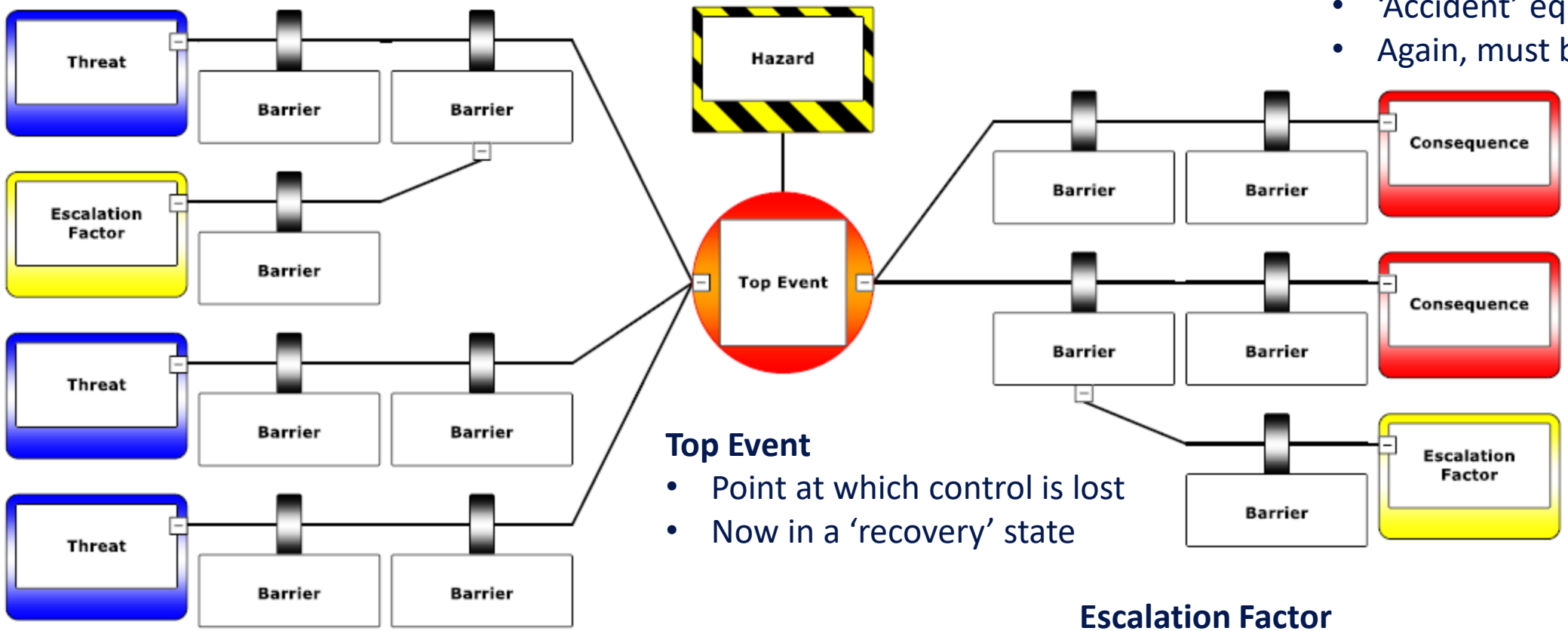


Bow-tie Terminology

Threat
- Cause of Top Event (1-many relationship)
- Direct cause, must be specific

Hazard
- Part of normal business
- Formulated in controlled state

Consequences
- ‘Accident’ equivalent
- Again, must be specific



Top Event
- Point at which control is lost
- Now in a ‘recovery’ state

Barrier
- …aka ‘Control’
- Physical / non-physical in nature

Escalation Factor
- Reduces Barrier effectiveness
- Not a direct cause

Information Routes – Risk Transfer

SQEP

Boeing / OEMs / USG

- SSHA – ETs & Recommendations
- USG modifications

DT

- Certification Non-Compliance (Case 2b & 3)
- Safety Assessment Outcomes with EC impact
- Novel items with EC impact

In-Service

- Operational envelope
- Service experience / occurrences
- Maintenance and reliability data

DT Safety

- ECL
- ECID

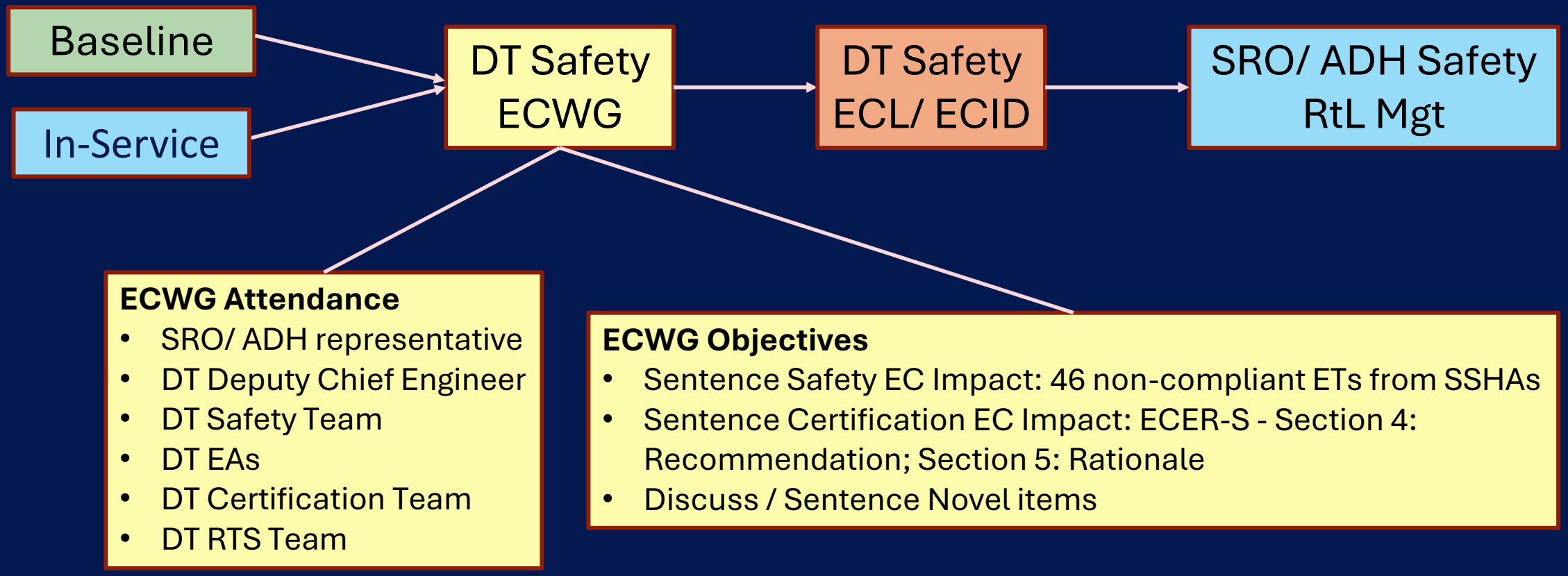
ECWG

SRO/ ADH

- SRO/ ADH RtL Mgt
- SRO / ODH Agreement

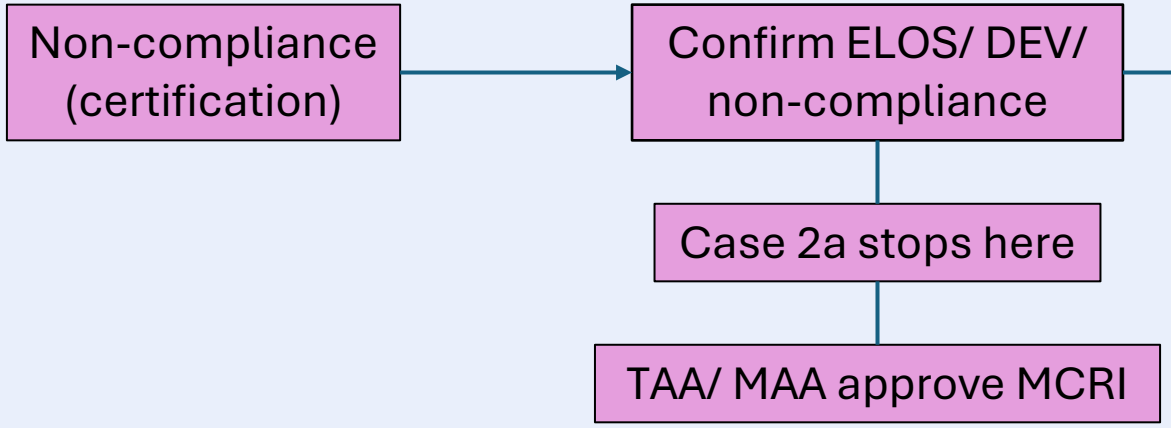
Equipment Contribution to Risk to Life

SQEP

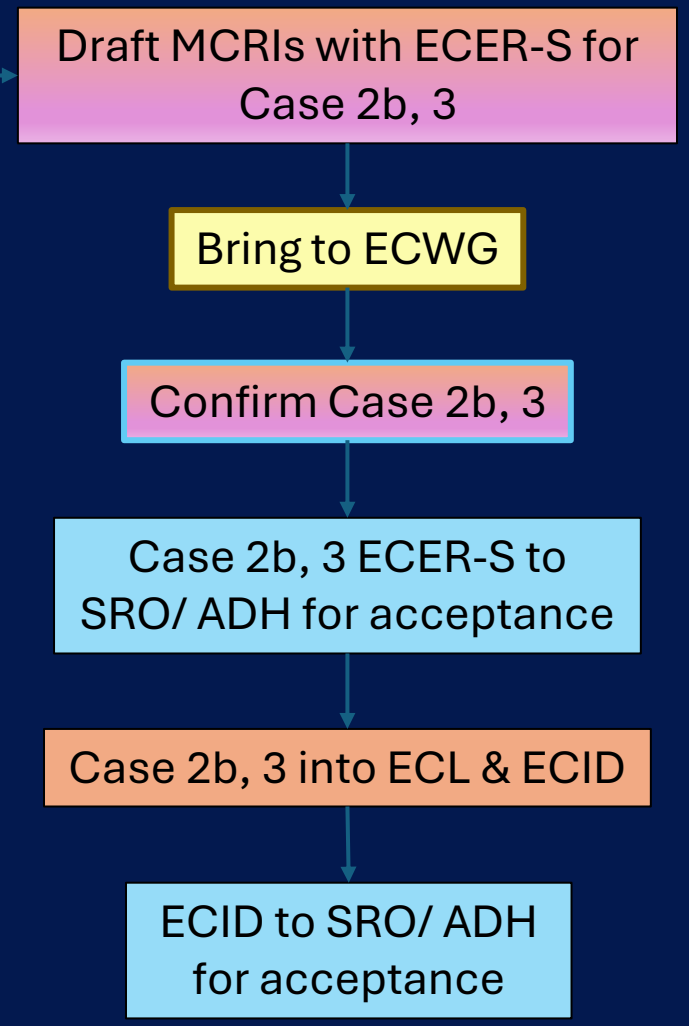


Process Example – Certification Outcomes

SQEP



Case	Initial State	Mitigation	Final State	Comments
1	Compliant	Not Required	N/A	
2a	Non-Compliant	**Yes** (**within** Eqpt DLoD)	Compliant ►(ELOS / DEV)◄	Within TAA's AoR (ie Equipment)
2b	Non-Compliant	**Yes** (**outside** Eqpt DLoD)	Compliant ►(ELOS / DEV)◄	ADH agreement for operating mitigation
3	Non-Compliant	None	Non-Compliant	Residual ECtRtL requires ADH accept



THE OUTCOME?

SQEP

A proportionate and pragmatic assessment of the system

A comprehensive and coherent transfer of risk

An enhanced capability

And Remember…

SQEP

“Insanity is doing the same thing over and over again and expecting different results.”

Albert Einstein (1879-1955)