A Systems Engineering Approach to Safety Performance Indicators and Accident Causality

Applying STAMP to Leading Indicators

Massachusetts Institute of Technology

Dr. John Thomas
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics
jthomas4@mit.edu

AIR SAFETY INVESTIGATORS

Captain Shem Malmquist, FRAeS
shem.malmquist@gmail.com

Predicting Accidents

- Desire to predict results in huge volumes of data collection in hopes something will pop out that is useful

- NASA was collecting 600 metrics/month prior to Columbia, none of which was helpful in predicting

Is enough data possible?

- Is it predictive?
  - Iceberg theory
  - Data rates

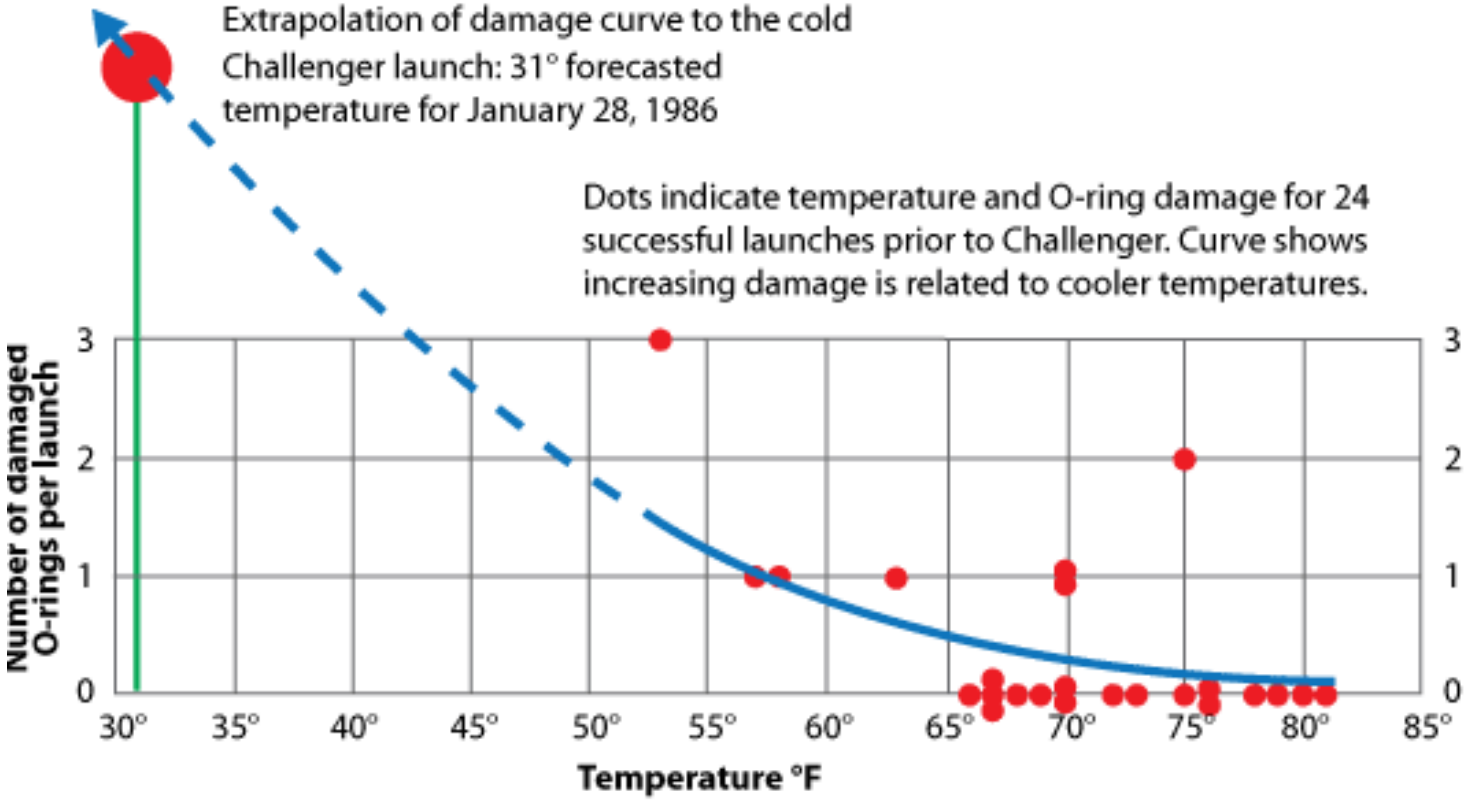
  - Predict accidents or just deviations as systems have become increasingly complex?

Complex accidents

- Multiple interactions and feedback mechanisms
- Tightly coupled and intractable
- Resistant to linear interpretation

Limitations of current methods

- Probability hazard analysis (PHA, FTA, FMEA, etc)
  - Limitations of Likelihood
  - Limits of event sets
  - Can exacerbate inherent bias



Cognitive bias can limit search

- Simple searches
- Confirmation bias
- Simple dramatic rather than chronic or cumulative
- Incomplete search for causes
- Defensive avoidance

Assumptions in Safety

1. Models and assumptions used in design were correct;
2. System will be constructed and operated as assumed by engineers
3. Original models and assumptions are not violated by
   A. changes over time
   B. changes in environment

Preventing Accidents

- Accidents occur when assumptions are wrong
  - Originally incorrect
  - Became incorrect over time
- Leading indicators of increasing risk can be identified based on the assumptions underlying the safety design process for the specific organization, product or operation

Aviation is an engineered system

- All engineering involves assumptions about behavior of the operational system and its environment
  - including organizational or management structure

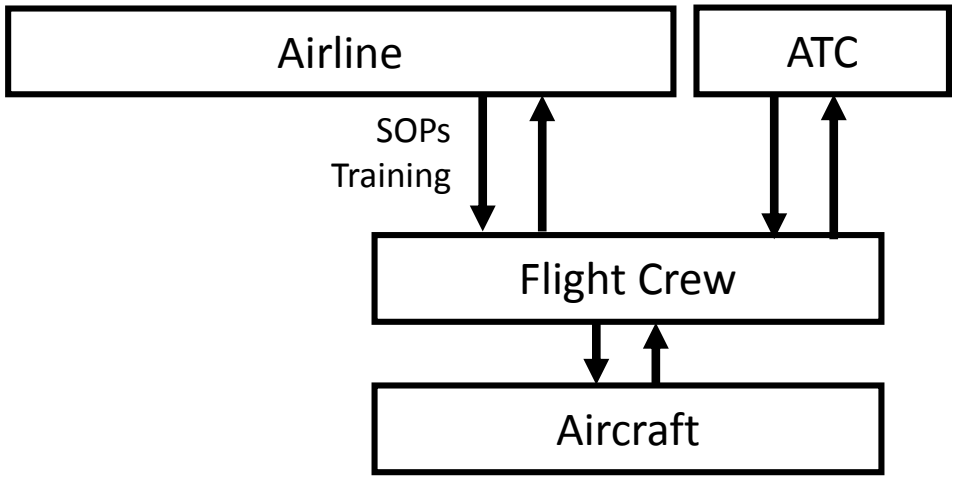
A Solution

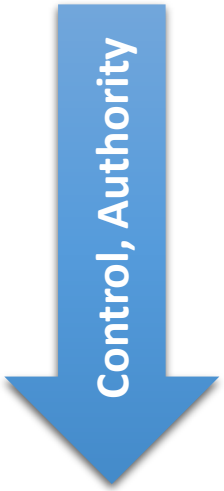
Systems Approach to Leading Indicators

1. Identify vulnerabilities
2. Identify existing controls and assumptions
3. Develop indicators
4. Plan future actions

Leveson, 2015; Scarinci & Giusti, 2016; Thomas, 2018

Control Structure model





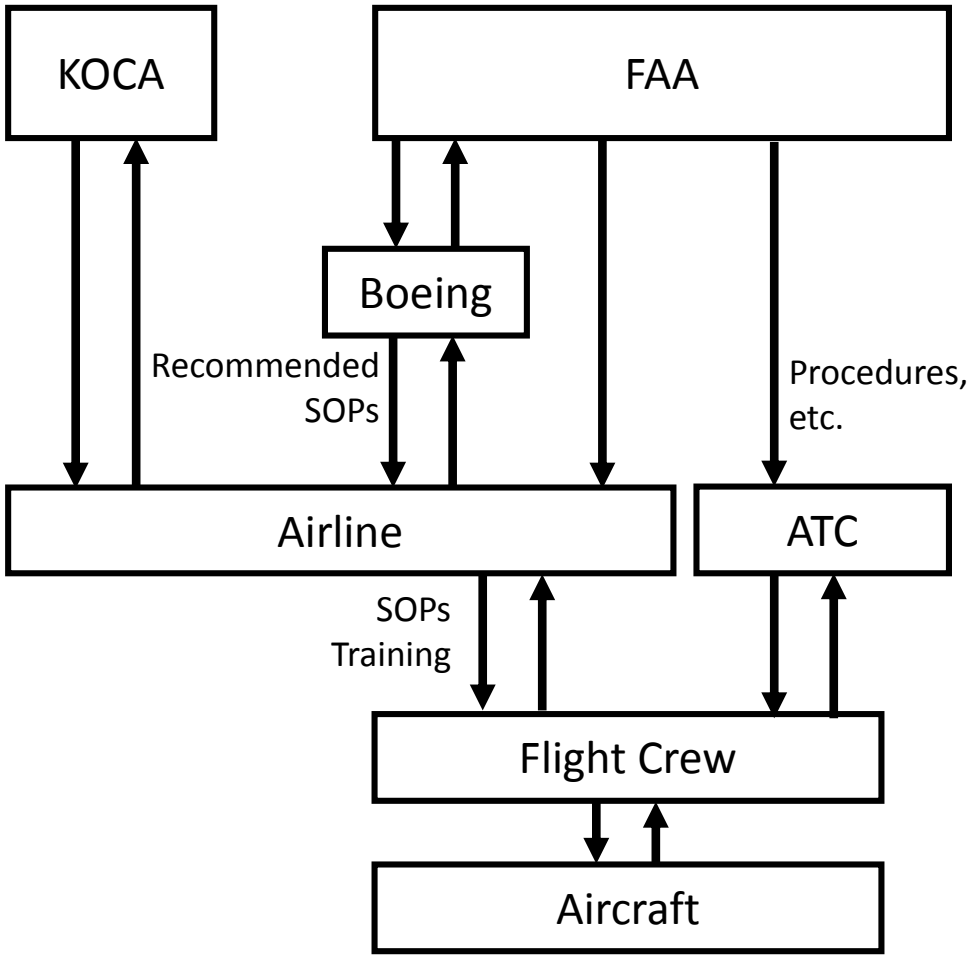
Social

Technical

Control Structure model

Operations

Development and Airworthiness



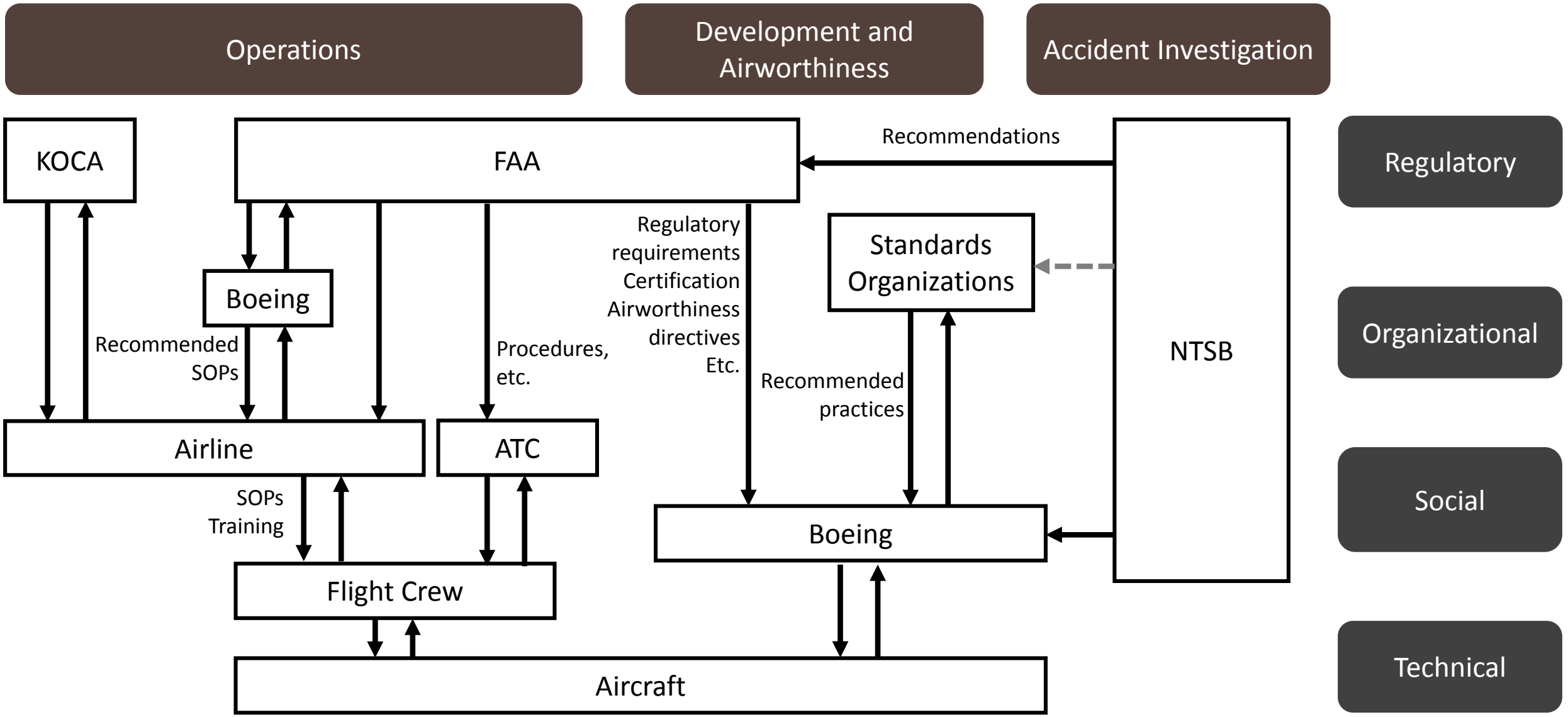
Regulatory

Organizational

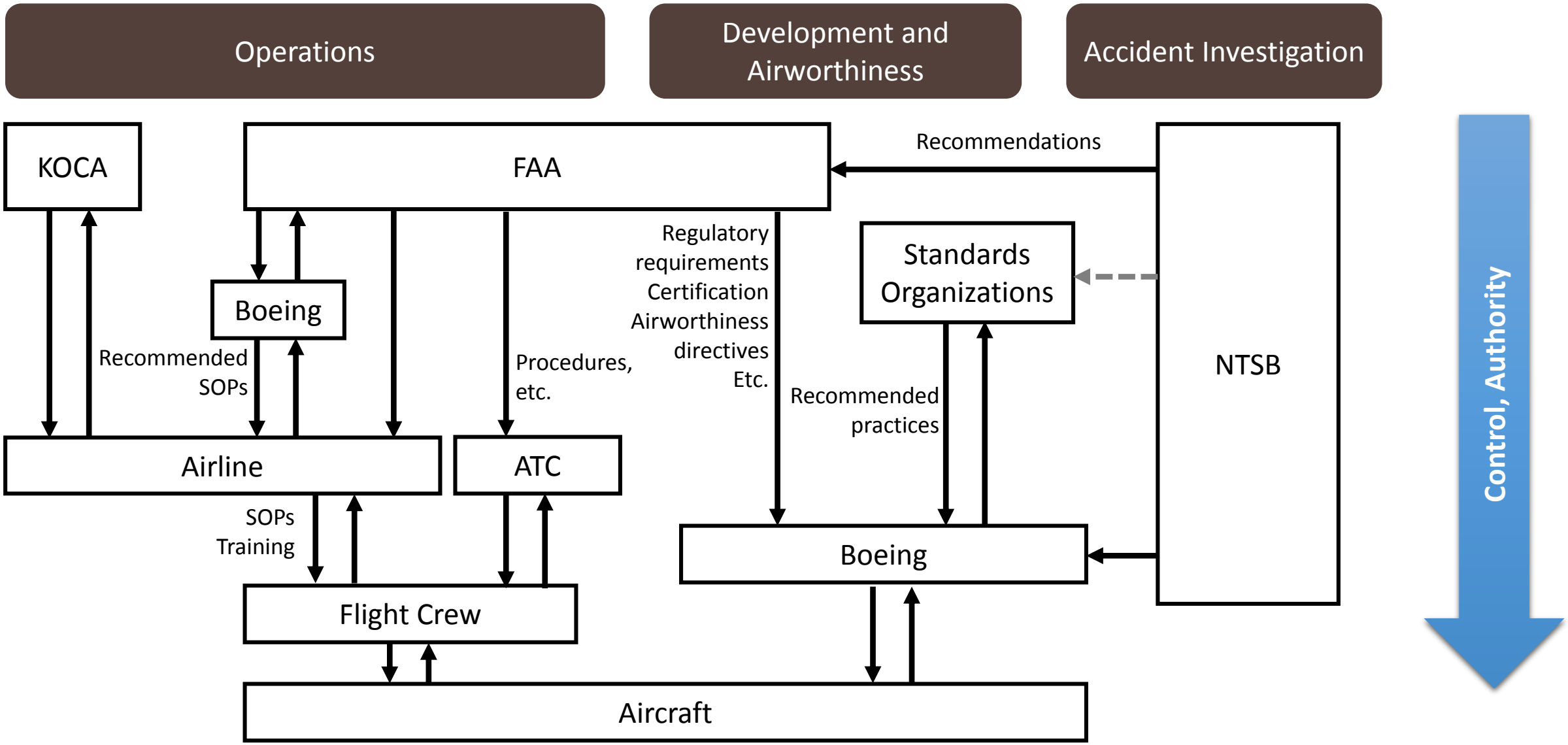
Social

Technical

Control Structure model



Control Structure model



A Solution

Systems Approach to Leading Indicators

1. Identify vulnerabilities
2. Identify existing controls and assumptions
3. Develop indicators
4. Plan future actions

Leveson, 2015; Scarinci & Giusti, 2016; Thomas, 2018

1) Identify vulnerabilities

CAST: Causal Analysis using System Theory

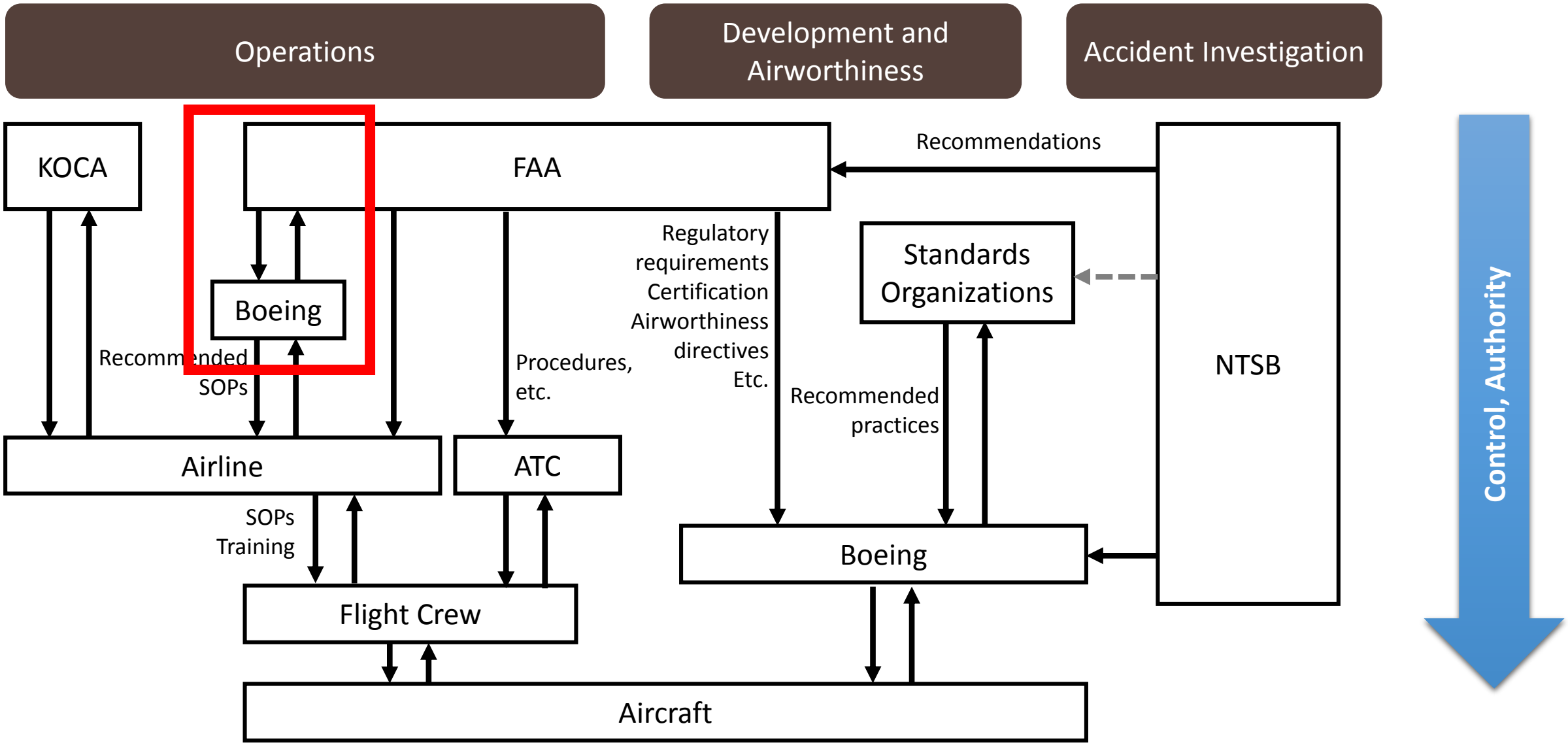
Systematically analyze past events

STPA: System Theoretic Process Analysis

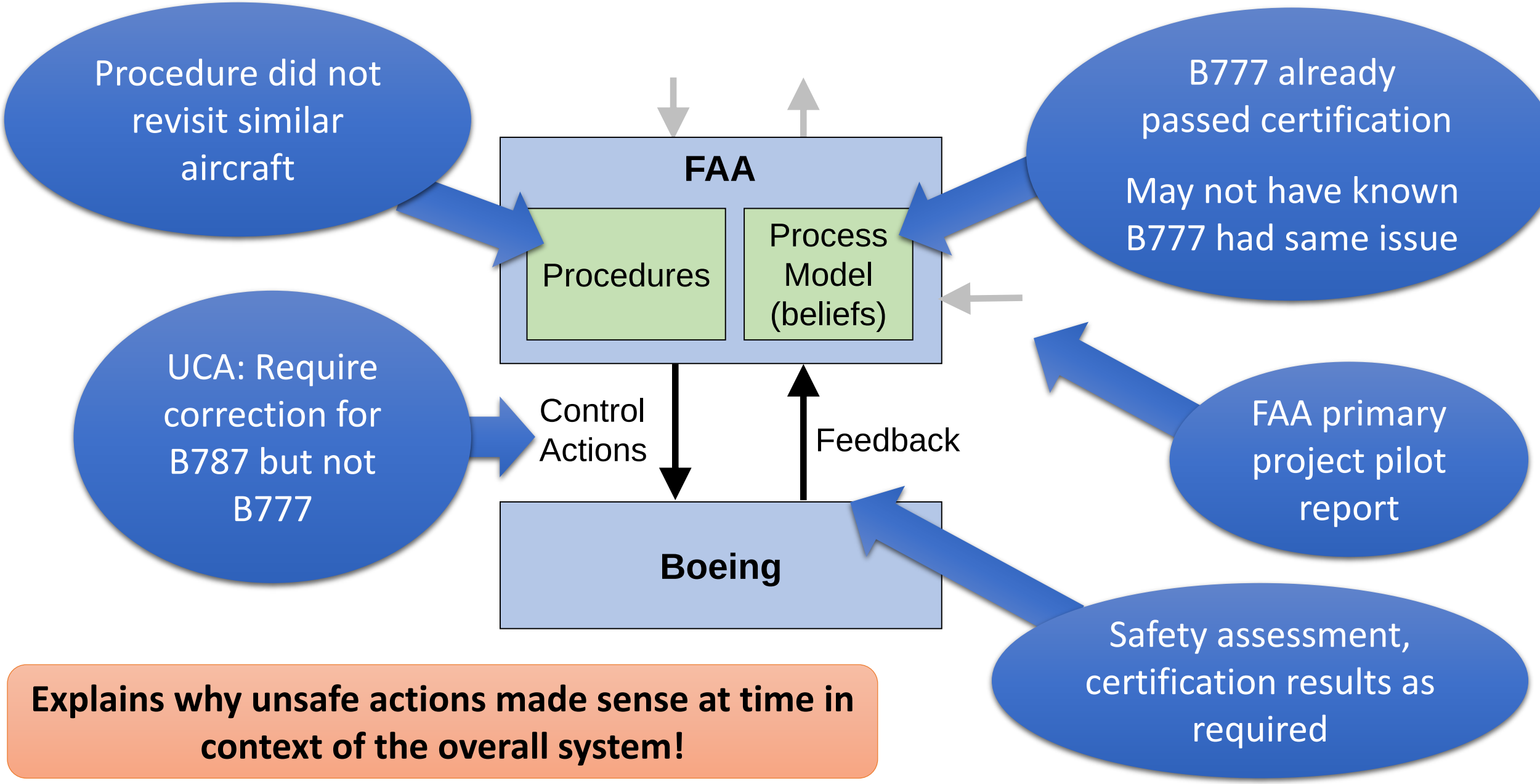
Prospective analysis of future problems

Leveson, 2012; Leveson and Thomas, 2018

CAST Example (Past Events)

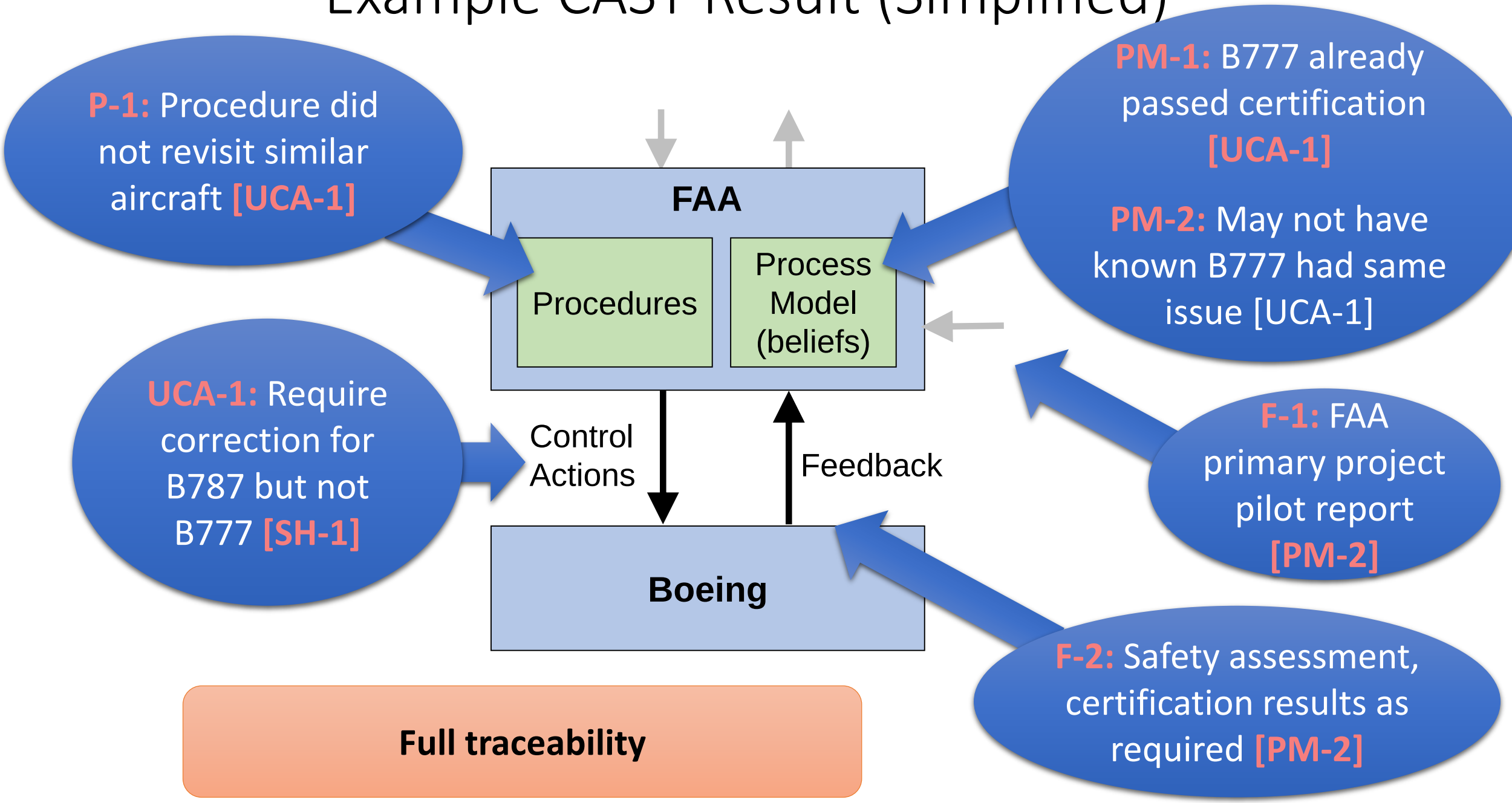


Example CAST Result (simplified)

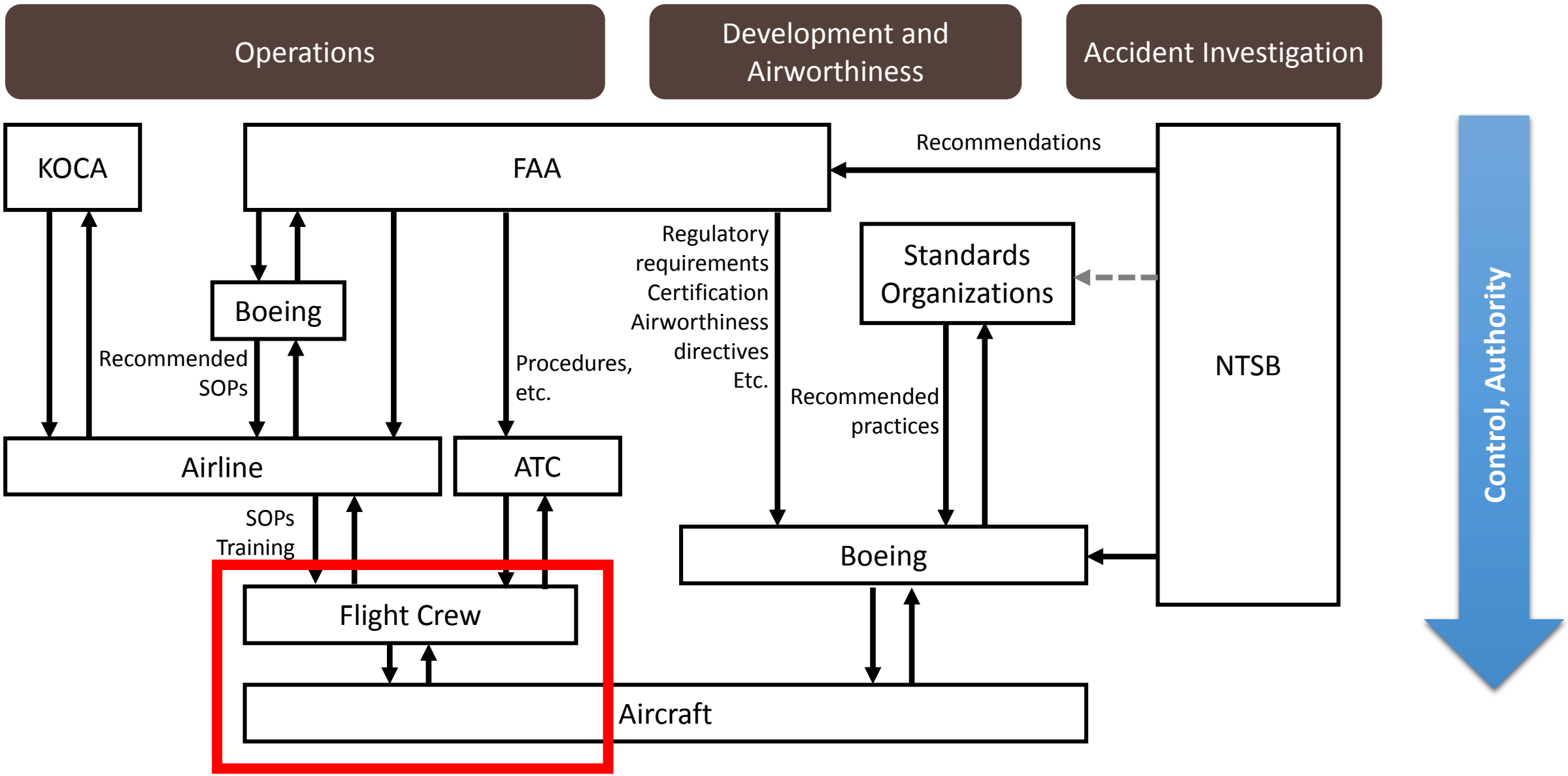


Explains why unsafe actions made sense at time in context of the overall system!

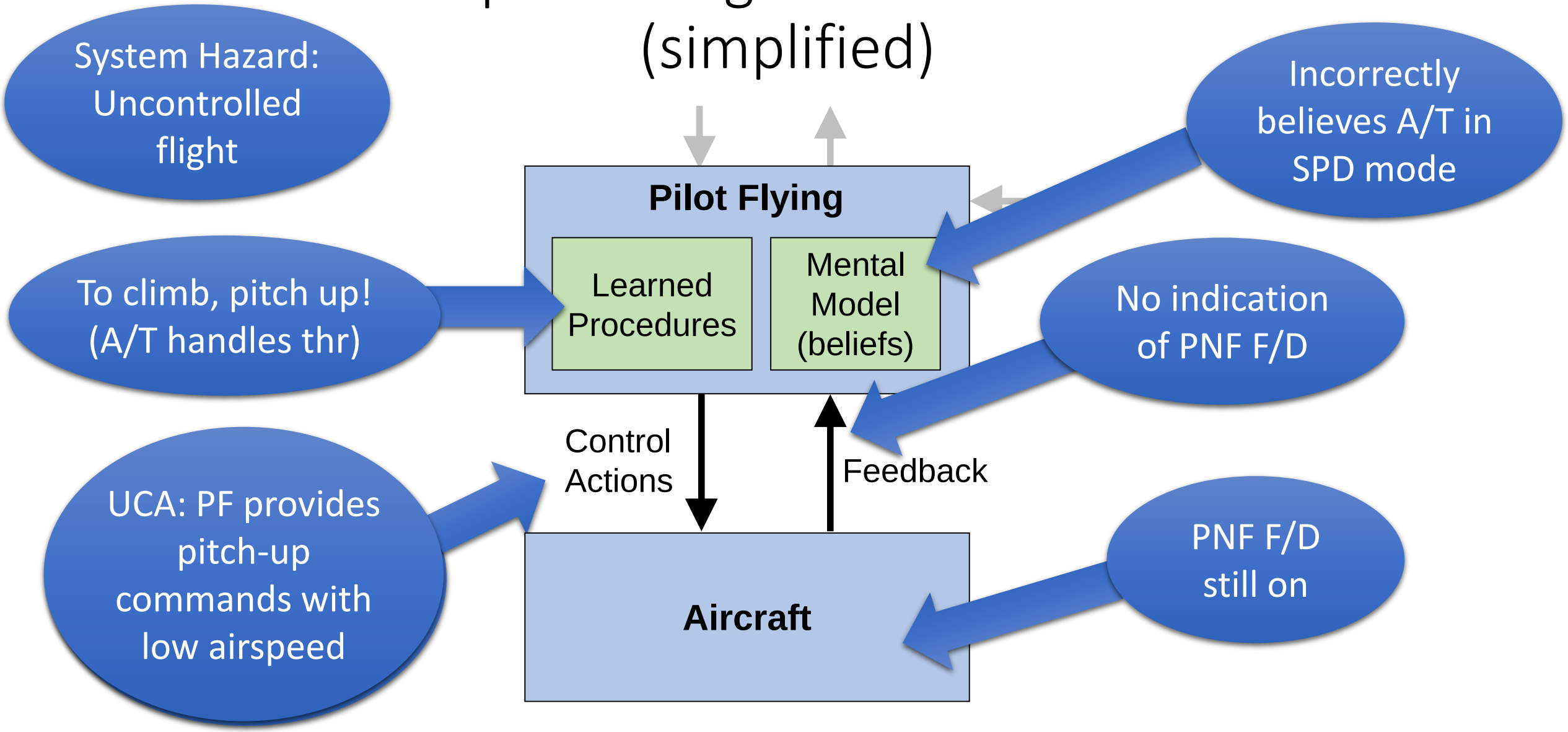
Example CAST Result (Simplified)



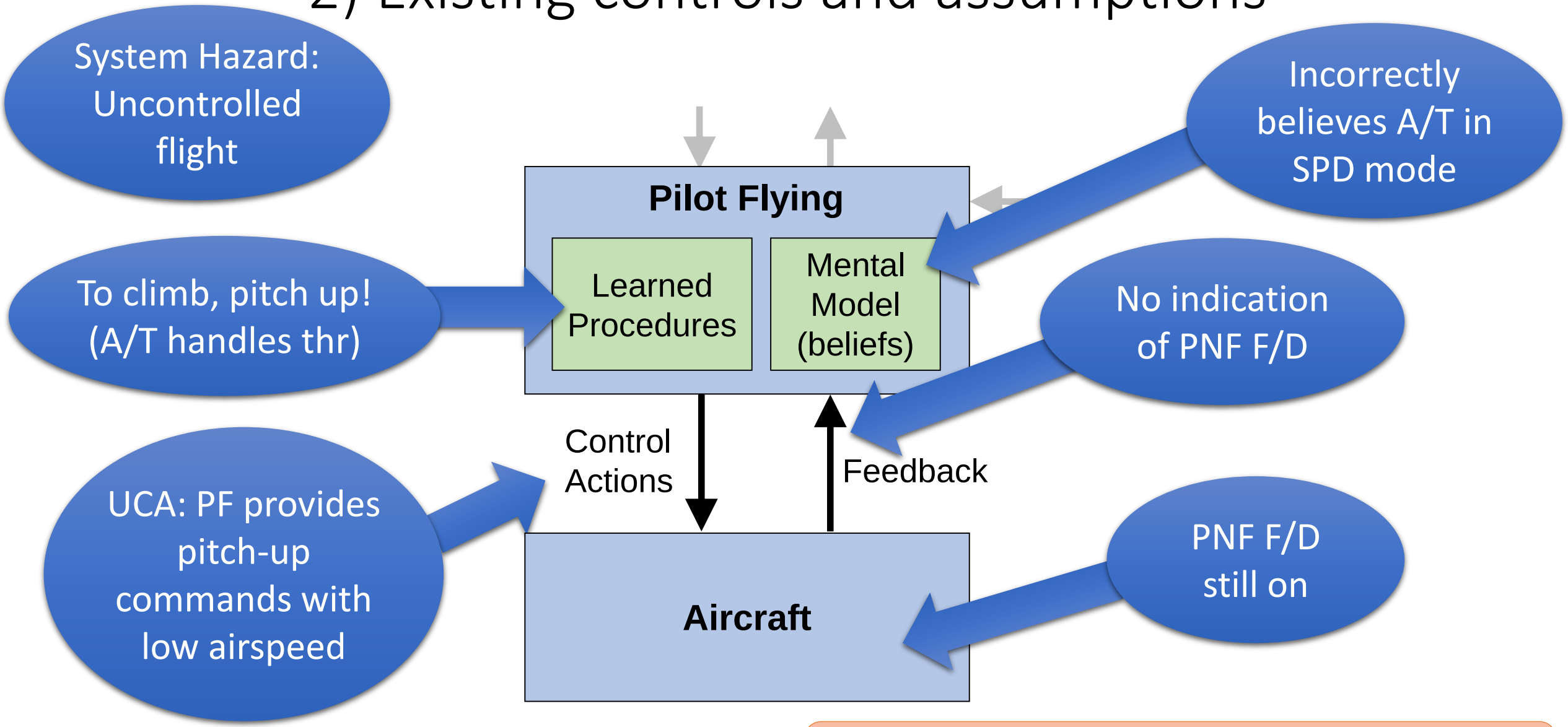
STPA Example (Future Events)



Example STPA-generated Scenario (simplified)



2) Existing controls and assumptions



<u>Assumption (& existing control):</u>
PF F/D and PNF F/D will be switched off together

3) Develop Indicators

Assumptions → ***Indicators***

A-1: PF F/D and PNF F/D will be switched off together **[UCA-1]** → **I-1:** Monitor PF and PNF F/D state, compare (FOQA) **[A-1]**

A-2: Maintenance technicians will only override warning when parts catalog is superseded **[UCA-2]** → **I-2:** Monitor parts catalog updates, compare to warning overrides **[A-2]**

Systems Approach to Leading Indicators

1. Identify vulnerabilities
2. Identify existing controls and assumptions
3. Develop indicators
4. Plan future actions

Leveson, 2015; Scarinci & Giusti, 2016; Thomas, 2018

3) Develop indicators

1) Vulnerabilities	2) Assumptions, existing controls	3) Indicators

3) Develop indicators

1) Vulnerabilities	2) Assumptions, existing controls	3) Indicators
PF pitch up commands with low airspeed	PF will recognize low airspeed, will not exceed AoA (Training)	Stall warning Pitch up with insufficient thrust
PF incorrectly believes A/T in SPD mode	PF will recognize A/T mode, PNF will call out mode changes (Callout procedures)	A/T automatically leaves SPD mode
PF incorrectly believes PNF F/D matches PF F/D	PF will provide F/D callout. PNF will acknowledge, execute. (Callout procedures)	PF F/D and PNF F/D turn off together
…	…	…

Simplified examples for purpose of presentation

4) Plan Future Actions

- Shaping actions
  - Prevent violation of assumptions
  - E.g. Interlocks, human-centered design, procedural checks, etc.
- Signposts
  - Anticipate changes that may violate assumptions, require re-assessment
  - E.g. new construction, new environment, etc.
- Assumption Checking
  - Monitor indicators over time, detect when assumptions invalid
  - E.g. FOQA data, ASRS, etc.
- Hedging (Contingency) actions:
  - Prepare for possibility an assumption will fail
  - E.g. Performance audits, fail-safe design, etc.

Systems Approach to Leading Indicators

1. Identify vulnerabilities
2. Identify existing controls and assumptions
3. Develop indicators
4. Plan future actions

Dewar, 2002; Leveson, 2015

Findings

- Quick, efficient method
- Identified incidents not reported
- Identifies hidden assumptions
- Provides traceability
- More comprehensive than other approaches

Questions?

Systems Approach to Leading Indicators

1. Identify vulnerabilities
2. Identify existing controls and assumptions
3. Develop indicators
4. Plan future actions