AIRCRAFT CERTIFICATION ASSUMPTIONS AND STPA

MIT STAMP WORKSHOP 2024

Presented by:

Dr John Thomas (MIT)
Kyle Ryan (The Boeing Company)
Dave Cummins (Bell Textron Inc)

Credit also to Aaron Katz (NATCA)

TRANSPONDER & TCAS DIAGRAM

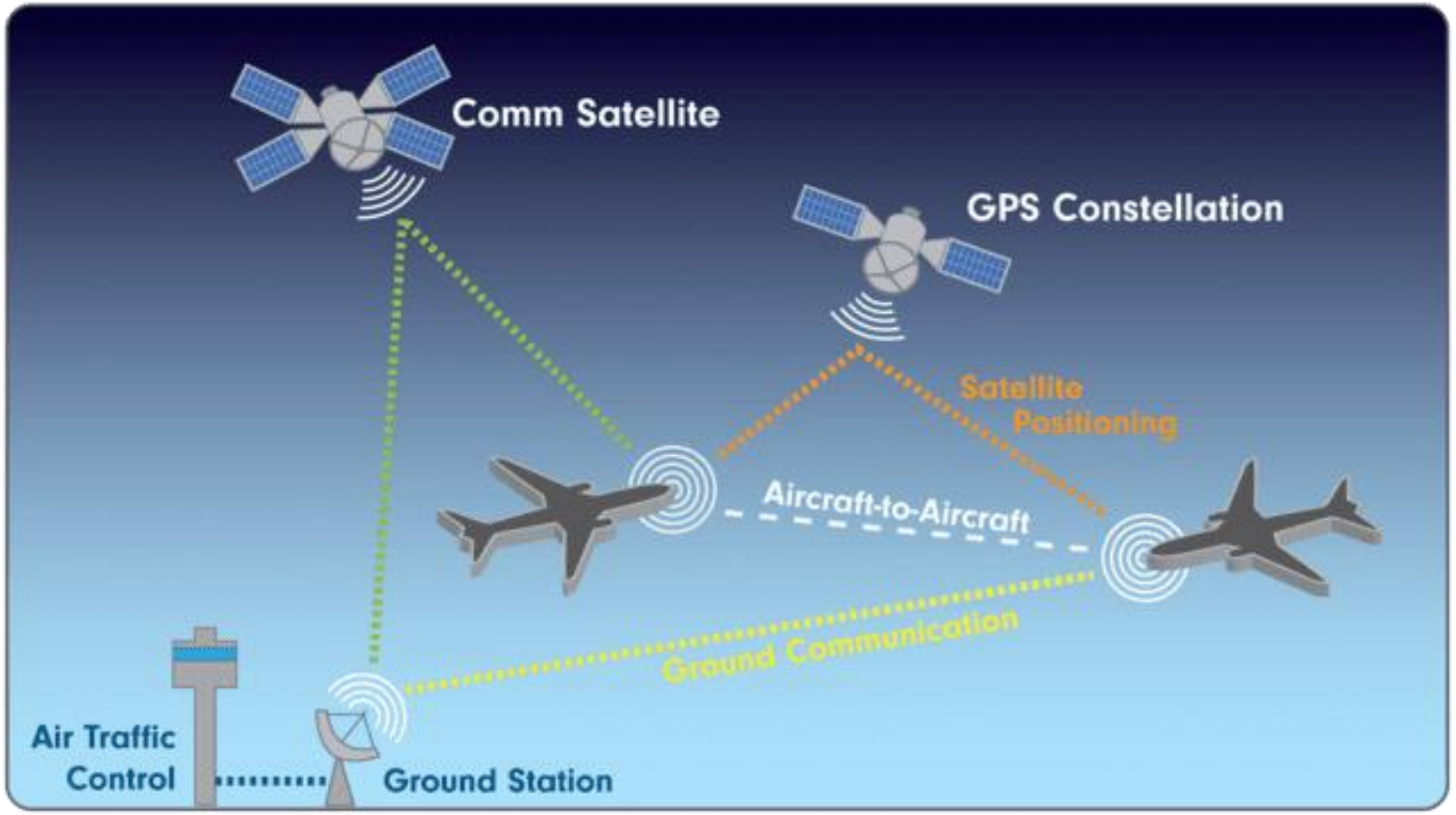


Image ref: airfactsjournal.com

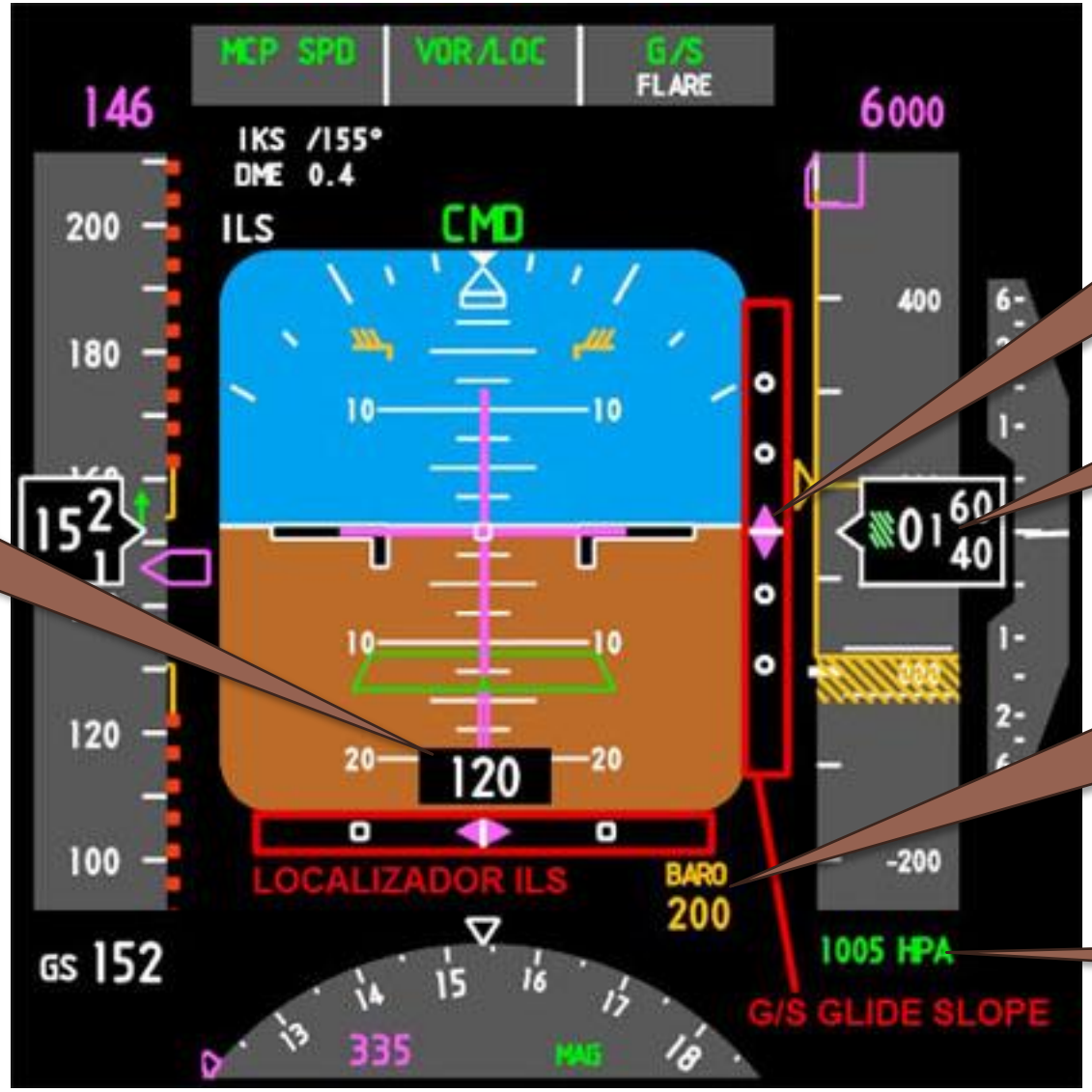
- Secondary surveillance RADAR
- Provides primary flight details to ATC Controller
- Provides proximity alerts of other aircraft to flight crew
- Data based on aircraft systems and navigation trace

AIR TRAFFIC CONTROL (ATC) SCREEN VIEWS

Image ref: FAA.gov/air_traffic

Image ref: aviation.stackexchange.com

PILOT'S PRIMARY FLIGHT DISPLAY (PFD)



ILS (Instrument Landing System) Glideslope

Barometric altitude

Radio Altitude (RA) (appears below certain height)

Approach minimums for visual acquisition of runway (depends on approach category)

QNH Setting

Image ref: https://www.aircraftnerds.com/2018/11/how-does-pilot-land-plane.html#google_vignette

EXAMPLES FROM TRADITIONAL CERTIFICATION PROCESS

SOME TRANSPONDER FAILURE CONDITIONS

Failure Condition	Flight Phase	Env	Failure Effects	Class	Assumptions
Loss of transponder data to ATC	All phases	IFR	Loss of aircraft transponder data on ATC screen. Slight reduction in safety margins and increase in flight crew workload to maintain safe separation.	MIN	ATC and flight crew will recognize a loss of transponder data and revert to an existing procedure/primary radar.
Malfunction of transponder data to ATC			Incorrect aircraft transponder data displayed on ATC screen. Misleading position data presented to controller. Significant reduction in safety margins and increase in flight crew workload to maintain safe separation.	MAJ	ATC and flight crew conduct regular cross-check of assigned flightpaths/levels which will identify incorrect transponder data to the flight crew/ATC. This failure may significantly mislead the controller/flight crew or may take some time to be recognized (delayed awareness of failure).

The assumptions bound the failure effects, classifications and design level or rigor.

But are they valid?

The overall assumption here is that the aircraft will not violate safe separation constraints!

TRADITIONAL REQUIREMENTS GENERATED

Reliability and level of rigor

- Loss of Transponder shall occur less than or equal to 1E-5 failures per flight hour
- Malfunction of Transponder shall occur less than or equal to 1E-5 failures per flight hour
- Transponder shall be developed to at least DAL C

MAJOR FAILURE CONDITION

Training and policy

- Flight manual instructions, likely to follow an established procedure in the event of loss/malfunction
- Regular simulator training requirement for flight crews to practice lost transponder scenarios
- Flight crew and ATCO readback of assigned squawk codes and instructions – to highlight errors

(1) The level of reliability, redundancy, and design rigor is reduced by the assumptions made in the failure condition assessment!
(2) There is absolutely nothing about the ATC controller, or their equipment in these requirements!

CAN STPA HELP? STPA EXAMPLE…

STPA STEP 1: LOSSES AND HAZARDS

L1: Loss of life or serious injury to aircraft occupants

H1: Aircraft violates minimum separation from other traffic.

H2: Aircraft violates minimum separation from terrain.

L2: Destruction of/ physical damage to aircraft structure

H1: Aircraft violates minimum separation from other traffic.

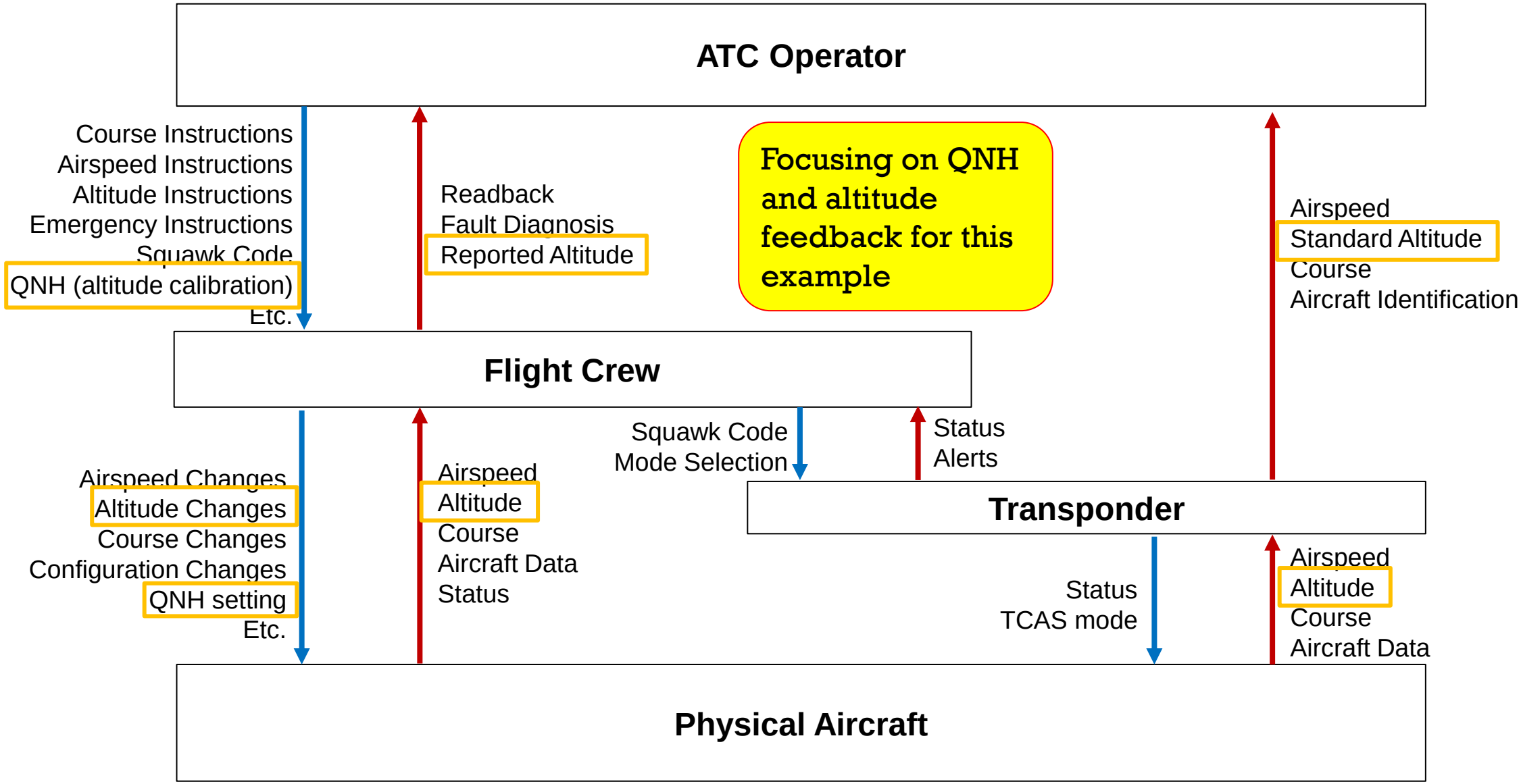
H2: Aircraft violates minimum separation from terrain.

L3: Monetary loss due to airspace infringement

H1: Aircraft violates minimum separation from other traffic.

H2: Aircraft violates minimum separation from terrain.

STPA STEP 2: CONTROL STRUCTURE



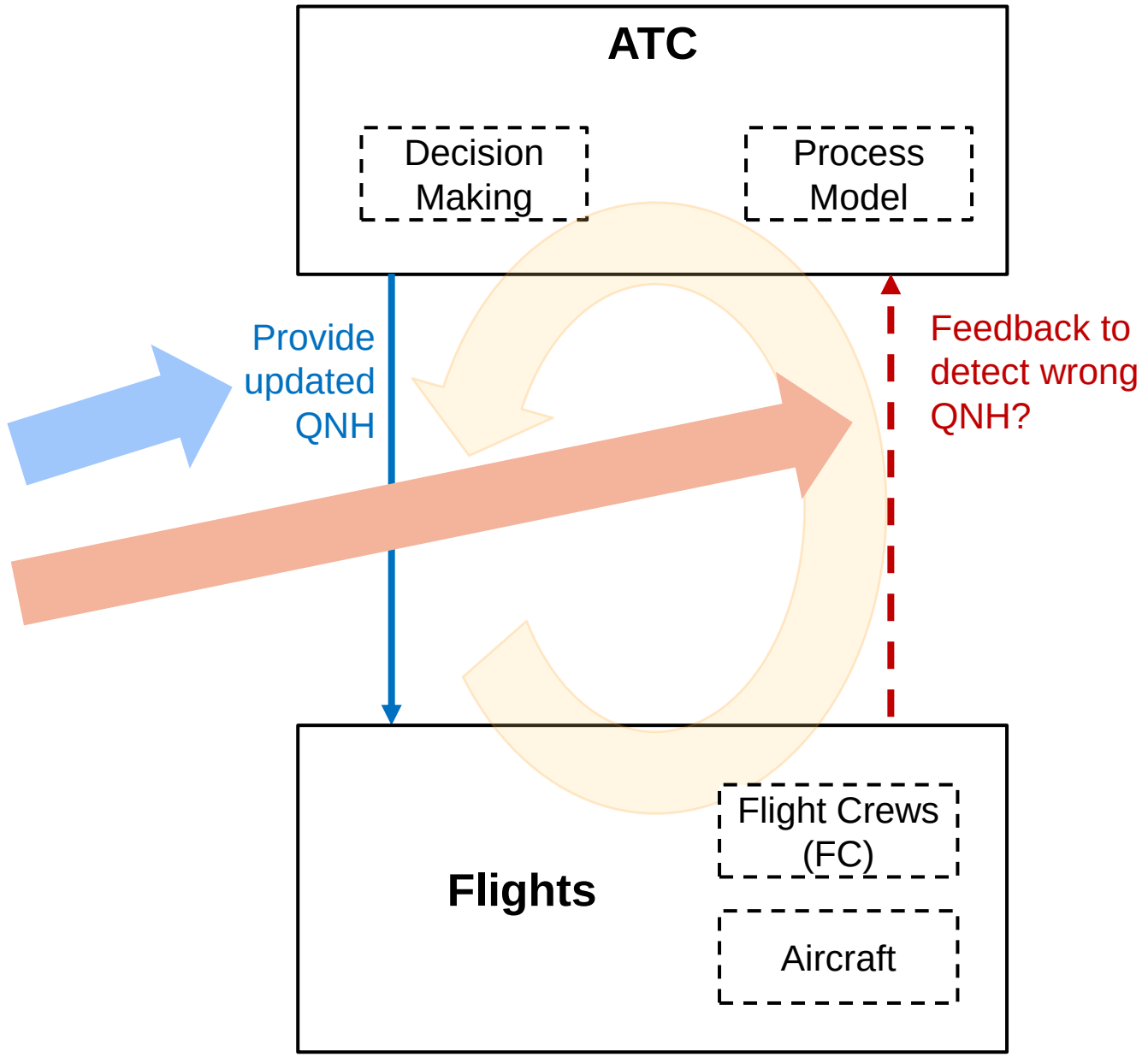
STPA STEP 3: IDENTIFY UNSAFE CONTROL ACTIONS (UCAS)

Controller	Control Actions	Not Providing Causes Hazard	Providing Causes Hazard	Too early, Too late, Out of order	Stopped too soon, Applied too long
ATC	Provide QNH	**ATC does not provide updated QNH when FC is using outdated QNH**	ATC provides incorrect QNH that does not match environmental conditions	ATC provides QNH too late after crew executes maneuvers based on wrong QNH	ATC continues providing incorrect QNH too long after conditions have changed
FC	Set QNH	FC does not Set QNH when aircraft is using outdated QNH	FC provides incorrect QNH setting that does not match environmental conditions	FC provides QNH setting too late after conditions have changed	FC continues using incorrect QNH too long after environmental conditions do not match QNH
ATC	Issue Control Instructions	ATC does not Issue Control Instructions when the aircraft is in controlled airspace	ATC Issue Control Instructions for aircraft not in the current sector ATC Issue Control Instructions in a way to creates a conflict with another aircraft	ATC Issue Control Instructions too late after a conflict arises	ATC continues Issue Control Instructions too long after … ATC stops Issue Control Instructions too soon before…
FC	Course Change	FC do not provide Course Change from conflicted flight path in current sector. [H1, H2].	FC provide Course Change to conflicted flight path in current sector. [H1, H2].	FC provide Course Change too late to after conflict with other traffic is irrecoverable. [H1, H2].	FC stops Course Change too soon leaving the aircraft on a conflicting flight path. [H1, H2].

UCA: ATC does not provide

updated QNH

when FC is using outdated QNH



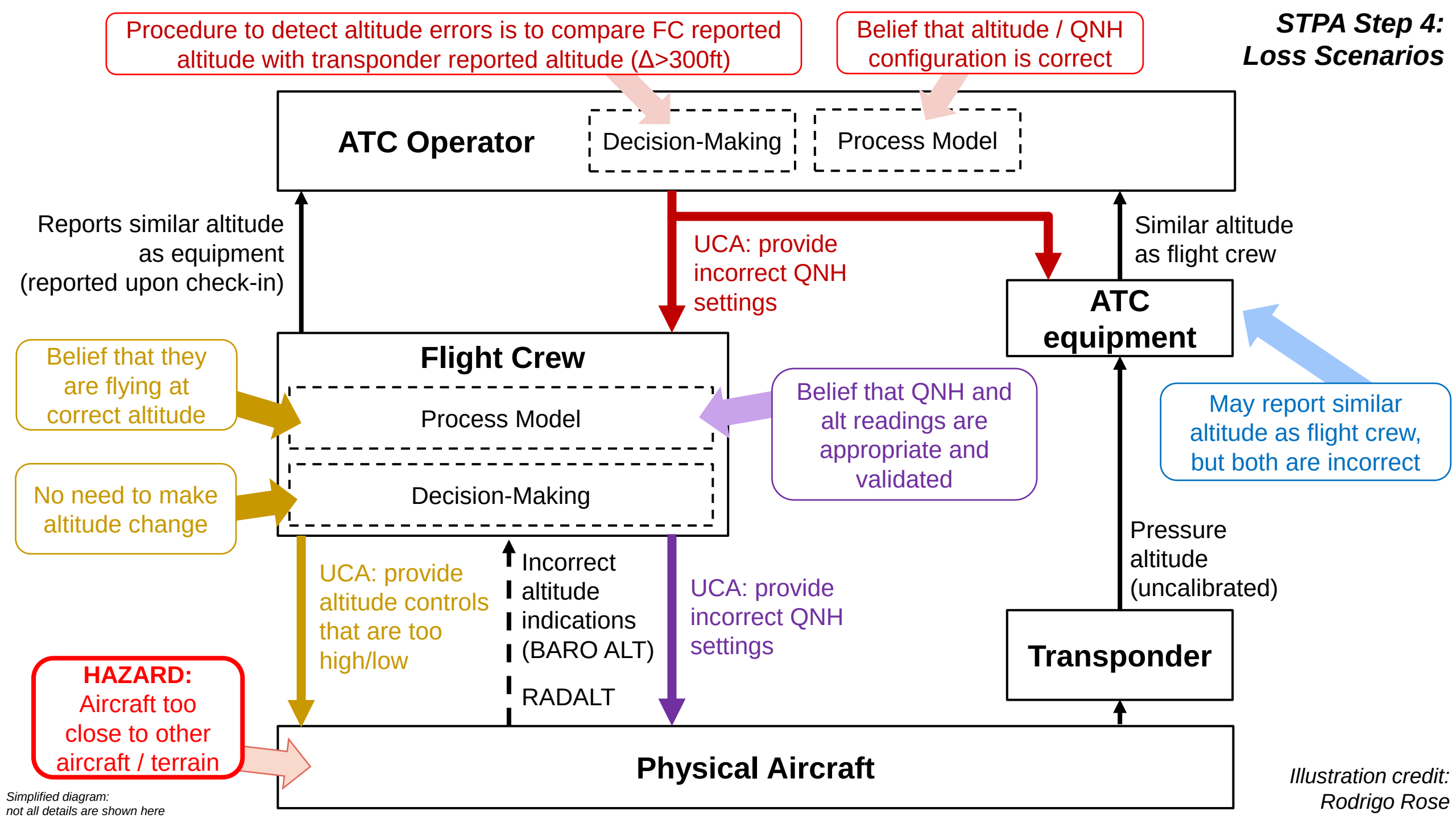
STPA STEP 3: IDENTIFY UNSAFE CONTROL ACTIONS (UCAS)

Controller	Control Actions	Not Providing Causes Hazard	Providing Causes Hazard	Too early, Too late, Out of order	Stopped too soon, Applied too long
ATC	Provide QNH	ATC does not provide updated QNH when FC is using outdated QNH	**ATC provides incorrect QNH that does not match environmental conditions**	ATC provides QNH too late after crew executes maneuvers based on wrong QNH	ATC continues providing incorrect QNH too long after conditions have changed
FC	Set QNH	FC does not Set QNH when aircraft is using outdated QNH	FC provides incorrect QNH setting that does not match environmental conditions	FC provides QNH setting too late after conditions have changed	FC continues using incorrect QNH too long after environmental conditions do not match QNH
ATC	Issue Control Instructions	ATC does not Issue Control Instructions when the aircraft is in controlled airspace	ATC Issue Control Instructions for aircraft not in the current sector ATC Issue Control Instructions in a way to creates a conflict with another aircraft	ATC Issue Control Instructions too late after a conflict arises	ATC continues Issue Control Instructions too long after … ATC stops Issue Control Instructions too soon before…
FC	Course Change	FC do not provide Course Change from conflicted flight path in current sector. [H1, H2].	FC provide Course Change to conflicted flight path in current sector. [H1, H2].	FC provide Course Change too late to after conflict with other traffic is irrecoverable. [H1, H2].	FC stops Course Change too soon leaving the aircraft on a conflicting flight path. [H1, H2].

STPA STEP 3: IDENTIFY UNSAFE CONTROL ACTIONS (UCAS)

Controller	Control Actions	Not Providing Causes Hazard	Providing Causes Hazard	Too early, Too late, Out of order	Stopped too soon, Applied too long
ATC	Provide QNH	ATC does not provide updated QNH when FC is using outdated QNH	**ATC provides incorrect QNH that does not match environmental conditions**	ATC provides QNH too late after crew executes maneuvers based on wrong QNH	ATC continues providing incorrect QNH too long after conditions have changed
FC	Set QNH	FC does not Set QNH when aircraft is using outdated QNH	**FC provides incorrect QNH setting that does not match environmental conditions**	FC provides QNH setting too late after conditions have changed	FC continues using incorrect QNH too long after environmental conditions do not match QNH
ATC	Issue Control Instructions	**ATC does not Issue Control Instructions when a conflict arises**	**ATC Issue Control Instructions in a way to creates a conflict with another aircraft**	**ATC Issue Control Instructions too late after a conflict arises**	ATC continues Issue Control Instructions too long after … ATC stops Issue Control Instructions too soon before…
		ATC does not Issue Control Instructions when the aircraft is in controlled airspace	ATC Issue Control Instructions for aircraft not in the current sector		
FC	Course Change	**FC do not provide Course Change from conflicted flight path in current sector. [H1, H2].**	**FC provide Course Change to conflicted flight path in current sector. [H1, H2].**	**FC provide Course Change too late to after conflict with other traffic is irrecoverable. [H1, H2].**	FC stops Course Change too soon leaving the aircraft on a conflicting flight path. [H1, H2].

STPA Step 4: Loss Scenarios



Simplified diagram: not all details are shown here

Illustration credit: Rodrigo Rose

CHALLENGING ASSUMPTIONS

Traditional	Transponder Loss / malfunction recognized by FC and ATC	Existing procedures are adequate to maintain safe separation	FC workload is manageable (nothing else is going on)	Collision highly unlikely due to multiple layers: training, procedures, redundancy, etc.
STPA	ATC may believe transponder output is correct. Relaying incorrect instructions to FC plausible.	Multiple UCAs where unsafe actions may not be recognized by FC or ATC	Multiple scenarios where workload is higher than expected (non-standard ops)	Every UCA can be traced to a loss of separation

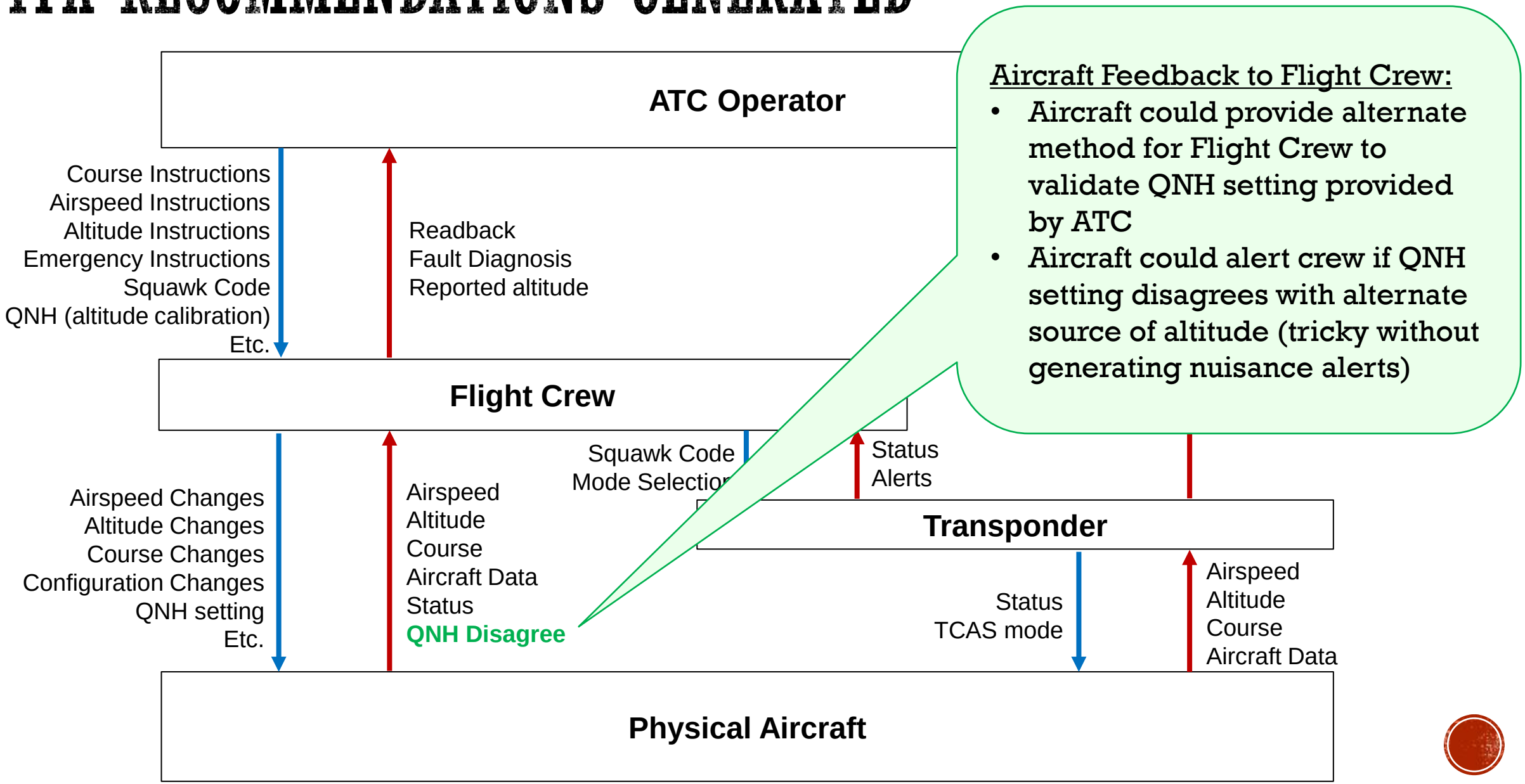
SO WHAT?

Remember our FHA hazard classifications?

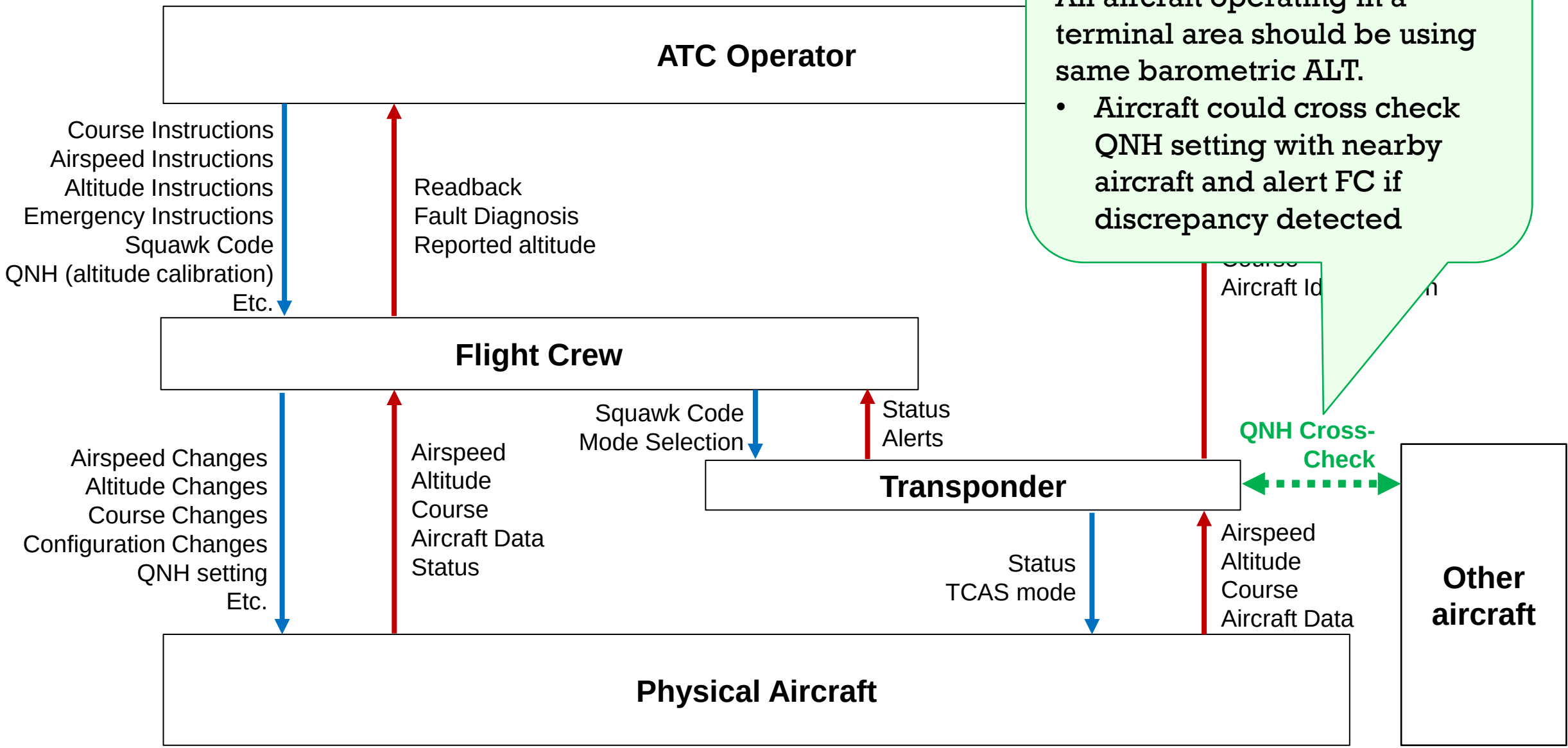
Failure Condition	Flight Phase	Env	Failure Effects	Class	Assumptions
Loss of transponder data to ATC	All phases	IFR	Loss of aircraft transponder data on ATC screen. Slight reduction in safety margins and increase in flight crew workload to maintain safe separation.	MIN	ATC and flight crew will recognize a loss of transponder data and revert to an existing procedure/primary radar.
Malfunction of transponder data to ATC			Incorrect aircraft transponder data displayed on ATC screen. Misleading position data presented to controller. Significant reduction in safety margins and increase in flight crew workload to maintain safe separation.	MAJ	ATC and flight crew conduct regular cross-check of assigned flightpaths/levels which will identify incorrect transponder data to the flight crew/ATC. This failure may significantly mislead the controller/flight crew or may take some time to be recognized (delayed awareness of failure).

- Would we consider driving up the severity with the loss / malfunction failure conditions? What would realistically be achieved?
- Could we introduce new functionality to provide better feedback?
- What would this new functionality be?
- Where in the traditional approach would we do this?

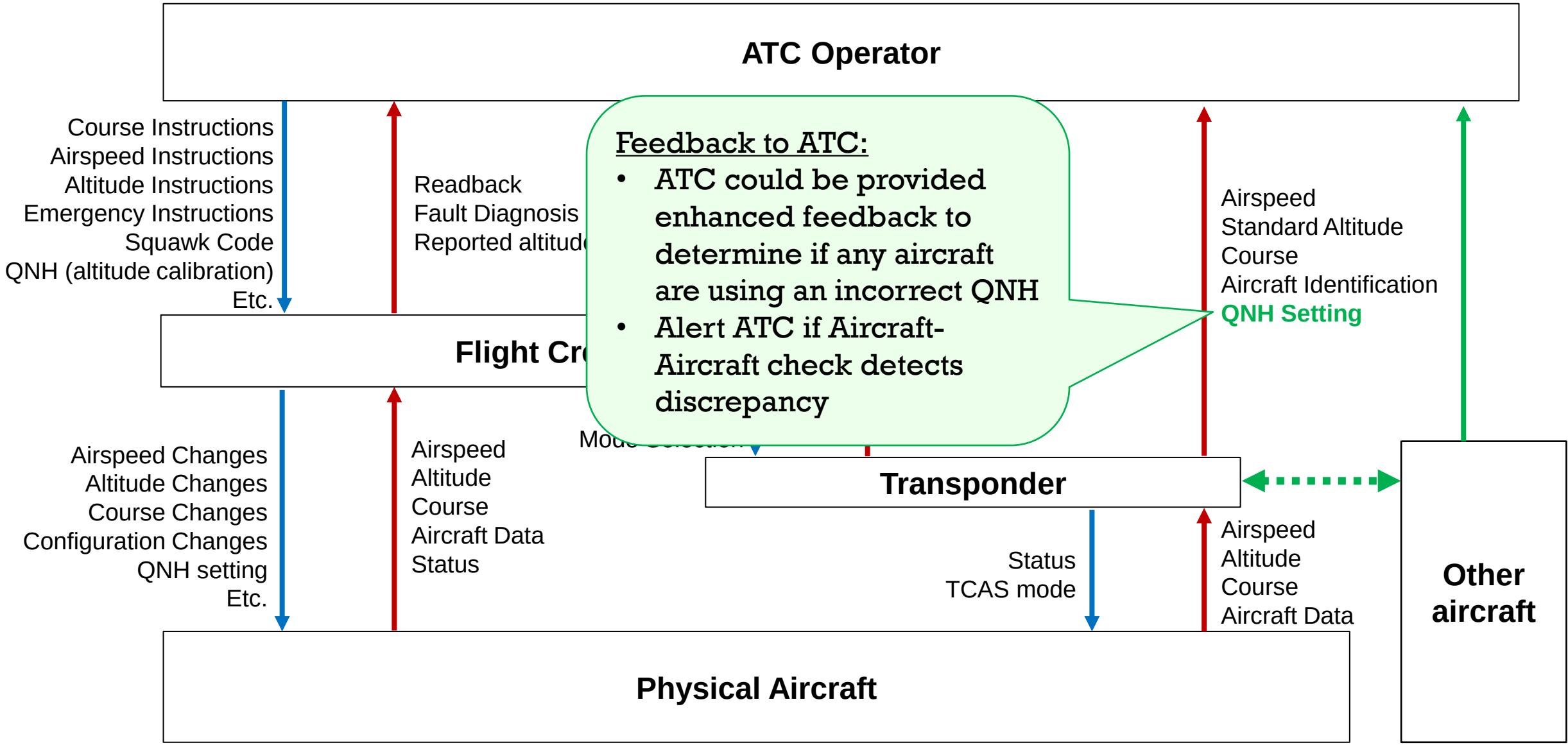
STPA RECOMMENDATIONS GENERATED



STPA RECOMMENDATIONS GENERATED

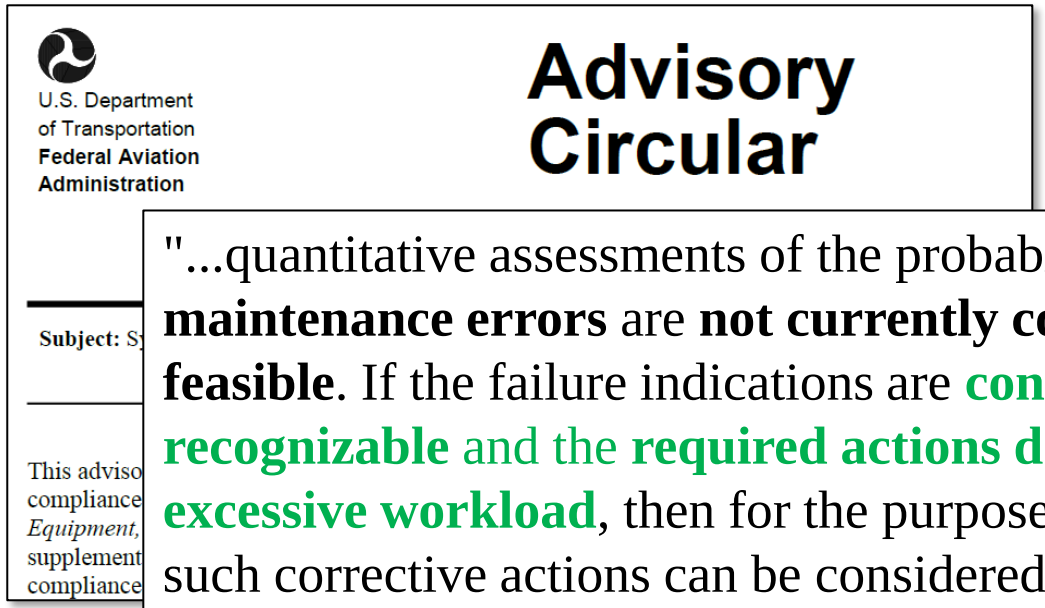


STPA RECOMMENDATIONS GENERATED



CAN STPA RESULTS HELP SUPPORT CERTIFICATION?

MEANS OF COMPLIANCE GUIDANCE (AC 25.1309-1B)


U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: S

This adviso
compliance
Equipment,
supplement
compliance

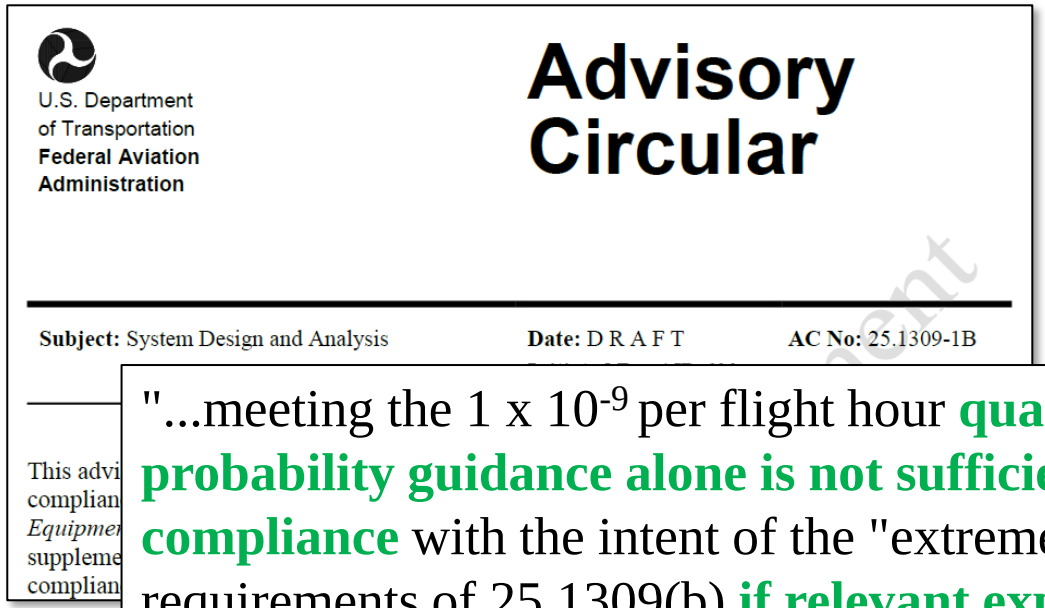
"...quantitative assessments of the probabilities of **crew or maintenance errors** are **not currently considered feasible**. If the failure indications are **considered to be recognizable** and the **required actions do not cause an excessive workload**, then for the purposes of the analysis, such corrective actions can be considered to be satisfactorily accomplished." (5-5)

"...Reasonable tasks are those that can be **realistically anticipated** to be **performed correctly** when they are required or scheduled." (8-1)

Questions STPA helps us consider:

- Recognizable to whom and with what training? Test pilot or line pilot?
- Excessive workload under what system conditions?
- How do we determine which tasks are reasonable? Are there situations in which tasks are not reasonable? (conflicting feedback, mental model flaws, etc)
- Realistic under which circumstances?
- What if tasks are not performed correctly?

MEANS OF COMPLIANCE GUIDANCE (AC 25.1309-1B)



U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: System Design and Analysis **Date:** D R A F T **AC No:** 25.1309-1B

This advi
complian
Equipmer
supplem
complian

"...meeting the 1 x 10^{-9} per flight hour **quantitative probability guidance alone is not sufficient to show compliance** with the intent of the "extremely improbable" requirements of 25.1309(b) **if relevant experience indicates the failure condition can occur**." (A-2)

Are these failure conditions or a loss of functionality?

- Subsystem intentionally deactivated for maintenance (MMEL)
- Transponder configured incorrectly
- ATC provides incorrect QNH
- Flight crew enters incorrect QNH
- Poor visibility inhibits crew's ability to visually confirm runway
- ILS down for maintenance
- ATC has no feedback to indicate QNH is incorrect

ATC SME comment on our UCAs: "I've seen all of these happen on a regular basis."

IN CONCLUSION

System Design and Analysis for Safety
AC 25.1309

Flightcrew Human Factors Assessment
AC 25.1302

IN CONCLUSION

System Design and Analysis for Safety
AC 25.1309

Flightcrew Human Factors Assessment
AC 25.1302

Total Systems Approach with STPA

QUESTIONS?

NOTE: The aviation system is very complex with many operational details and subtleties we didn't have time to address today.