MIT STAMP WORKSHOP 2026 – 17th September 2026

# Breaking the Chain of Failure

## STPA for safer flight test of a reconfigurable flight-control system

The system met every requirement the programme had written for it. **STPA identified a hazardous condition those requirements could not express — and the simulator then measured a 6.2 g envelope departure.**

**Dr. Kishan S. Chowhan, CSEP (INCOSE), SM (SFTE)**
Group Director, Aeronautical Development Agency (ADA),
Bengaluru, India

# Disclaimer and data provenance

**This is an independent, research-oriented study.**
The reconfigurable control laws referenced here were developed by the author during doctoral research and are evaluated on an F-16C simulation model built entirely from the openly published NASA Technical Paper 1538.

The material does not reference, reveal or represent any proprietary data, software or test plan for the operational Lockheed Martin F-16, and does not describe or imply the status of any current or planned Aeronautical Development Agency programme.

All scenarios, control laws and results are presented solely to illustrate the application of STPA and MBSE to flight-test risk management.

03

# The aircraft, its control surfaces, and what STPA is for

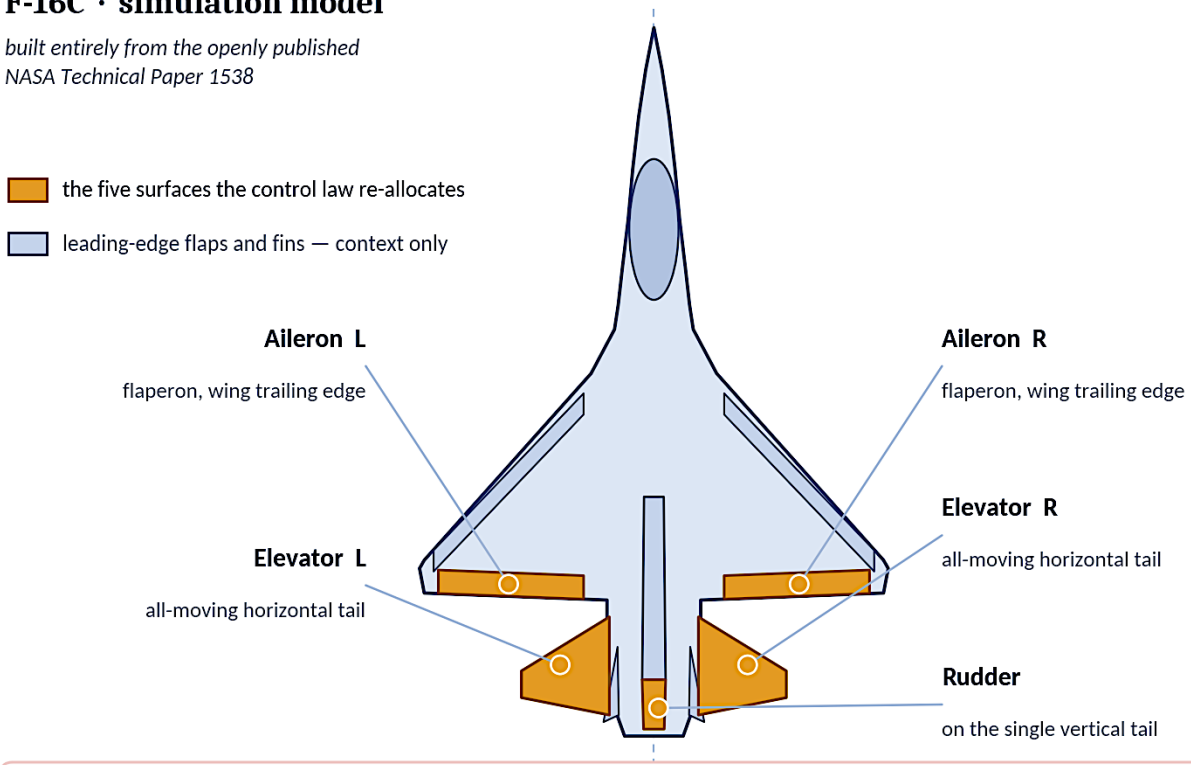
*An F-16C simulation model from NASA TP 1538, its five control surfaces, and the faults injected into them.*

ORIENTATION — BEFORE THE ANALYSIS

## THE AIRCRAFT AND ITS FIVE CONTROL SURFACES

### F-16C · simulation model

*built entirely from the openly published NASA Technical Paper 1538*




**Where the faults are injected**

Elevator R — stuck +7.5° (TC-01) · jammed +12.5° (TC-11) · detached (TC-10)
Aileron L — stuck −15° (TC-05)  Rudder — biased +15° (TC-02) · stuck +30° (TC-08)

## WHAT STPA IS, AND WHY IT IS USED HERE

1. **Losses and hazards**
   States of the aircraft we must never allow — not the causes that might produce them.
2. **Control structure**
   Who commands what, and on what feedback — the test director and the pilot included.
3. **Unsafe control actions**
   The contexts in which a correct, by-design command becomes hazardous.
4. **Loss scenarios**
   Why that context can arise — and the safety requirement that removes it.

**Why here**

This control law is designed to keep working after a component fails. Nothing is “broken”, so the hazard lives in the commanding — not the hardware.

04

# The problem, and why FMEA could not close it

*Clearing an adaptive, self-modifying control law for piloted flight test.*

PROGRAMME BASELINE — BEFORE STPA

## WHAT IS BEING FLIGHT-TESTED

**Surface fault · jam · hardover · surface loss**

↓

**UKF**

re-estimates the inertia tensor online after damage

**NDI + ANN**

nonlinear inversion with a neural-network augmentation

↓

**Control allocation**

authority re-distributed across the five remaining surfaces

↓

**...and the aircraft keeps flying**

*The hazardous behaviour is the system doing exactly what it was designed to do.*

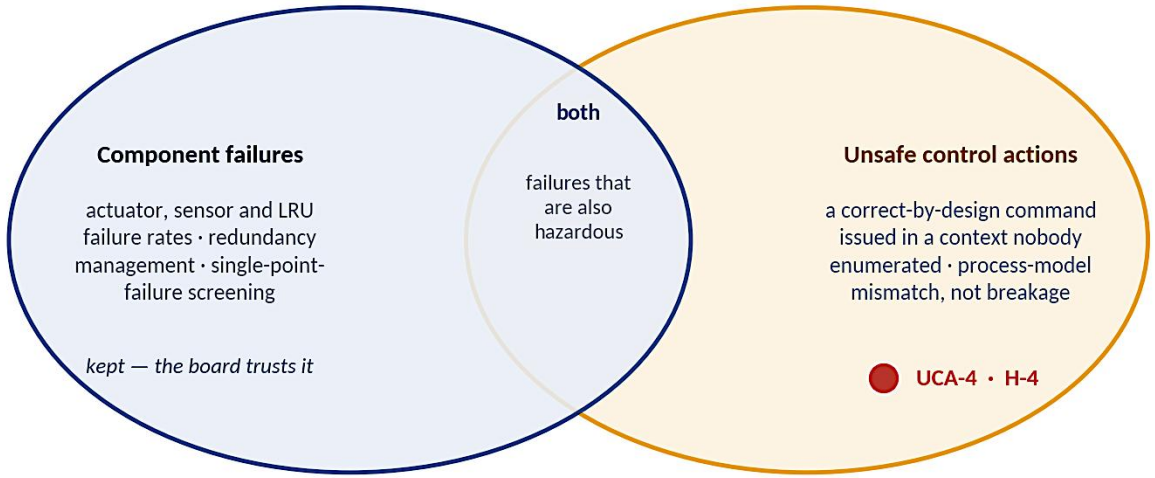
## WHY THE USUAL SAFETY CASE DOES NOT CLOSE

**FMEA asks**

*"what happens if it breaks?"*

**STPA asks**

*"in what context is this behaviour unsafe?"*




**The gap FMEA cannot reach**

Nothing is broken. Add a pilot who may not know which law is flying the aircraft, and the risk lives in the interactions — not in any one component.

The rule we settled on: **if the hazardous behaviour can be described without using the word "broken", it belongs to STPA.**

05

# STPA Step 1 — losses and system-level hazards

*Hazards are states of the aircraft, not causes. Failure-based items move to Step 4.*

OUTPUT OF THIS STPA ANALYSIS

## Losses

L-1 Loss of the aircraft

L-2 Death of or injury to the test pilot

L-3 Injury to ground personnel or the public

L-4 Damage to third-party property

L-5 Loss of the flight-test evidence needed for the airworthiness decision

L-6 Compromise of sensitive programme information

| ID | System-level hazard (state of the aircraft) | Losses |
|---|---|---|
| H-1 | Aircraft departs controlled flight | L-1…L-4 |
| H-2 | Aircraft exceeds its structural or aerodynamic limits — normal acceleration, angle of attack, sideslip | L-1…L-4 |
| H-3 | Aircraft violates minimum separation from terrain, other traffic or the range boundary | L-1…L-4 |
| H-4 | Aircraft operates outside the conditions cleared on the flight-test card | L-1, L-2, L-5 |
| H-5 | Aircraft cannot be commanded to the attitude or flight path the pilot requires | L-1, L-2 |
| H-6 | Evidence required for the airworthiness decision is not captured or is corrupted | L-5 |

*H-4 did not exist in the programme's pre-STPA hazard list, which was organised around component failures. Writing hazards as aircraft states is what produced it — and it is the hazard a flight-test programme actually manages.*

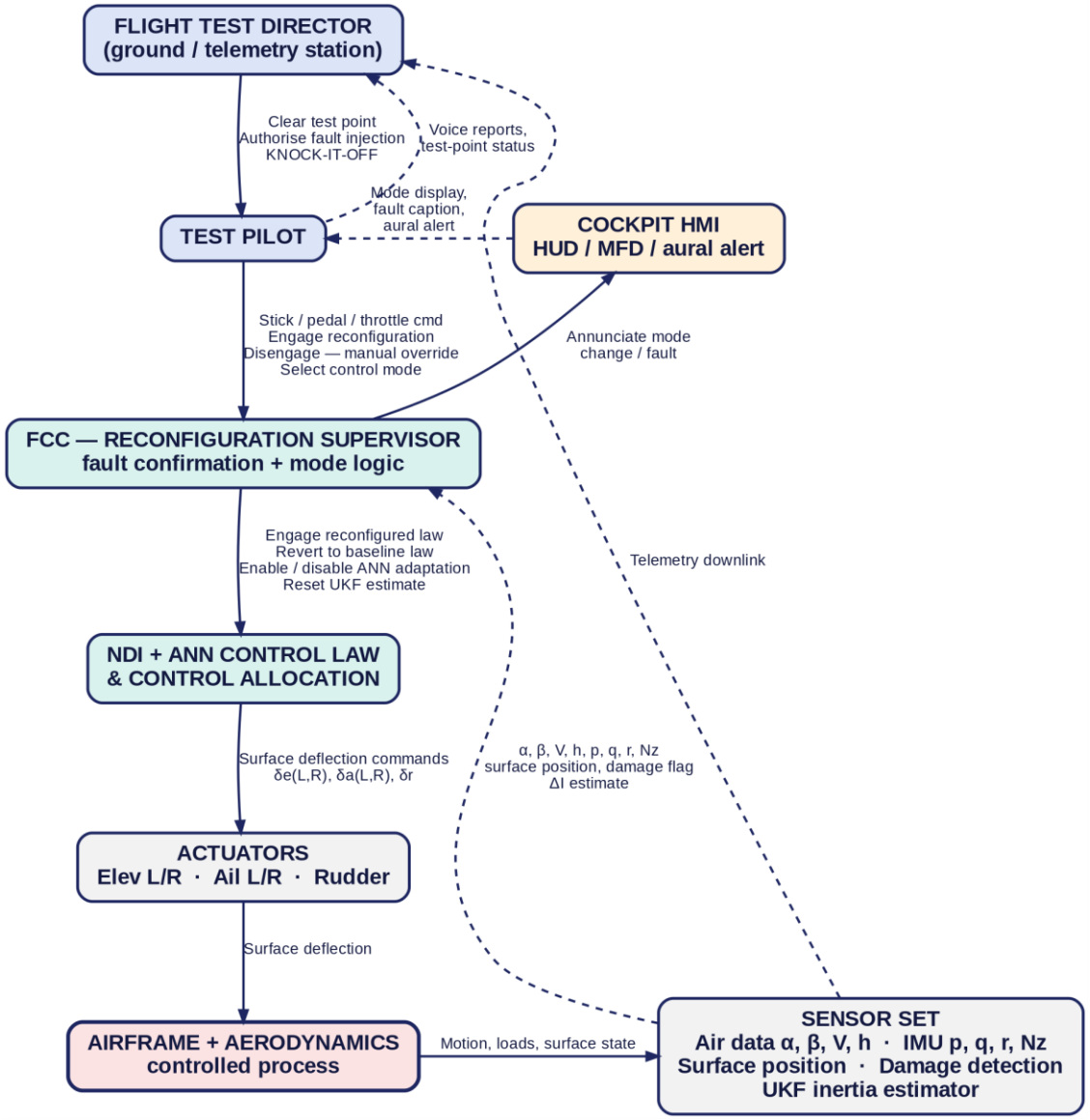
⊕ constraints

06

# STPA Step 2 — control structure

*Every arrow is a named control action or feedback signal. Five controllers.*

OUTPUT OF THIS STPA ANALYSIS




## Controllers and their control actions

**Flight Test Director**
Clear test point · authorise fault injection · knock-it-off

**Test Pilot**
Stick, pedal and throttle commands · engage reconfiguration · disengage and take manual control · select control mode

**FCC — Reconfiguration Supervisor**
Engage reconfigured law · revert to baseline law · enable or disable ANN adaptation · reset UKF estimate · annunciate mode change

**NDI + ANN law and allocation**
Surface deflection commands to the five surfaces

**Cockpit HMI**
Mode display, fault caption and aural alert to the pilot

*The supervisor and the control law are separated deliberately: they have different control actions and different unsafe contexts.*

07

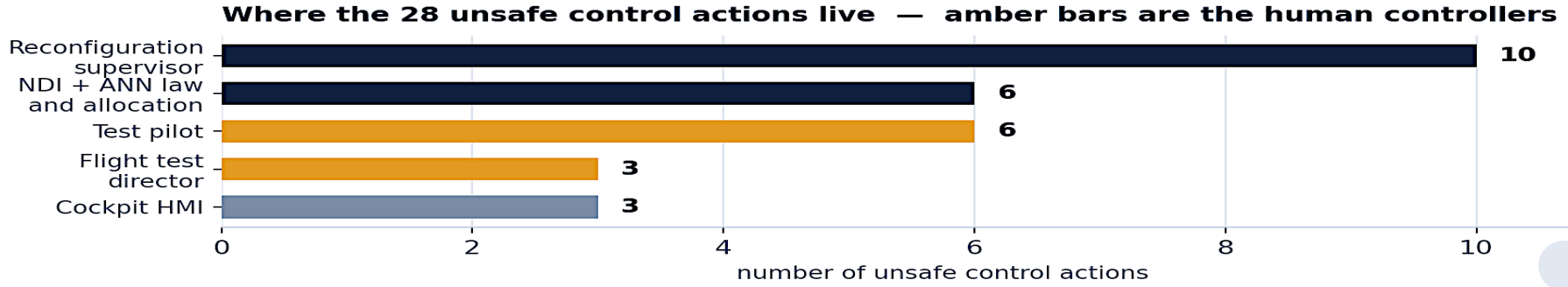
# STPA Step 3 — one control action, all four guide phrases

*Control action: Reconfiguration Supervisor → Engage reconfigured law*

OUTPUT OF THIS STPA ANALYSIS

| Not providing causes hazard | Providing causes hazard | Too early / too late / wrong order | Stopped too soon / applied too long |
|---|---|---|---|
| UCA-2 Supervisor does not provide Engage-reconfigured-law when a control surface is jammed or detached and the baseline law cannot trim the aircraft [H-1, H-5] | UCA-1 Supervisor provides Engage-reconfigured-law when no surface fault is present and the baseline law retains full authority [H-1]<br><br>UCA-4 Supervisor provides Engage-reconfigured-law when normal acceleration is already above 4 g [H-2] | UCA-3 Supervisor provides Engage-reconfigured-law more than 1.0 s after a confirmed surface fault while the aircraft is diverging in pitch or roll [H-1]<br><br>UCA-5 Supervisor provides Engage-reconfigured-law on a single-source anomaly, before dual-channel confirmation, while the aircraft is | UCA-6 Supervisor continues to apply the reconfigured law after the fault indication has cleared, while the law is commanding a diverging surface deflection [H-1]<br><br>UCA-7 Supervisor stops applying the reconfigured law while the surface is still jammed [H-1, H-5] |

**UCA-4 was not on anyone's list before this table was filled in.** It falls out mechanically from asking "in what context does providing this command cause a hazard?" — and it is the one that later cost us a test point. Every UCA names the source controller, the type, the control action, the context, and the hazards. No component failures, no outcomes, no use of the word "fails".



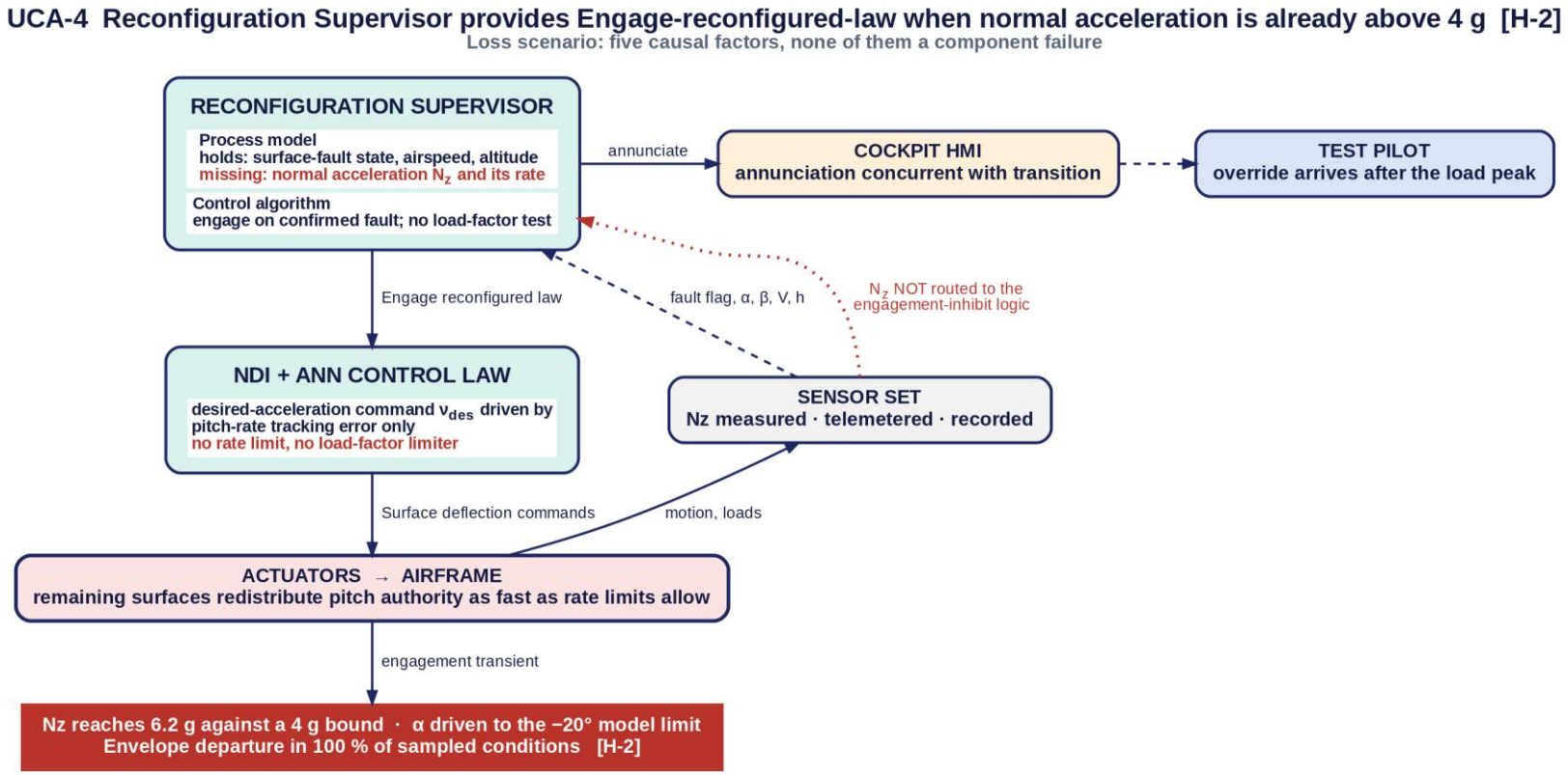

all 28 UCAs

08

# The same scenario, drawn on the control loop

*The controller constraint falls straight out of the diagram*

OUTPUT OF THIS STPA ANALYSIS




## Controller constraint C-4

*"The Reconfiguration Supervisor must not provide Engage-reconfigured-law while normal acceleration exceeds 4 g, unless the engagement is entered in a load-limited mode."*

## Reading the diagram

The red path is the whole finding: Nz is measured, telemetered and recorded, and never reaches the logic that decides whether to engage. Nothing on this diagram is broken.

**Scenario E — the part of Step 4 that is easiest to skip.**

The Handbook also asks how a correctly issued control action can still be executed differently from the way it was intended. At high dynamic pressure the surfaces are rate-limited, so the deflection achieved lags the deflection commanded, and the supervisor's filtered surface-position feedback lags further still. Both controllers then act on a surface state the aircraft no longer has — which is why SR-29 limits the command rather than the surface.

⊕ scenario table

09

# From scenario to requirement to test point

*Six requirements that did not exist before Step 4 — and the chain that carries them to the flight-test card.*

OUTPUT OF THIS STPA ANALYSIS




| SR | New or revised safety requirement | From | Kind of change |
|---|---|---|---|
| SR-4 | The supervisor shall include current normal acceleration and its rate in the state on which the engage decision is made. | Scenario A, C | Process model |
| SR-28 | Engagement shall be inhibited, or entered in a reduced-authority mode, while normal acceleration exceeds 4 g. | Scenario A, B | Mode logic |
| SR-29 | The desired-acceleration command generated during the engagement transient shall be rate-limited so that predicted Nz stays within 4 g. | Scenario B | Control law |
| SR-12 / SR-30 | Mode-change annunciation shall lead, not accompany, a supervisor-commanded transition, and be downlinked within 1 s. | Scenario C, D | HMI + telemetry |
| FTR-09 | No test point shall inject a surface fault above 3 g until SR-28 and SR-29 are verified on the simulator and the HIL bench. | Scenario A–D | Flight-test card |

**FTR-09 is a test point we removed from the card. It is the clearest return on the analysis: a hazardous flight condition that will not be flown, with a written reason why.**

⊕ full SR set

10

# The simulator campaign that gates flight test

*Every case exists because an STPA-derived safety requirement demanded it.*

SIMULATOR EVIDENCE

| TC | Injected fault | Trim / manoeuvre | Acceptance criteria |
|---|---|---|---|
| TC-01 | Right elevator stuck +7.5°, CG +0.3%, right-wing damage 10% | 10 000 m / 250 m/s, wings level | Activation ≤ 1 s · recovery < 5 s · ≤ 1 oscillation cycle · HQ ≤ Level 2 |
| TC-02 | Rudder biased +15°, CG −0.2%, left-wing damage 12% | 8 500 m / 235 m/s, 30° banked turn | Bias removed · ≤ 3 oscillation cycles · recovery < 5 s · HQ ≤ Level 2 |
| TC-05 | Left aileron stuck −15°, 25% right-rudder loss | 11 000 m / 265 m/s, wings level | Roll recovery < 5 s · bank < 30° · ≤ 3 cycles · HQ ≤ Level 2 |
| TC-08 | Rudder stuck +30° full deflection, 5% spanwise lift loss | 11 500 m / 260 m/s, pull-up | Adaptation converges < 2 s · sideslip within ±5° · recovery < 5 s |
| TC-10 | Right elevon detached, $\Delta I_z$ = +150 kg·m², symmetric thrust loss | 8 800 m / 230 m/s, turning | UKF identifies $\Delta I_z$ < 30 s · activation ≤ 1 s · recovery < 5 s |
| TC-11 | Right elevator jammed +12.5°, $\Delta I_y$ = −200 kg·m² | 10 000 m / 250 m/s, wings level | Activation ≤ 1 s · UKF identifies $\Delta I_y$ < 30 s · normal acceleration ≤ 4 g |

**Why no pilot in these runs:** stick and pedal are held at their pre-fault reference after injection, so the reconfigurable law alone has to stabilise the aircraft. That keeps the Monte-Carlo deterministic and repeatable, keeps the timing criteria measured against a known reference, and separates the autonomous evidence cleanly from the piloted campaign that follows it.

⊕ TC-01/05/10

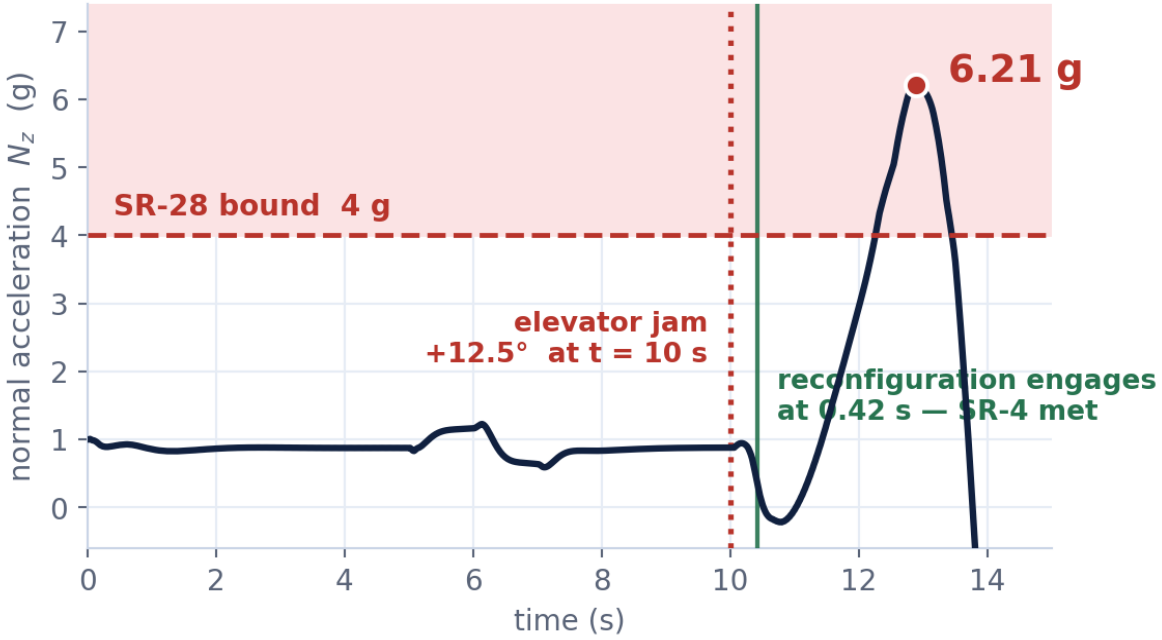
11

# TC-11 — the case that changed the programme

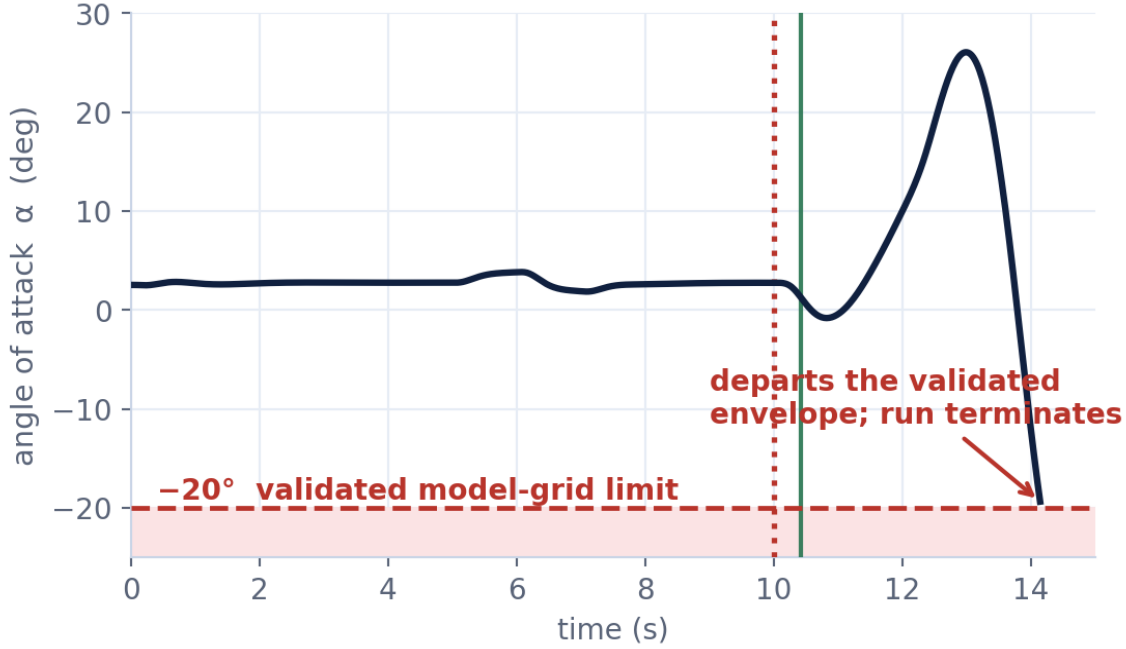
*Right elevator jammed +12.5° with $\Delta I_y = -200$ kg·m², injected at t = 10 s from 10 000 m / 250 m/s.*

SIMULATOR EVIDENCE

## SR-4 met, SR-28 violated




## …and the envelope departure that followed




**0.42 s**

time to engage the reconfigured law.
SR-4 requires 1.0 s — comfortably met.

**6.21 g**

peak normal acceleration in the engagement transient.
SR-28 bounds it at 4 g — violated.

**100%**

of sampled altitude and airspeed conditions produce the same departure. Not a corner case.

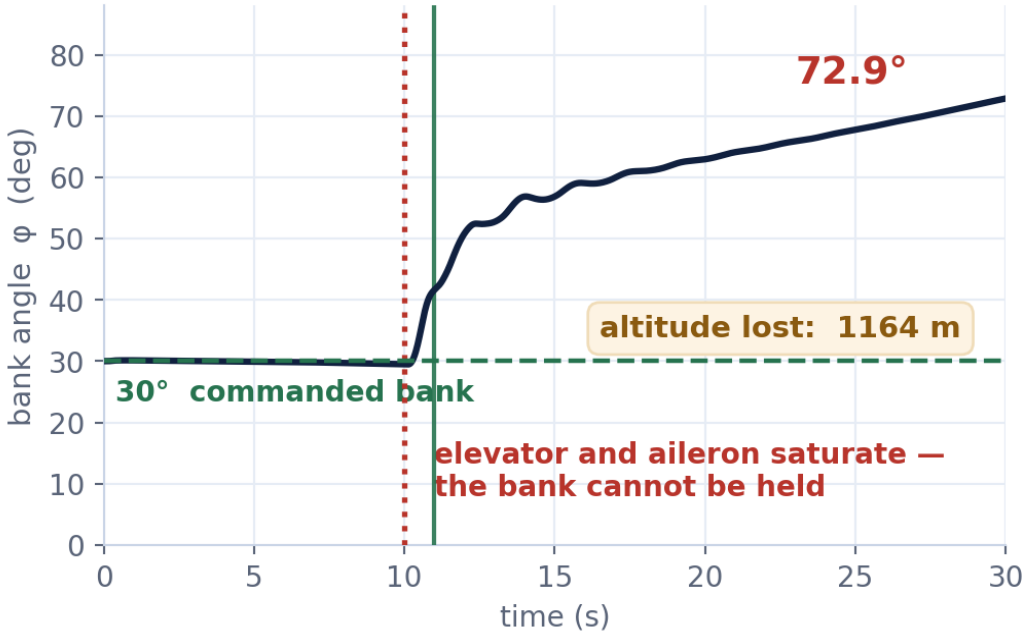
**Before this analysis TC-11 was scored on activation time and inertia identification alone — against those criteria it passes. The 4 g bound it violates is SR-28, and SR-28 exists only because STPA Step 3 produced UCA-4.**

# Two more findings, binding for different reasons

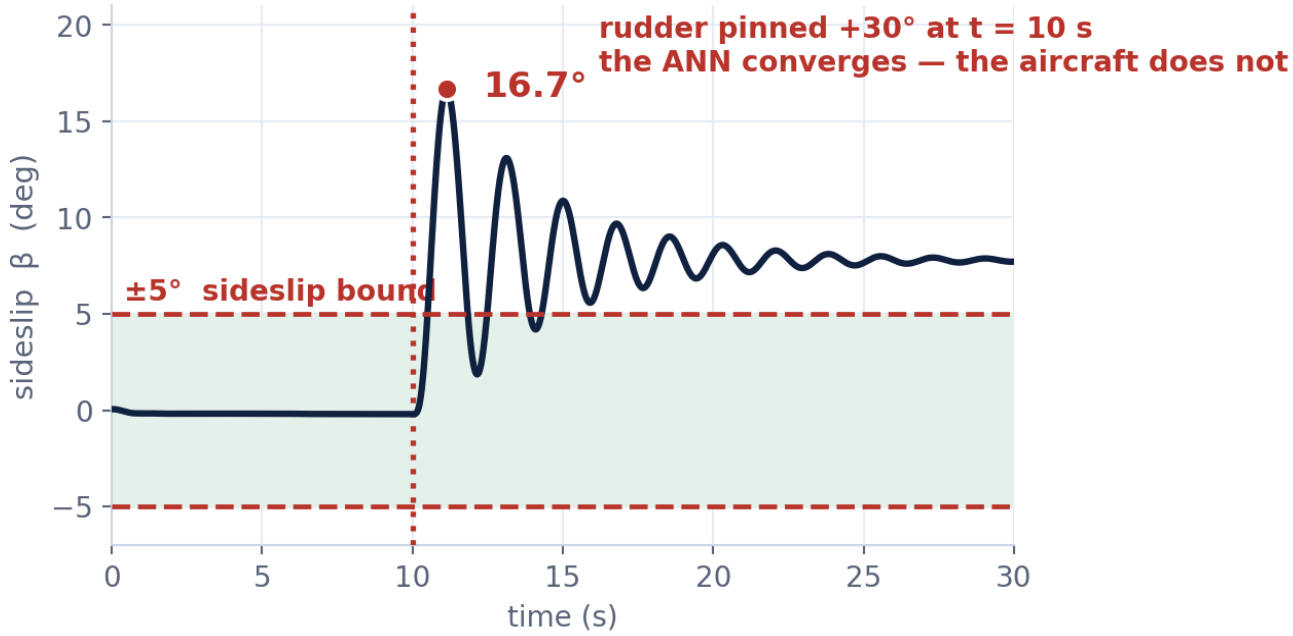
*Both engaged on time. Both failed for reasons the timing requirement cannot express.*

SIMULATOR EVIDENCE

### TC-02 — control authority binds




### TC-08 — directional damping binds




**TC-02 — authority, not timing.** The yaw-channel adaptive element drives toward the correct bias-cancelling value and never gets there: elevator and aileron saturate first. Maps to UCA-11.

**TC-08 — damping, not convergence.** The metric everyone expected to bind — adaptation speed — is not the problem. With the rudder pinned, the aircraft's own directional response is. Maps to UCA-12.

Four findings, four different binding constraints — **control authority, directional damping, handling degradation, load factor. None of them activation latency, which is what the programme had been optimising.**

# Results — one clean pass, one marginal, four findings

*The 4 g clause in TC-11's criteria is SR-28, an STPA output. Without it, TC-11 scores a pass.*

SIMULATOR EVIDENCE

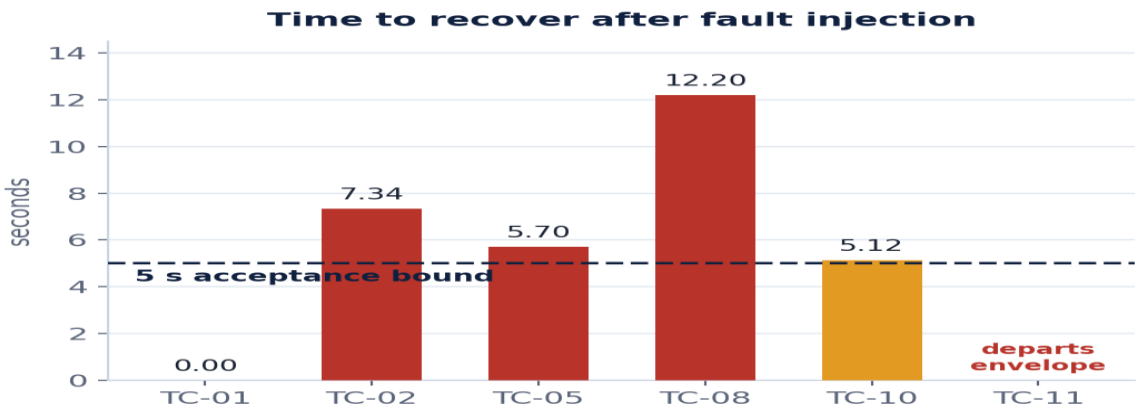
| TC | Activation (≤ 1 s) | Recovery (< 5 s) | Osc. cycles | HQ (≤ 2) | Outcome |
|---|---|---|---|---|---|
| TC-01 | 0.30 s | 0.0 s | 0 | 1.12 | **PASS** |
| TC-02 | on time | 7.34 s | 4 | 6.73 | FINDING — control authority exhausted |
| TC-05 | 0.20 s | 5.70 s | 0 | 3.53 | FINDING — Level 3 handling qualities |
| TC-08 | on time | 12.2 s | 6 | 10 | FINDING — sideslip 16.7° against ±5° |
| TC-10 | 1.06 s | 5.12 s | 0 | 4.05 | MARGINAL — deadlines missed by ~0.1 s |
| TC-11 | 0.42 s | — departs | — | — | **FINDING — 6.2 g vs 4 g; envelope departure** |

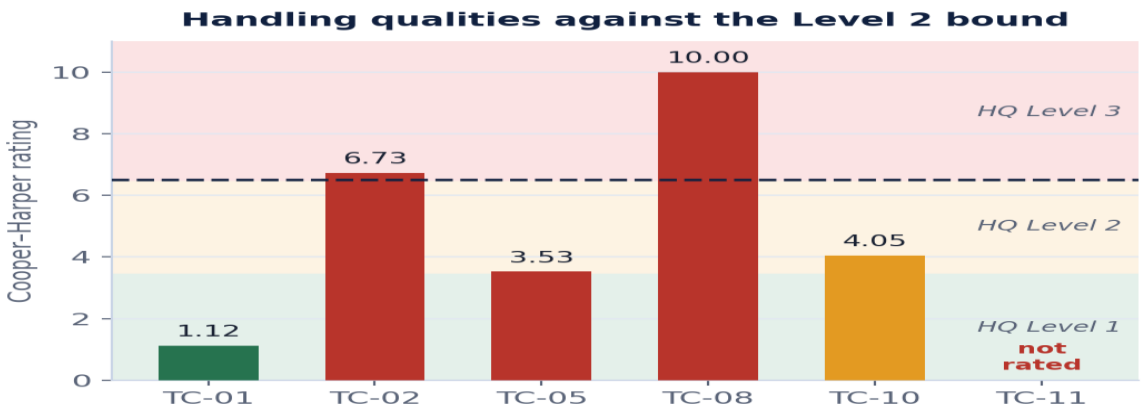
### Envelope sweep

Each fault re-injected across 8 500–12 000 m and 230–270 m/s. TC-11 departs the validated envelope in 100% of sampled conditions, median peak load near 6 g. No other case departs, and no other case exceeds 4 g.

### What binds, case by case

Control authority · directional damping · handling degradation · load factor. Four different constraints — none of them activation latency.



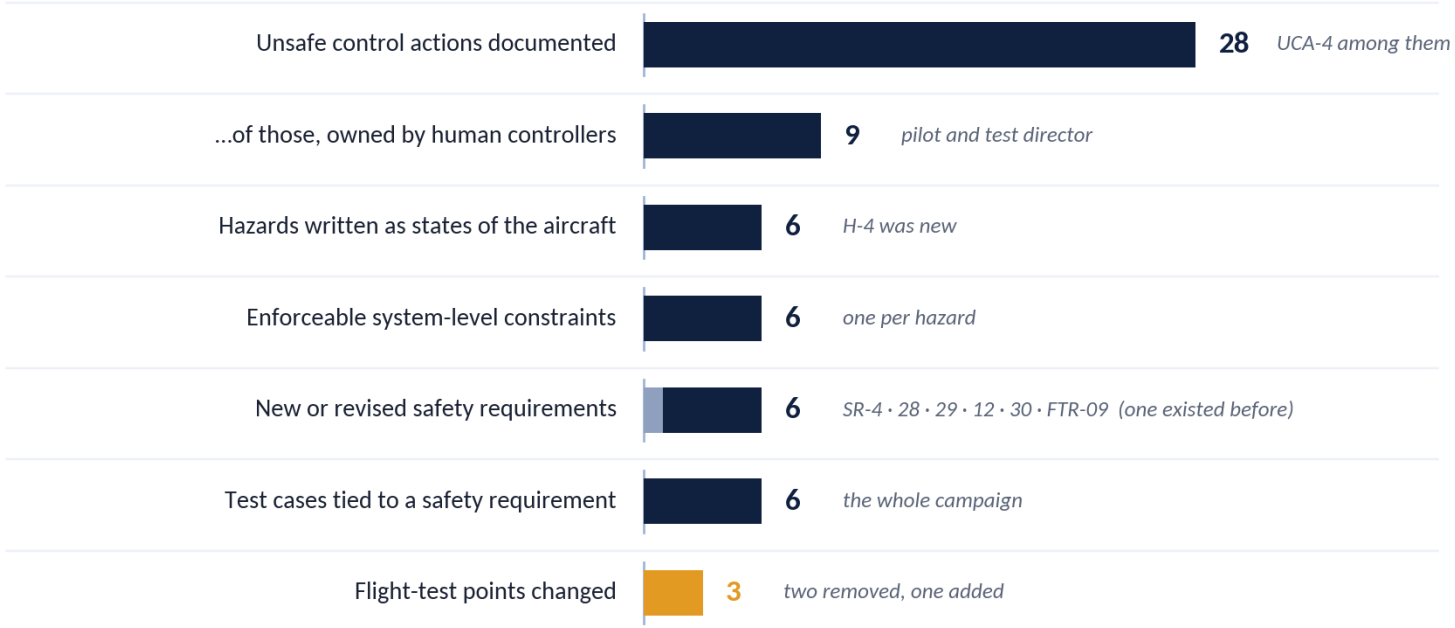




envelope sweep

# What STPA found that we did not already know

*The middle column is the claim being made. None of it existed in the programme's safety case before this analysis.*

## WHAT DID NOT EXIST IN THE SAFETY CASE BEFORE THIS ANALYSIS




Counts are of artefacts that the programme's pre-STPA safety case did not contain. The one non-zero "before" is the single headline requirement the programme had been optimising: reconfigure within 1 s of a confirmed fault.

## AND HOW THE CLAIM WAS CONFIRMED

**TC-11 · right elevator jammed +12.5°**

*scored against the pre-STPA criteria, this case passes*

**0.42 s** ✓ met

activation, against the 1 s deadline the programme wrote

**6.21 g** ✗ violated

peak normal acceleration, against the 4 g bound STPA produced

**100 %** ✗ not a corner case

of sampled altitude and airspeed conditions depart the envelope

The 4 g clause in TC-11's acceptance criteria is SR-28, and SR-28 exists only because Step 3 produced UCA-4.

**The honest summary:** the programme knew the system worked. It did not know the conditions under which making it work was itself the hazard. That gap is what STPA closed, and it is the whole of the benefit claimed in this talk.

# 15 What changed as a direct result of the STPA analysis

*Every item traces to a specific UCA or loss scenario.*

OUTPUT OF THIS STPA ANALYSIS

## WHERE EACH CHANGE LANDS

**Flight Test Director** — 6 5 4
clear point · authorise · knock-it-off

↓

**Test Pilot**
stick · engage · disengage · mode

↓

**Cockpit HMI** — 3
mode display · caption · aural alert

↓

**Reconfiguration Supervisor** — 2
engage · revert · adapt · reset

↓

**NDI + ANN law and allocation** — 1
surface deflection commands

↓

**Actuators → Airframe**
five surfaces · the controlled process

Numbered badges mark the controller each change acts on.

## WHAT CHANGED — AND THE ARTEFACT IT CAME FROM

**1 Control law** — UCA-4 → SR-28, SR-29
A load-factor limiter in the desired-acceleration path; engagement inhibited or authority-limited above 4 g.

**2 Supervisor process model** — Scenario C → SR-4
Normal acceleration and its rate became inputs to the engage decision — measured all along, never routed to the controller that needed them.

**3 Cockpit HMI** — UCA-16, UCA-17 → SR-12, SR-30
Annunciation now leads the control-law transition rather than accompanying it, whenever the supervisor commands it.

**4 Flight-test cards** — UCA-4, UCA-26 → FTR-09
No surface fault injected above 3 g until SR-28 and SR-29 are verified on the simulator and the HIL bench; altitude blocks raised.

**5 Abort criteria** — UCA-27
Knock-it-off became a quantitative telemetry threshold on normal acceleration and sideslip, not a judgement call by the test director.

**6 Test scope** — UCA-11, UCA-12
TC-08 and TC-02 conditions not cleared for piloted flight until the authority and damping findings close. Two points removed, one added.

changes how the aircraft is built

changes how it will be flown — the outputs a flight-test organisation can act on immediately

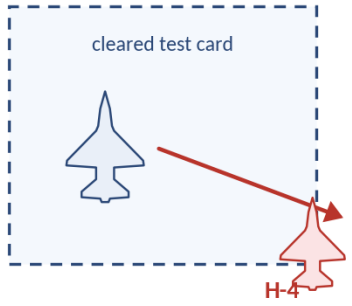
16

# What we would tell another flight-test organisation

*Transferable lessons from applying STPA.*

OUTPUT OF THIS STPA ANALYSIS

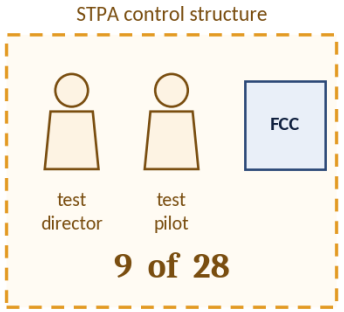
## 1 HAZARDS




**STPA hazards written as aircraft states surface the flight-test hazards.**

*H-4 — operating outside the cleared test card*

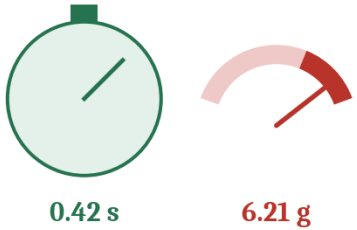
## 2 SCOPE




**Put the test director inside the STPA control structure.**

*9 of the 28 UCAs belong to human controllers*

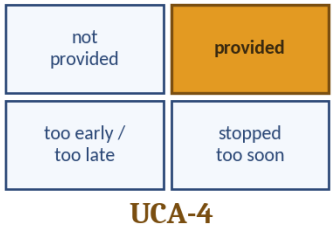
## 3 CRITERIA




**A timing requirement is not a safety requirement.**

*latency bound in none of the six cases*

## 4 METHOD

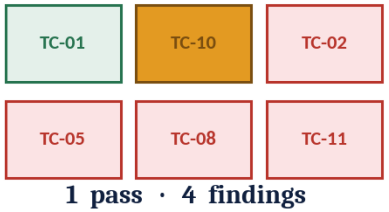



mechanical, not brainstormed

**The most valuable UCA was the one nobody proposed.**

*UCA-4 fell out of the four guide phrases*

## 5 OUTPUT




the findings rewrote the programme

**Findings are the product. Passes are not.**

*one clean pass · four findings*

17

# What this STPA analysis cost us

*Reported honestly, including the parts that were slower than expected.*

COST OF THIS STPA ANALYSIS

## TEN CALENDAR WEEKS OF ONE ENGINEER, PART-TIME

**Learning the method**

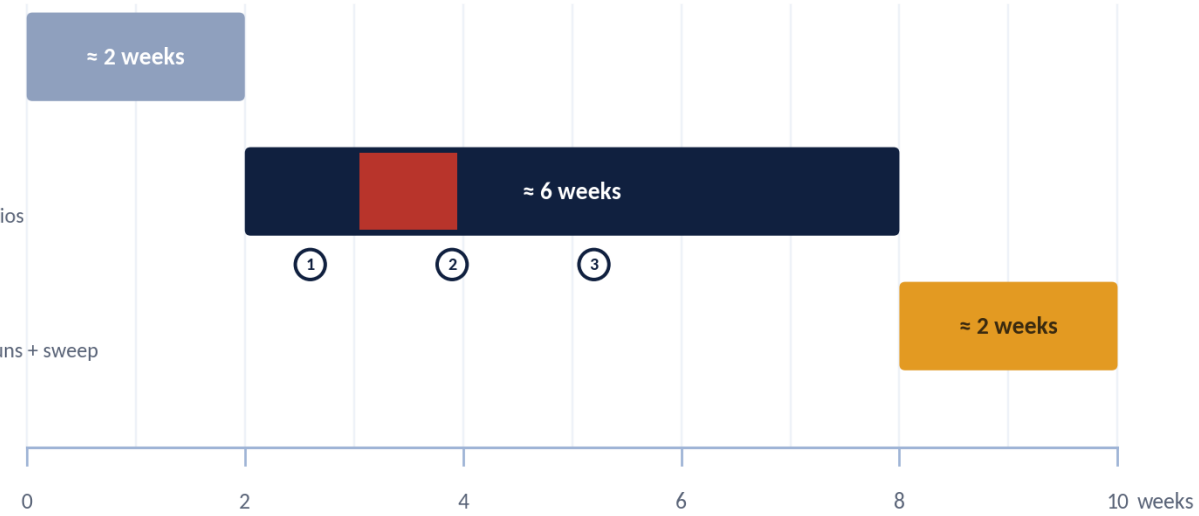
STPA Handbook · MIT online material

**STPA Steps 1 – 4**

blank page → 28 UCAs with loss scenarios

**Simulator campaign**

safety requirements → deterministic runs + sweep




1 week lost — the first hazard list held six causes dressed as hazards, and every downstream artefact inherited the error. Rewriting it was avoidable.

① ② ③ Three iterations of the control structure — the single most expensive artefact, and the one that determined the quality of everything downstream.

## AGAINST EXPECTATION — AND WHAT IT BOUGHT

### ▼ Cheaper than expected

Filling in the UCA table. Once the control structure was right, the four guide phrases generated the UCAs almost mechanically — UCA-4 included. The artefact set ports to the next platform unchanged.

### ▲ More expensive than expected

Persuading engineers that a hazard is a state of the aircraft and not a cause. And keeping the traceability live once requirements started changing — tooling helps, discipline decides.

### Set against

**2** hazardous flight-test points that will never be flown

**1** design change made before first flight, not after it

**6** safety requirements that did not exist before Step 4

# Conclusions

| | |
|---|---|
| **STPA identified a hazardous condition the programme's own requirements could not express.** | The system met its 1 s activation deadline in all six simulator cases. STPA Step 3 produced UCA-4 — engaging the reconfigured law above 4 g — and Step 4 explained the mechanism. The simulator then measured 6.2 g and an envelope departure in 100% of sampled conditions. |
| **Without this STPA analysis, the pivotal test case would have been recorded as a pass.** | The 4 g clause in TC-11's acceptance criteria is SR-28, and SR-28 exists only because of this work. Scored against the pre-STPA criteria — activation time and inertia identification — TC-11 passes. |
| **STPA outputs changed the aircraft and the way it will be flown.** | A load-factor limiter and engagement inhibit in the control law, normal acceleration added to the supervisor's process model, annunciation re-timed, altitude blocks raised, knock-it-off made quantitative, and two hazardous flight-test points deleted from the card. |
| **The cost was about six weeks of one engineer, part-time.** | Set against a design change made before first flight rather than after it, and two hazardous test points that will now never be flown. The artefact set is platform-independent and ports to the next programme. |

**If you quote one line:** ***"STPA found a way to fail that our requirements could not describe — the system met every deadline it was given, and still departed the flight envelope."***

# Appendix

Material for the workshop archive — not presented in the 15-minute talk.
System-level constraints, all 28 UCAs, the Step 4 scenario table, the full requirement set and traceability matrix, the remaining three test cases, and the randomized envelope sweep.
Every appendix slide links back to the main slide it supports; the main slides carry a link out to it.

◀ back to slide 18 · conclusions

20

# STPA Step 1 — system-level constraints

*One enforceable constraint per hazard, binding on the design and on the test card.*

APPENDIX — NOT PRESENTED

| SC | System-level constraint | H |
|---|---|---|
| SC-1 | Following any single credible control-surface jam, hardover or structural loss within the cleared envelope, the aircraft must remain in controlled flight. | H-1 |
| SC-2 | The transient produced by engaging or disengaging the reconfigured control law must not take normal acceleration, angle of attack or sideslip beyond validated limits. | H-2 |
| SC-3 | A fault must not be injected, and reconfiguration must not be engaged, unless the remaining altitude block is sufficient for recovery. | H-3 |
| SC-4 | The aircraft must not be flown outside the conditions cleared on the test card; when it drifts outside, the test point must be terminated. | H-4 |
| SC-5 | The pilot must at all times be able to determine which control law is in command and to revert to the baseline law. | H-5 |
| SC-6 | Telemetry and instrumentation must capture the parameters on which the airworthiness decision depends, for every test point flown. | H-6 |

**SC-2 is the constraint the campaign later violated — and it was violated by a reconfiguration that engaged correctly and on time. That is the whole story of this submission in one line.**

◀ back to slide 5

# STPA Step 3 — representative UCAs across the other controllers

*28 UCAs in total. Nine belong to the human controllers.*

APPENDIX — NOT PRESENTED

| UCA | Controller | Unsafe control action, with context | H |
|---|---|---|---|
| UCA-11 | NDI law / allocation | Provides surface deflection commands that saturate the remaining unfailed surfaces while the aircraft is in a banked turn still requiring roll authority | H-1, H-5 |
| UCA-12 | NDI law / allocation | Continues to command opposing aileron against a pinned rudder for longer than 5 s while sideslip exceeds 5°, sustaining the divergence | H-1, H-2 |
| UCA-16 | Reconfiguration Supervisor | Does not provide the mode-change annunciation to the HMI when the control law transitions from baseline to reconfigured | H-4, H-5 |
| UCA-17 | Reconfiguration Supervisor | Provides the mode-change annunciation more than 1 s after the transition, while the pilot is applying a large stick input | H-1, H-5 |
| UCA-21 | Test Pilot | Provides a large pitch command during the reconfiguration transient, while the adaptive element has not yet converged | H-1, H-2 |
| UCA-23 | Test Pilot | Does not provide the disengage / manual-override command when the reconfigured law is driving the aircraft toward the angle-of-attack limit | H-1, H-2 |
| UCA-26 | Flight Test Director | Provides Clear-for-fault-injection when the aircraft is below the minimum altitude block cleared for recovery | H-3, H-4 |
| UCA-27 | Flight Test Director | Does not provide Knock-it-off when telemetry shows normal acceleration above the cleared limit | H-2, H-4 |

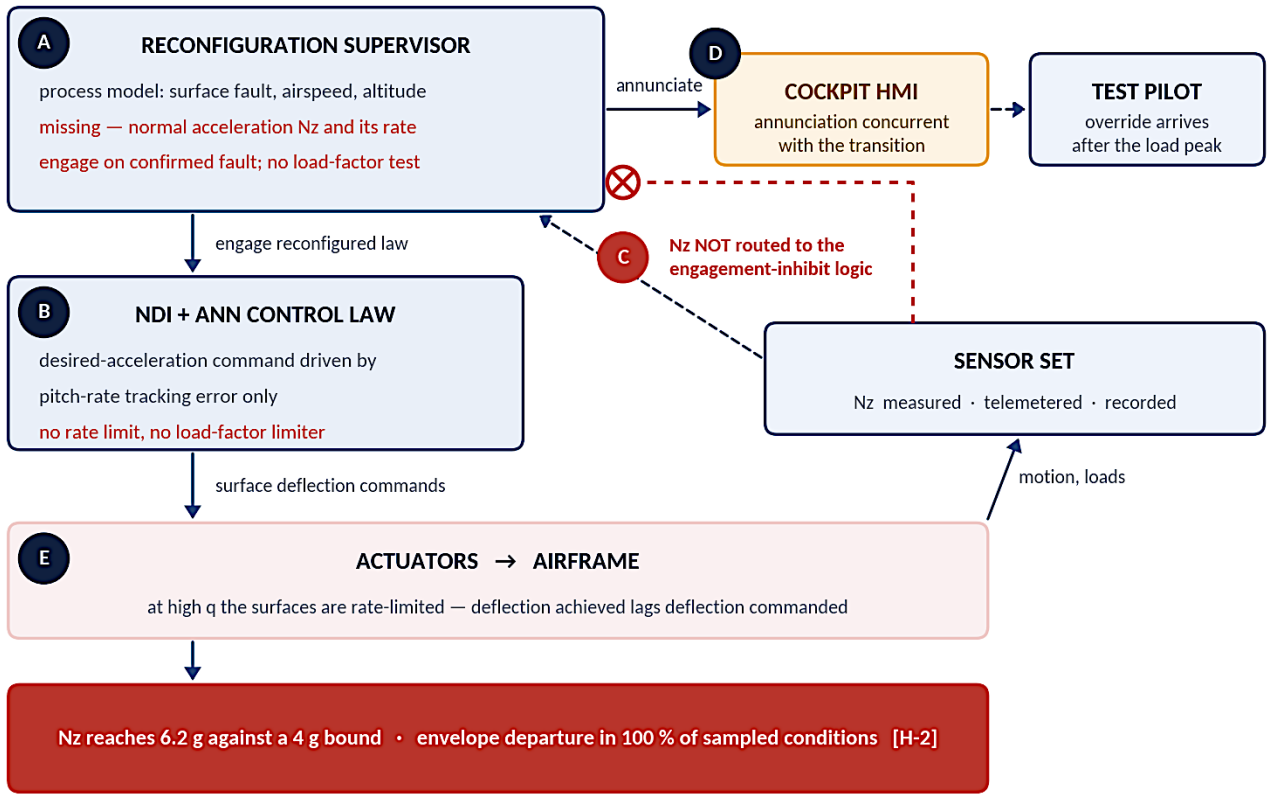
◀ back to slide 7

# STPA Step 4 — loss scenario for UCA-4

*UCA-4: supervisor provides Engage-reconfigured-law above 4 g [H-2]*

APPENDIX — NOT PRESENTED

## THE FIVE CAUSAL FACTORS, LOCATED ON THE CONTROL LOOP




## NONE OF THE FIVE IS A COMPONENT FAILURE

**A — Process-model flaw**

The supervisor holds surface-fault state, airspeed and altitude — but not current normal acceleration. Engagement looks unconditionally beneficial.

**B — Control-algorithm flaw**

The desired-acceleration command is driven purely by pitch-rate tracking error. No load-factor limiter anywhere in the desired-acceleration path.

**C — Feedback routing** — became a design change

Nz is measured, telemetered and recorded — and is not an input to the engagement-inhibit logic. The feedback exists; it does not reach the controller.

**D — Human-controller interaction**

Annunciation is concurrent with the transient, not ahead of it, so manual override arrives after the load peak (UCA-16, UCA-17).

**E — Issued but not executed as intended**

Handbook Step 4, part 2. Rate-limited surfaces and filtered position feedback: both controllers act on a surface state the aircraft no longer has.

**None of these five is a component failure.** Scenario C is the one that turned into a design change — and it is invisible to a method that starts from "what broke?".

◀ back to slide 8

# 23 What the scenario changed

*Requirements that did not exist before STPA Step 4.*

APPENDIX — NOT PRESENTED

| SR | New or revised safety requirement | From | Kind of change |
|---|---|---|---|
| SR-4 | The reconfiguration supervisor shall include current normal acceleration and its rate in the state on which the engage decision is made. | Scenario A, C | Process model |
| SR-28 | Engagement of the reconfigured law shall be inhibited, or entered in a reduced-authority mode, while normal acceleration exceeds 4 g. | Scenario A, B | Mode logic |
| SR-29 | The desired-acceleration command generated during the engagement transient shall be rate-limited so that predicted normal acceleration stays within 4 g. | Scenario B | Control law |
| SR-30 | Entry into reduced-authority engagement shall be annunciated to the pilot and downlinked to the telemetry station within 1 s. | Scenario C, D | HMI + telemetry |
| SR-12 | The mode-change annunciation shall lead, not accompany, the control-law transition wherever the transition is commanded by the supervisor rather than the pilot. | Scenario D | HMI timing |
| FTR-09 | No test point shall inject a surface fault while the aircraft is above 3 g, until SR-28 and SR-29 are verified on the simulator and on the HIL bench. | Scenario A–D | Flight-test card |

**FTR-09 is a test point we removed from the card. It is the clearest return on the analysis: a hazardous flight condition that will not be flown, with a written reason why.**

◀ back to slide 9

⊕ traceability

# The chain that has to hold

*Hazard → UCA → constraint → requirement → V&V → test case → flight-test point*

APPENDIX — NOT PRESENTED




| Hazard | UCA | SR | V&V / TC | What the test case has to demonstrate |
|---|---|---|---|---|
| H-1, H-5 | UCA-2 | SR-1 | VV-01 / TC-01 | Pitch authority is re-allocated and trim is recovered after a control-surface loss with airframe damage |
| H-1, H-5 | UCA-11 | SR-5 | VV-02 / TC-02 | Lateral-directional stability and bias removal are retained in a coordinated turn |
| H-5 | UCA-11 | SR-9, SR-17 | VV-05 / TC-05 | Roll authority is reassigned under a stuck aileron with reduced rudder |
| H-1, H-2 | UCA-12 | SR-1 | VV-08 / TC-08 | Adaptation converges and directional damping is retained under a pinned rudder |
| H-1 | UCA-2 | SR-7, SR-17 | VV-10 / TC-10 | Inertia change is identified online after structural detachment |
| H-2, H-4 | UCA-4 | SR-1, SR-28 | VV-11 / TC-11 | Engagement is timely AND the load-factor bound is respected |

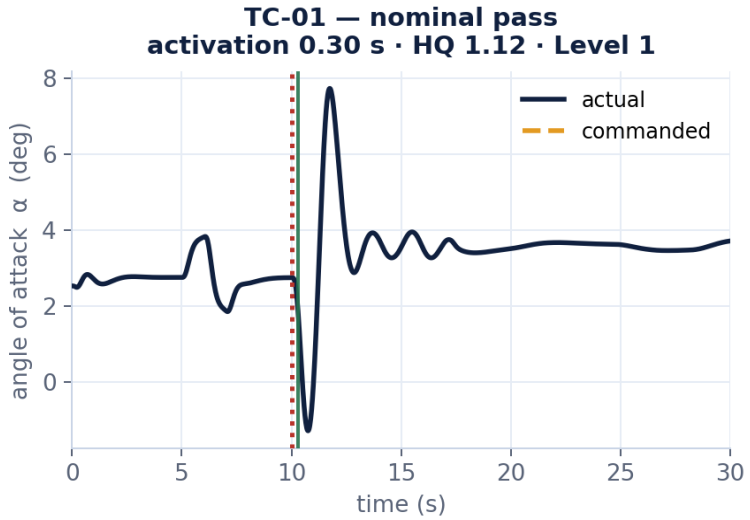
*TC-11 is the only row where the safety requirement had two clauses. It passed the first and failed the second — which is exactly why the row is worth having.*

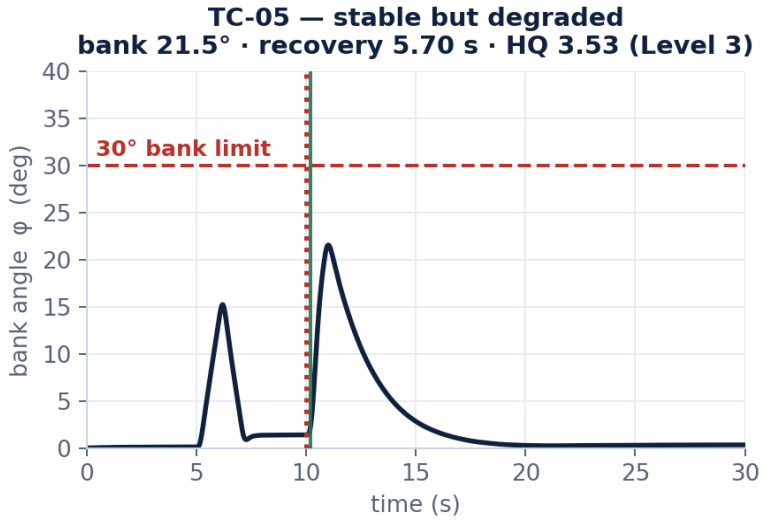
◀ back to slide 9

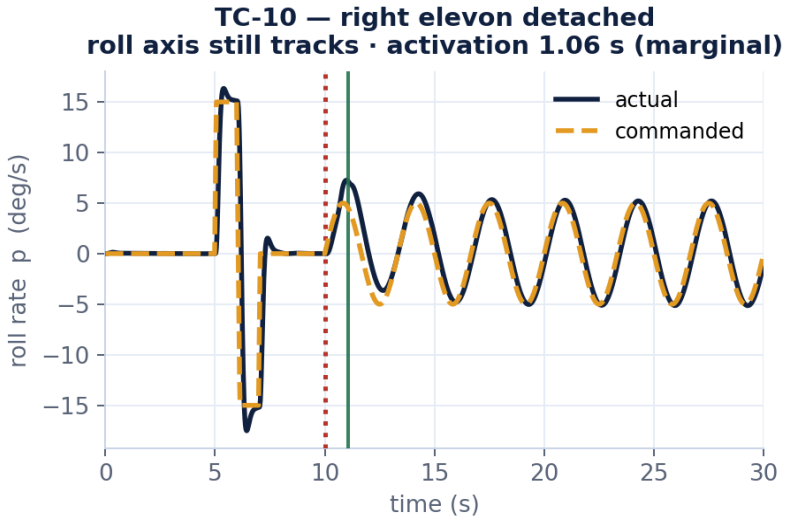
# Appendix — the other three test cases

*TC-01 nominal pass, TC-05 degraded handling, TC-10 marginal timing after structural loss.*

APPENDIX — NOT PRESENTED




**TC-01 — nominal pass.** Right elevator stuck at +7.5° with CG shift and right-wing damage. Angle of attack returns to the commanded trim inside the tracking band; activation 0.30 s, no residual oscillation, Level-1 handling (HQ 1.12). Pitch authority is redistributed to the left elevator and differential ailerons.

**TC-05 — stable but degraded.** Left aileron stuck at −15° with 25% right-rudder loss. Bounded and stable — bank peaks at 21.5° with no oscillation — but roll recovery takes 5.70 s, just past the 5 s line, for a Level-3 rating (HQ 3.53).

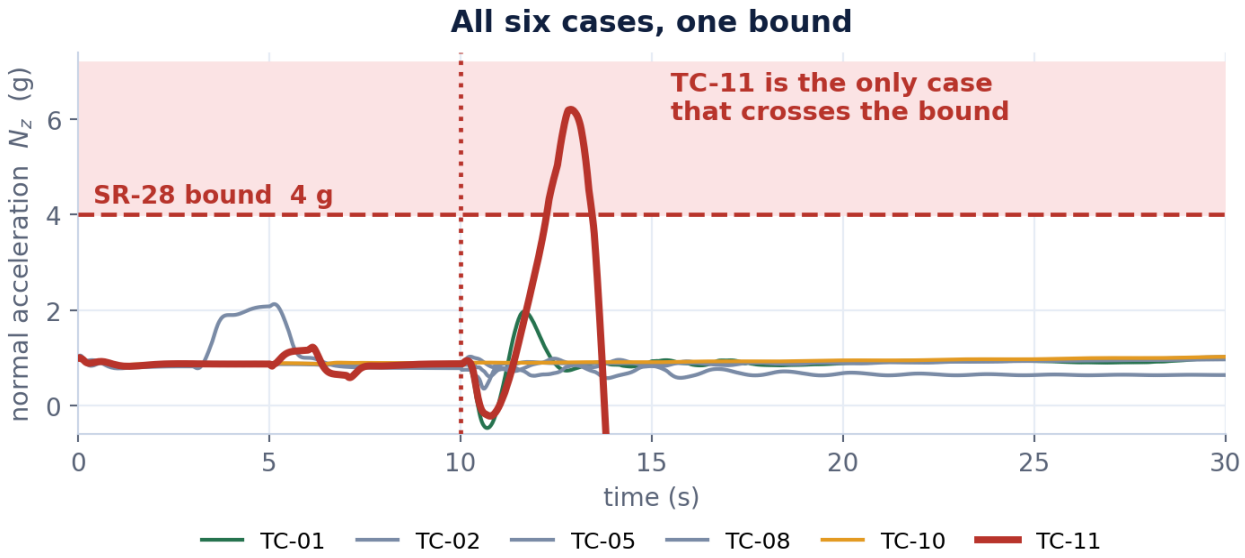
**TC-10 — marginal success.** Right elevon detached, $\Delta I^2$ = +150 kg·m². The roll axis still tracks the commanded sinusoid cleanly and the UKF identifies the inertia change within 30 s, but activation (1.06 s) and recovery (5.12 s) each miss their deadlines by about a tenth of a second.

◀ back to slide 10

# Appendix — the randomized envelope sweep

*Each fault re-injected across 8 500–12 000 m and 230–270 m/s, 1000 runs per case.*

APPENDIX — NOT PRESENTED




## The decisive statistic

The TC-11 elevator jam departs the validated envelope in 100% of sampled conditions, with a median peak load near 6 g.

**Every other case never departs and never exceeds 4 g.**

That is what rules out “unlucky trim point” as an explanation, and what justifies deleting the flight-test point rather than moving it.

**Reading the overlay.** All six deterministic cases are plotted on one load-factor axis against the SR-28 bound. Five of them sit at or below about 2 g for the whole run; TC-11 is the single trace that crosses 4 g, and it does so AFTER a reconfiguration that met its activation deadline. The Monte-Carlo composites behind this slide — recovery-time distribution and handling quality against fault severity — are in the paper as Figs. 5 and 6.

◀ back to slide 13

# 27 References and provenance


Leveson, N. G. and Thomas, J. P. (2018). STPA Handbook. MIT, Cambridge, MA.

Thomas, J. P. (2019). Common Mistakes in STPA and CAST. MIT PSAS, revised October 2019.

Nguyen, L. T., Ogburn, M. E., Gilbert, W. P., Kibler, K. S., Brown, P. W. and Deal, P. L. (1979). Simulator Study of Stall/Post-Stall Characteristics of a Fighter Airplane with Relaxed Longitudinal Static Stability. NASA Technical Paper 1538.

Chowhan, K. S. (2024). Vision-Based Fault Detection and Intelligent Control Reconfiguration of an Impaired Fighter Aircraft. PhD thesis, IIT Bombay.

Chowhan, K. S. et al. (2022). Design of intelligent reconfigurable control laws towards loss-of-control prevention of an impaired high-performance fighter aircraft. 4th ICECIE. doi:10.1109/ICECIE55199.2022.10000337

Chowhan, K. S. et al. (2022). Real-time simulation-based handling-quality assessment of an impaired fighter aircraft with intelligent reconfigurable control laws. IEEE CONECCT. doi:10.1109/CONECCT55679.2022.9865771

IEEE Std 1012-2016. System, Software and Hardware Verification and Validation.

MIL-STD-1797B (2022). Flying Qualities of Piloted Aircraft. · MIL-STD-882E (2012). System Safety. · SAE ARP4754A (2010).


*Full UCA table, controller constraints, loss scenarios and test matrix are provided with these slides for the workshop archive.*