

STPA Adoption in a Large Defence Organisation

Strategy, Challenges, and Unexpected Value

Joe Poole

BAE Systems Submarines

London, UK

MIT STAMP Workshop — 25 March 2026

Disclaimer

The views expressed are those solely of the Author/Presenter.

All information is designated as NOT CLASSIFIED with respect to the UK Government Security Classifications system.

18 months into STPA adoption at BAE Systems Submarines

We have no formal STPA outputs.

It's been one of the most valuable things we've done.

Context - Stakeholders



End User

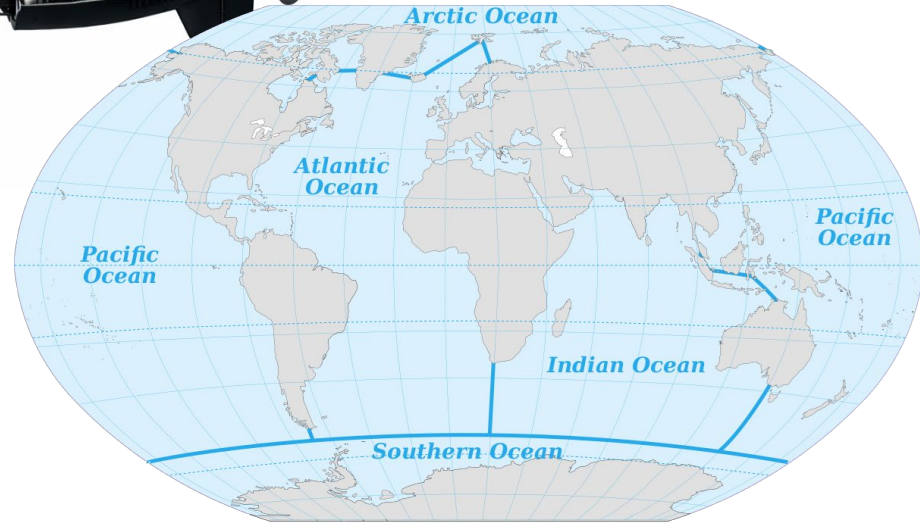


Submarine
Delivery Agency

BAE SYSTEMS



Context - System



Problem: Our analysis toolbox has limits

'Traditional methods' help in traditional context

Increased complexity changing the context

Tool limits being exposed

Need: Tools for integrated system interrogation



Goal: equip the organisation to use STAMP-based methods on appropriate challenges; increase our toolbox capability.

The risks and challenges

Goal: equip the organisation to use STAMP-based methods on appropriate challenges

Systems Engineering journey

New working practices, new people to the domain

Complex delivery environment

Large and distributed design effort

Long road ahead

Multi-decade programme

New brand fragility

One poor application poisons the well

Steep learning curve

Handbook and materials are helpful primers

Security constraints

Information classification limits external sharing

The strategy

WORK STREAMS

- 1 Training & Awareness**
Objective: Build internal capability
- 2 Case Study Development**
Objective: Validate the knowledge on representative problems
- 3 Method Integration**
Objective: Integrate STPA into the programme safety management system

1

Training & Awareness

Objective: Build internal capability

APPROACH:

- Procured expert support
- Developed a course:
 - Targeted safety/domain cohort split
 - Sys Eng competence
 - 2 days in-person
 - STPA theory + practical application
 - Post-course project
 - Volunteers, not conscripts

"Supervised STPA Practitioner"

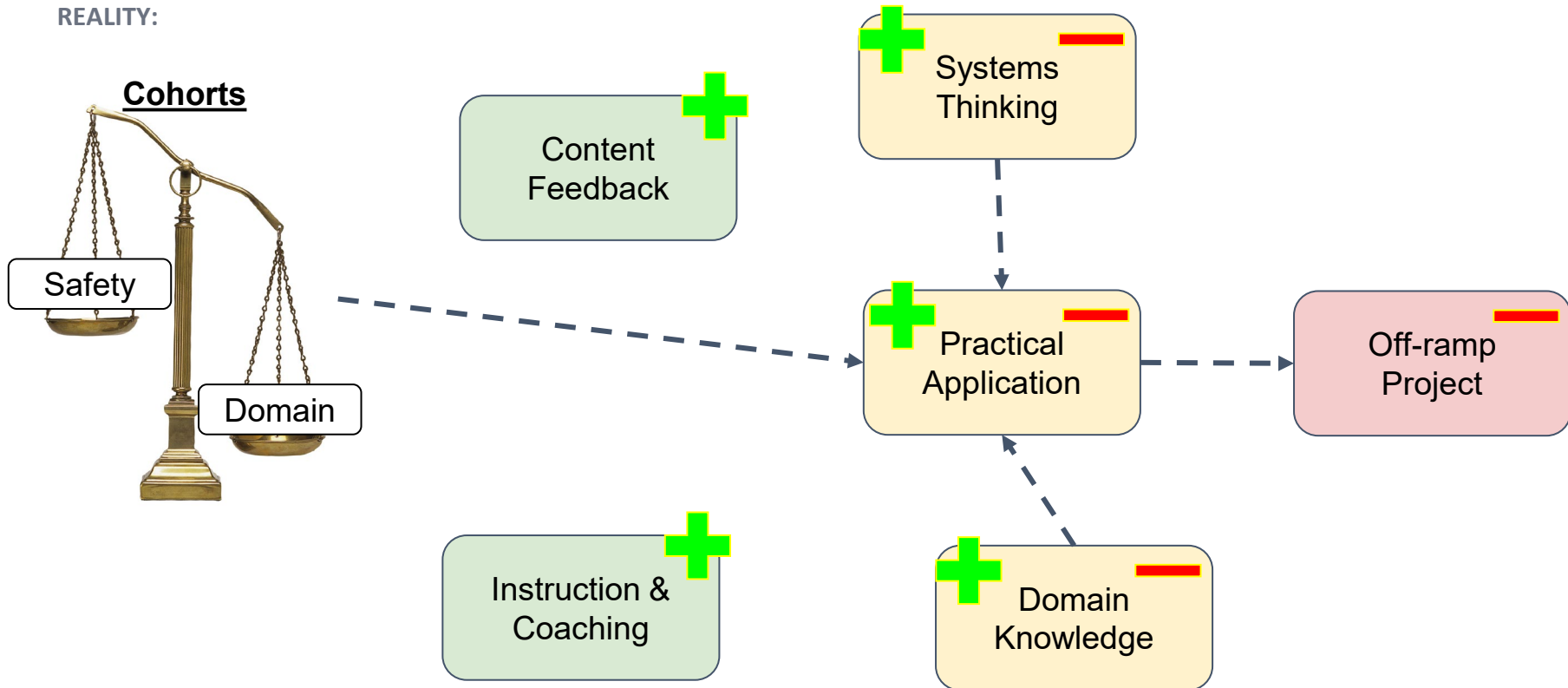
Someone able to contribute effectively to facilitated STPA, not an independent analyst.

1 Training & Awareness

Objective: Build internal capability

After 12 months, 3 cohorts, 30 delegates...

REALITY:



1

Training & Awareness

Objective: Build internal capability

What have we learnt?

Candidate selection

Need domain expertise
Need systems thinking
Tighter control
Who *needs* it?

Off-ramp project

Must offer *real value*
Small scope
Sandbox environment

Knowledge ≠ adoption

Support knowledge
application

2

Case Study Development

In Progress

Objective: Validate the knowledge on representative problems

Success Criteria

A representative STPA example for the submarine enterprise

New practitioners apply STPA in sandbox environment before the live programme

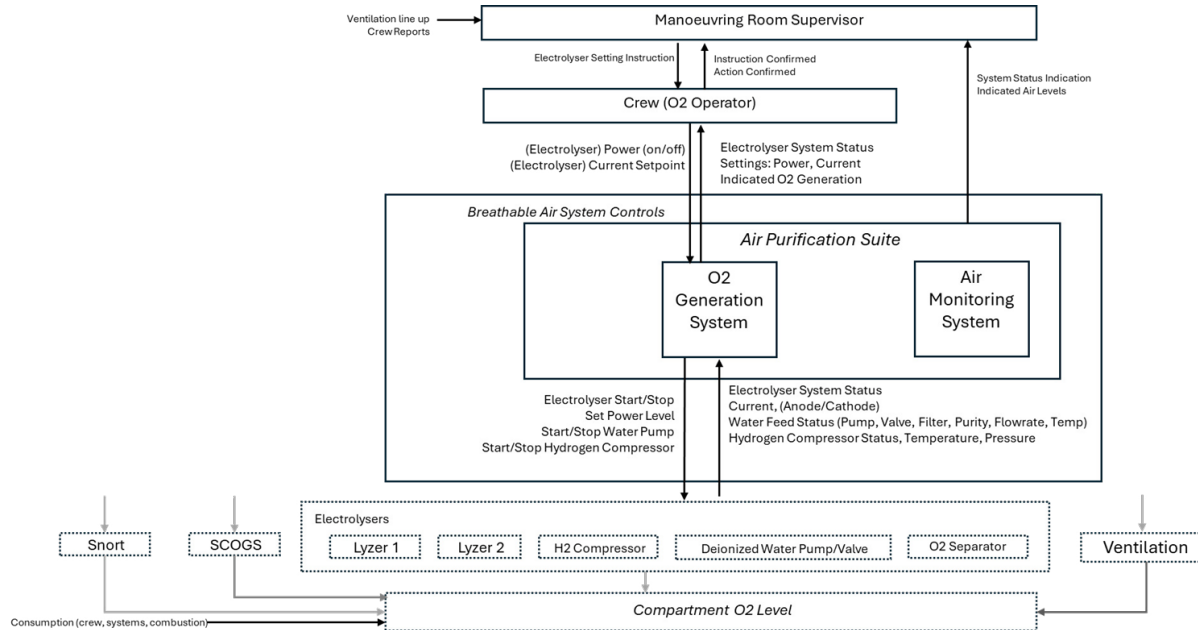
APPROACH

- Deliberately narrow and deep: full Steps 1–4 on a single topic
- In-person workshops over two days — essential at this stage of adoption
- Publicly available data — shareable, no security constraints

Case Study Development

Objective: Validate the method on representative problems

In Progress



Losses

- L1 Loss of Mission
- L2 Injury / Loss of Life
- L3 Damage to / Loss of Submarine
- L4 Environmental Damage

System Hazards

- H1 O₂ concentration exceeds acceptable limits [L2]
- H2 CO₂ concentration exceeds acceptable limits [L2]
- H3 Uncontrolled combustion or explosion [L1, L2, L3]
- H4 Atmosphere contaminants exceed acceptable limits [L2]

EXAMPLE UCAs

- UCA1.1 Crew does not power on the O₂ Gen System when O₂ levels fall below acceptable limits
- UCA1.2 Crew powers on the O₂ Gen System when O₂ levels rise above acceptable limits
- UCA2.4 O₂ Gen System Controller Starts Electrolyser when there is insufficient capability to circulate the O₂ produced

2

Case Study Development

In Progress

Objective: Validate the method on representative problems

UNEXPECTED PROGRAMME BENEFIT

BEFORE

"Failure to produce oxygen"

Functional failure mode

Conditional on data availability

Bounded to one system

Not a behavioural objective



AFTER

O₂ concentration exceeds acceptable limits

System state / condition

Agnostic to causation

Crosses system boundaries

Informs behavioural objectives



4

Hazard Redefinition using STAMP Principles

Objective: Iterate the programme system hazard set using STAMP criteria

4 Hazard Redefinition using STAMP Principles

Objective: Iterate the programme system hazard set using STAMP criteria

What have we gained?

1 Programme system hazard redefinition

Engineers now have consistently defined system states to work against.

Clarity in the safety ask.

2 Roads to multiple destinations

State-based hazards interface with FMEA, FTA, ETA

STAMP principles benefit the enterprise even where STPA isn't used.

3 Laid the groundwork for STPA's arrival

When full STPA begins, the hazard dataset is already STAMP-compatible.

2

Case Study Development

Objective: Validate the method on representative problems

In Progress

What have we learnt?

Narrow
Technical



Face to Face



Information
Restrictions



Deep Analysis



Limited Domain
Expertise



Be Open
Minded!

3

Method Integration

Objective: Integrate STPA into the programme safety management system

Success Criteria

STPA process, support, and tools available to practitioners

STPA data flowing in / out of programme information management systems

PLANNED APPROACH

- Process & support suitable for the organisation
- Analysis tool sets; procurement, in-house solutions, make-do
- Integration with information management systems - Hazard Log
- Change management

3 Method Integration

Objective: Integrate STPA into the programme safety management system

CHANGE MANAGEMENT

Frameworks for organisational change, COM-B

Capability

Awareness, knowledge, skills



Opportunity

Tools, time, facilitation



Motivation

Beliefs, drives, goals



Behaviour

“How we work round here”



WORK STREAMS

1 Training & Awareness

3 Method Integration (Process & Tools)

2 Case Study Development

Organisation is equipped and using STAMP-based methods on appropriate challenges

The key insights from 18 months of STPA adoption...

INSIGHT 1

1

Choose the right people to join you on the journey.

INSIGHT 2

2

4

STAMP principles can reshape programme practice before a single STPA output is formally documented.

INSIGHT 3

3

This is organisational transformation, not process rollout.
Give Change Management the respect it deserves.

We have no formal STPA outputs.

- Customer and engineers thinking differently about system safety
 - Programme hazard set defined in system state or condition terms
 - Established training programme cultivating supervised STPA practitioners
 - Enterprise recognising safety as a systems problem
 - STPA adoption strategy that respects the scale of the challenge ahead
-

It's been one of the most valuable things we've done.

Questions I'm taking into the next phase

How do we measure the success of STPA adoption?

How do we integrate STPA with model-based systems engineering?

How do we rebuild the connection between safety thinking and core engineering?