Active STPA – A Systems-based Hazard Analysis for Safety Management Systems (SMS)

BAF Lt Col Diogo Silva Castilho

castilho@mit.edu

2019

Summary

- Safety Management Systems in aviation
- Original STPA
- Assumptions-based Leading Indicators
- Active STPA
- Case study on parallel approaches
- I-SMS

Safety Management International Collaboration Group – SM ICG

Development of a Common Taxonomy for Hazards



Core membership of the SM ICG

- National Civil Aviation Agency (ANAC) of Brazil
- Civil Aviation Safety Authority (CASA) of Australia
- European Aviation Safety Agency (EASA)
- Federal Office of Civil Aviation (FOCA) of Switzerland
- United States Federal Aviation Administration (FAA)

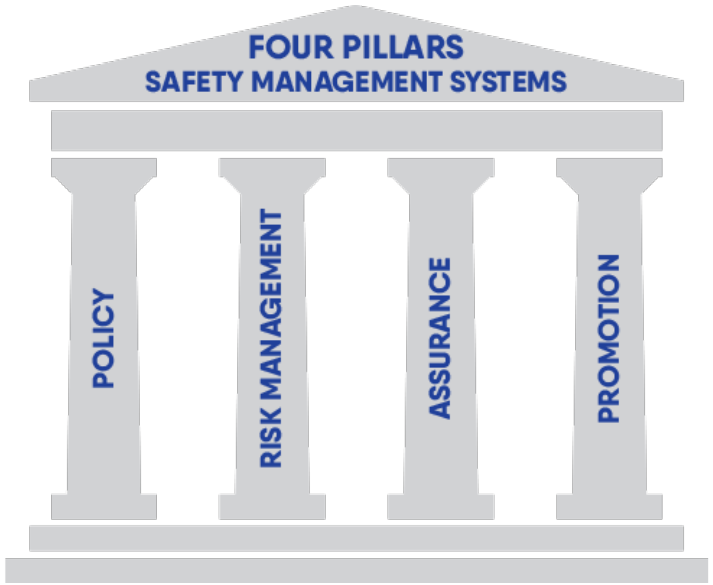
  Aviation Safety Organization
- International Civil Aviation Organization (ICAO)
- Transport Canada Civil Aviation (TCCA)
- Civil Aviation Authority of United Kingdom

Source: SM ICG

Background of SMS (Safety Management Systems)

- The International Civil Aviation Organization (ICAO) requires SMS for the management of safety risk in **air operations, maintenance, air traffic services, aerodromes**, **flight training and design and production** of aircraft.
- Annex 19 is the first new ICAO Annex in over **thirty years.**
- The SMP (Safety Management Panel) **delivered** the first phase of Annex 19 in **2012**.
- It was adopted by the ICAO Council on February, 2013 and became **applicable in November 2013**.
- The Amendment 1 to Annex 19 is effective in July 2016 and **applicable in November 2019.**

SMS – Safety Management System



Doc 9859 – SMM – Safety Management Manual

Framework for SMS – Annex 19

1. Safety policy and objectives

- 1.1 Management commitment
- 1.2 Safety accountability and responsibilities
- 1.3 Appointment of key safety personnel
- 1.4 Coordination of emergency response planning
- 1.5 SMS documentation

2. Safety risk management

- 2.1 Hazard identification
- 2.2 Safety risk assessment and mitigation

3. Safety assurance

- 3.1 Safety performance monitoring and measurement
- 3.2 The management of change
- 3.3 Continuous improvement of the SMS

4. Safety promotion

- 4.1 Training and education
- 4.2 Safety communication ANNEX

SPI – Safety

Appendix 2 of Annex 19

2. Safety risk management

2.1 – Hazard identification

2.1.1 The service provider shall develop and maintain a process to identify hazards associated with its aviation products or services.

2.1.2 Hazard identification shall be based on a combination of reactive and proactive methods.

2.2 Safety risk assessment and mitigation:

The service provider shall develop and maintain a process that ensures analysis, assessment and control of the safety risks associated with identified hazards.

3. Safety assurance

3.1 Safety performance monitoring and measurement

3.1.1 The service provider shall develop and maintain the means to verify the safety performance of the organization and to validate the effectiveness of safety risk controls.

3.1.2 The service provider's safety performance shall be verified in reference to the safety performance indicators and safety performance targets of the SMS in support of the organization's safety objectives.

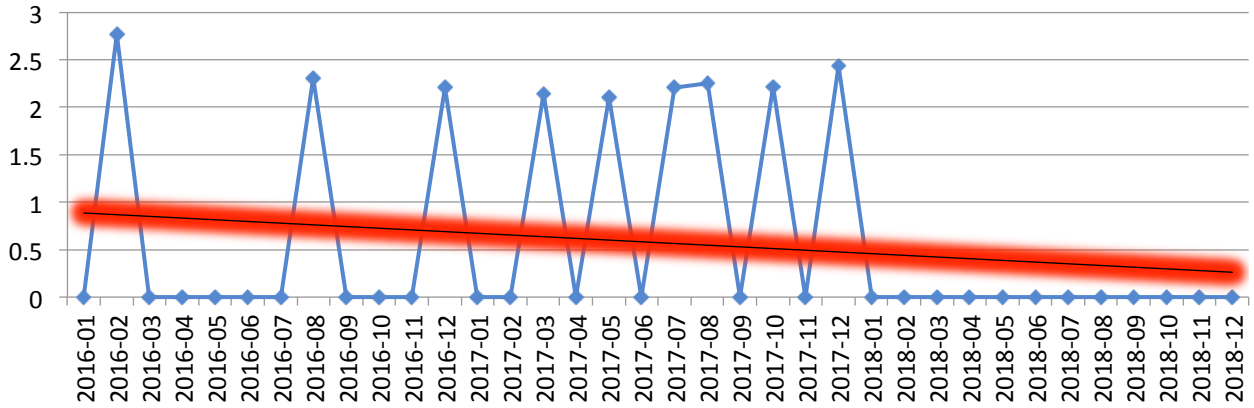
SPI (Safety Performance Indicator)

Flight Data Analysis Programme - Events Triggering Criteria		
This is an uncontrolled document published for general reference only - please contact the Flight Data Centre for the latest settings. (Last Update : 11-May-2017)		
Alert Code & Designation	**A300-600F**	**AHK B744 Freigther**
01 VMO EXCEEDENCE	CAS ≥ VMO	CAS ≥ VMO
02 MMO EXCEEDENCE	CAS ≥ MMO	CAS ≥ MMO
03A EXCEEDENCE OF FLAP PLACARD SPEED	CAS ≥ VFE for at least 2 sec	CAS ≥ VFE for at least 2 sec
03F EXCEEDENCE OF GEAR PLACARD SPEED - IAS	CAS ≥ VLE for at least 2 sec	CAS ≥ VLE for at least 1 sec
03G EXCEEDENCE OF GEAR DOWN LIMIT SPEED - MACH	CAS ≥ VLE (Mach) for at least 2 sec	CAS ≥ VLE (Mach) for at least 1 sec
03H EXCEEDENCE OF GEAR RETRACTION SPEED - KNOTS	CAS ≥ VLO (Retraction) for at least 2 sec	CAS ≥ VLO (Retraction) for at least 1 sec
03I EXCEEDANCE OF GEAR EXTENSION SPEED	CAS ≥ VLO (Extension) for at least 2 sec	CAS ≥ VLO (Extension) for at least 1 sec
04 EXCEEDENCE OF FLAP ALTITUDE LIMIT	Pressure Altitude ≥ FL200 for at least 2 sec	Pressure Altitude ≥ FL200 for at least 2 sec
05 EXCEEDENCE OF MAXIMUM OPERATING ALTITUDE	Pressure Altitude ≥ published service ceiling for at least 2 sec	Pressure Altitude ≥ published service ceiling for at least 2 sec
06B APPROACH SPEED HIGH - BETWEEN 500 FEET AND 50 FEET	CAS ≥ Vapp Target + 40 kts for at least 1 sec	CAS ≥ Vref + 30 kts for at least 2 sec

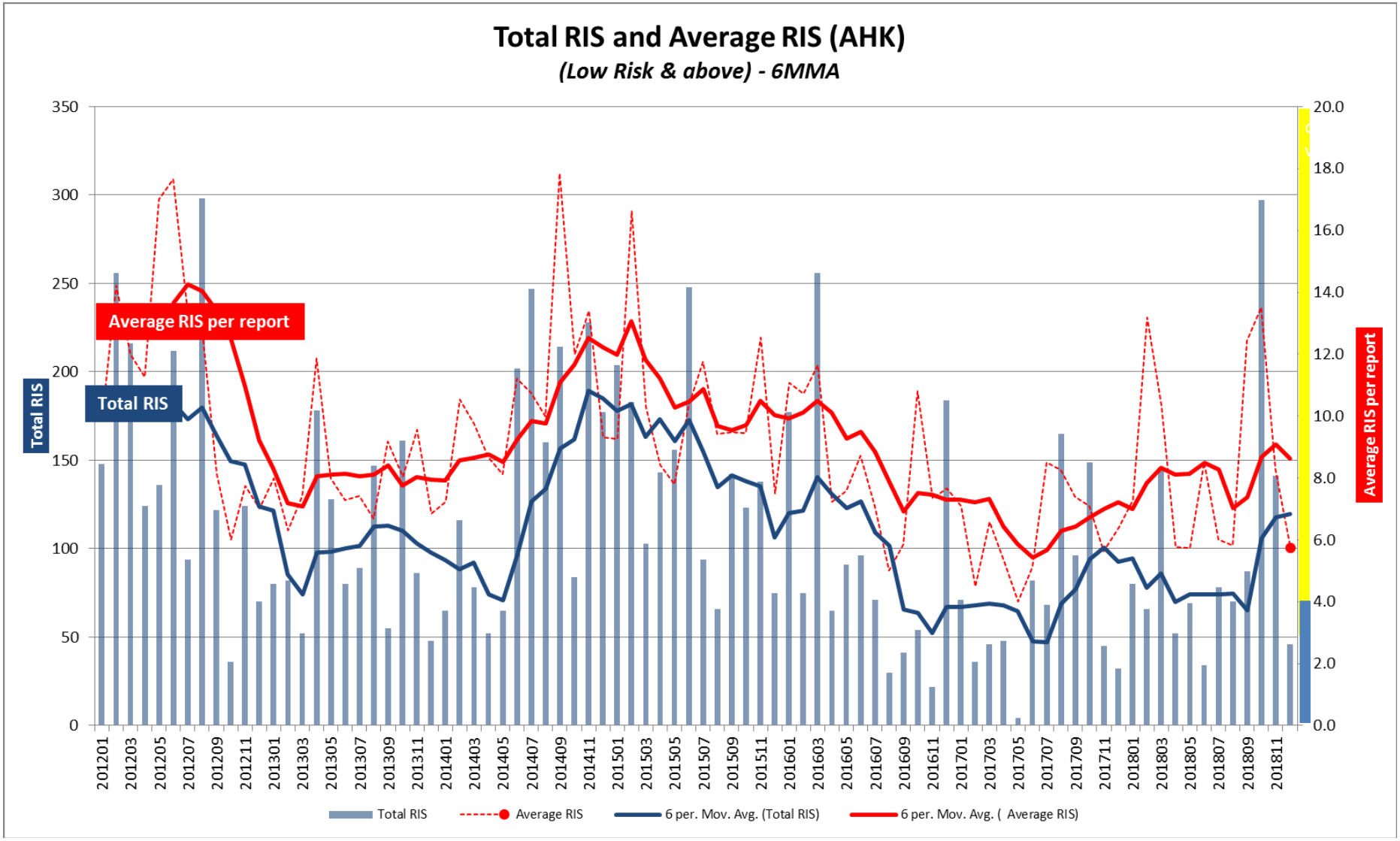
<u>Partner – Air Hong Kong</u>

Flight Data (FOQA) Exceedance

- 128 Monitored SPI
- 67 related with Approaches



Combined Trends



Lifetime of Boeing 777

- 1990: First group meeting
- 1994: Roll out and first flight
- 1995: Certification and entry into service

Lifetime expectancy: 40+ years

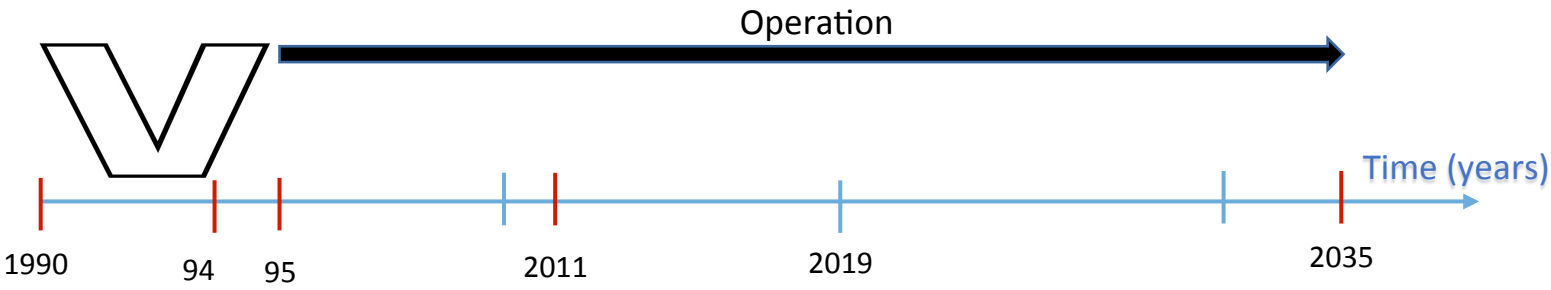
- 2011: Release of third generation B-777X



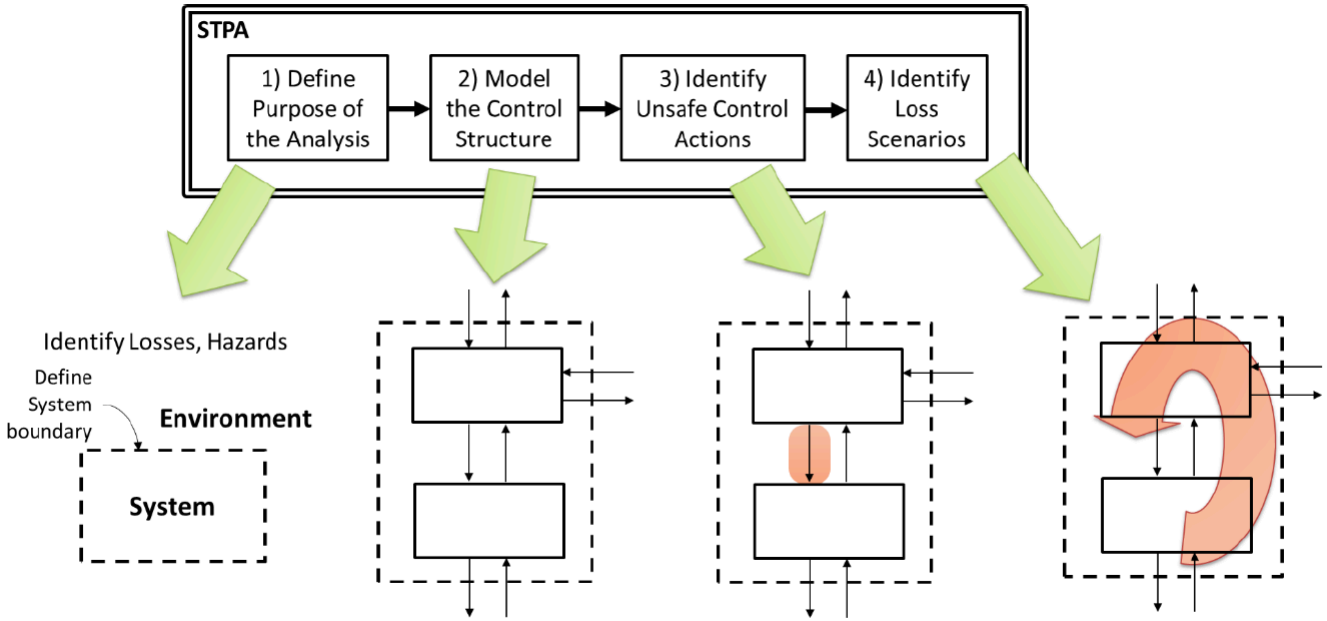


Hazard Analysis

Safety Management: Safety officers and engineers responding to accidents/incidents and managing reports



Losses on missed approaches, incidents and accidents



Source: STPA Handbook (2018)

- L1: Human life, injury, motion sickness, fright.
- L2: Environmental: oil and fuel pollution, debris in nature.
- L3: Material or Financial
- L4: Company reputation
- L5: Operational performance: delays and consequences on planning

Losses on missed approaches, incidents and accidents

- L3: Material or Financial:
  - Insurance company: premium for the accident and third party property damage
  - Airline: extra fuel and crew working hours on missed approaches, damage to the aircraft, cleaning debris, providing hangar to investigation, and law suits.
  - Airline investors: stock market decay
  - Manufacturer: Investigation and changes to manuals or procedures
  - Third party companies
  - Countries: Air Force search and rescue missions, aviation agencies accident investigation.
  - ATC: controller seclude.
  - Airports: Equipment loss, runway damage, runway or apron interdiction.
  - Passengers: personal belongings and many possible consequences of not finishing the planned trip.
  - Cargo clients: loss of packages.
- L4: Company reputation:
  - Airline: doubts about employee selection, quality of training.
  - The manufacturer: Design errors, usability of equipment, robustness of philosophy, quality of manufacturing.
  - Crew Reputation

Hazards

- H1: Aircraft violates criteria for stable approaches
  - H1.1: Lateral instability [L1, L3]
    - Possible consequence: touchdown misaligned or outside runway lateral limits
  - H1.2: Longitudinal instability [L1, L3, L5]
    - Possible consequence: Hard landing
  - H1.3: Energy in excess [All losses]
    - Possible consequence: inability to break within runway length
  - H1.4: Lack of energy [L1, L2, L3, L5]
    - Possible consequence : shaker activation or touchdown before runway threshold
  - H1.5: Loss of control [All losses]
- H2: Controlled Flight Into Terrain (CFIT) [All losses]
- H3: Aircraft violates minimum separation from airspace or other aircraft [All losses]
- H4: Low fuel level after missed approaches [L1, L3, L4, L5]

System-level Requirements and Constraints (SR – SC)

- SC-1: Aircraft must maintain criteria for stable approaches [H-1]
  - SC-1.1: Aircraft must be within lateral navigation limits [H-1.1]
  - SR-1.1: if lateral navigation is off limits, the PM must detect and inform [H-1.1]
  - SC-1.2: Aircraft must be longitudinally stable [H-1.2]
  - SR-1.2 : if the aircraft is longitudinal unstable before landing, the PF must GA [H-1.2]
  - SC-1.3: Aircraft must keep adequate amount of energy [H-1.3]
  - SR-1.3 : if the shaker is activated, the PF must GA [H-1.3]
  - SC-1.4: Aircraft must keep adequate amount of energy [H-1.4]
  - SR-1.4 : if the aircraft is more than 500ft above recommended altitude at the middle marker or more than 300ft above at final marker, the PF must GA [H-1.4]
  - SC-1.5: Flight must be controlled [H-1.5]
  - SR-1.5 : Pilots need to be trained to recover the control of their aircraft, including CRM procedures [H-1.5]

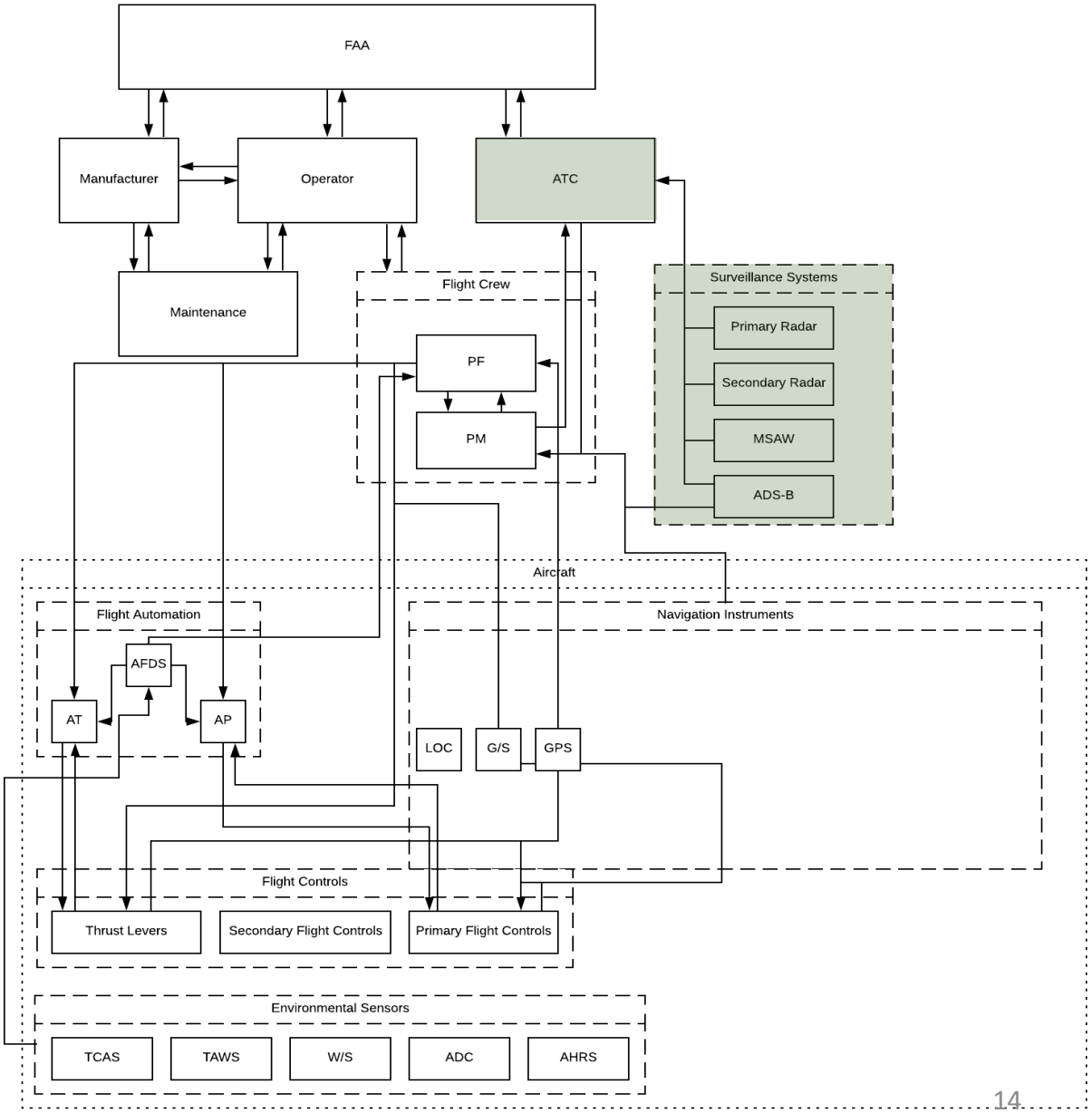
Safety Functional Control Structure

Systems boundary

Commercial aircraft approaching for landing

Controllers

- ATC
- The crew
- Crew of other aircraft or drone



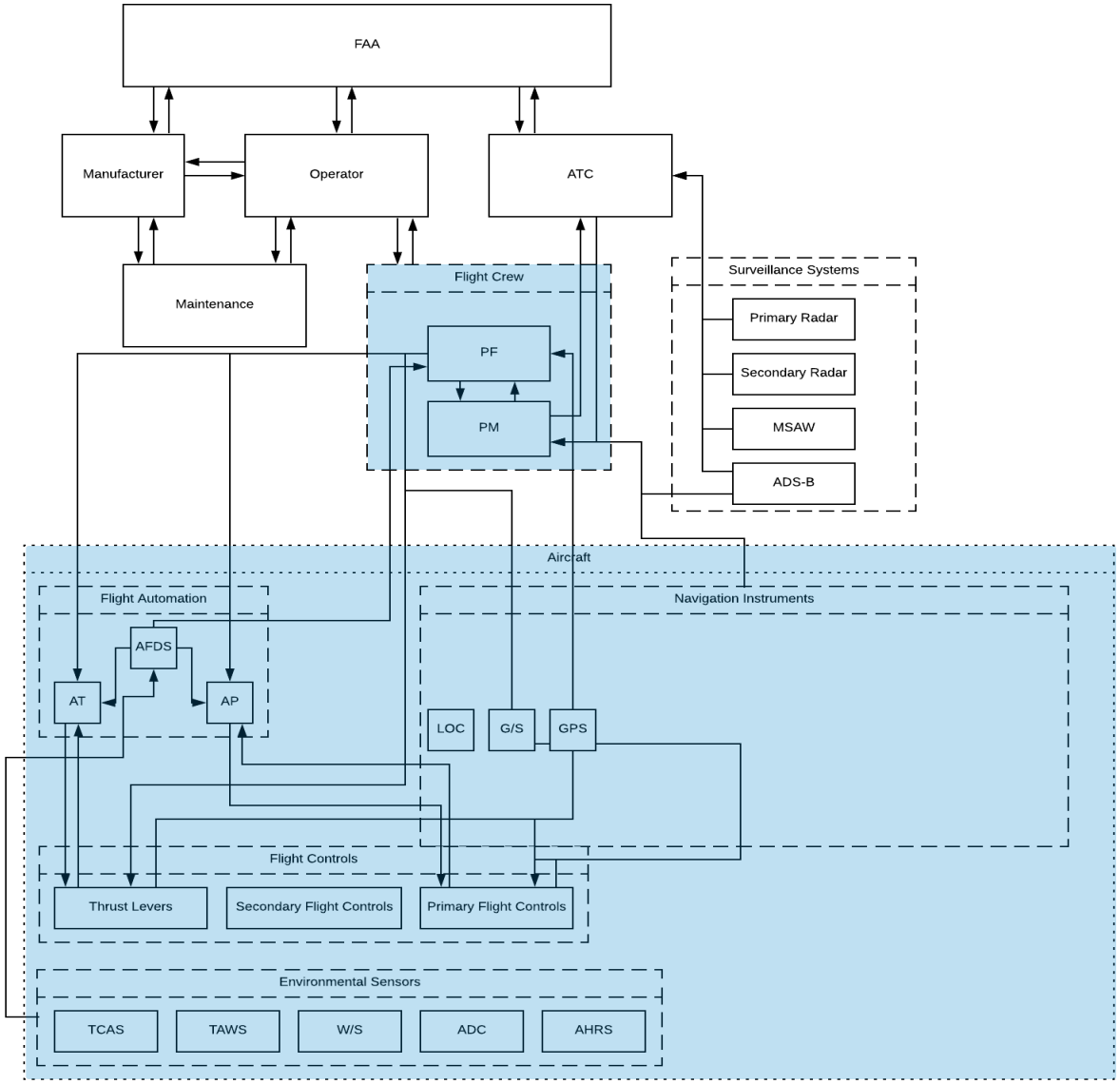
Safety Functional Control Structure

Systems boundary

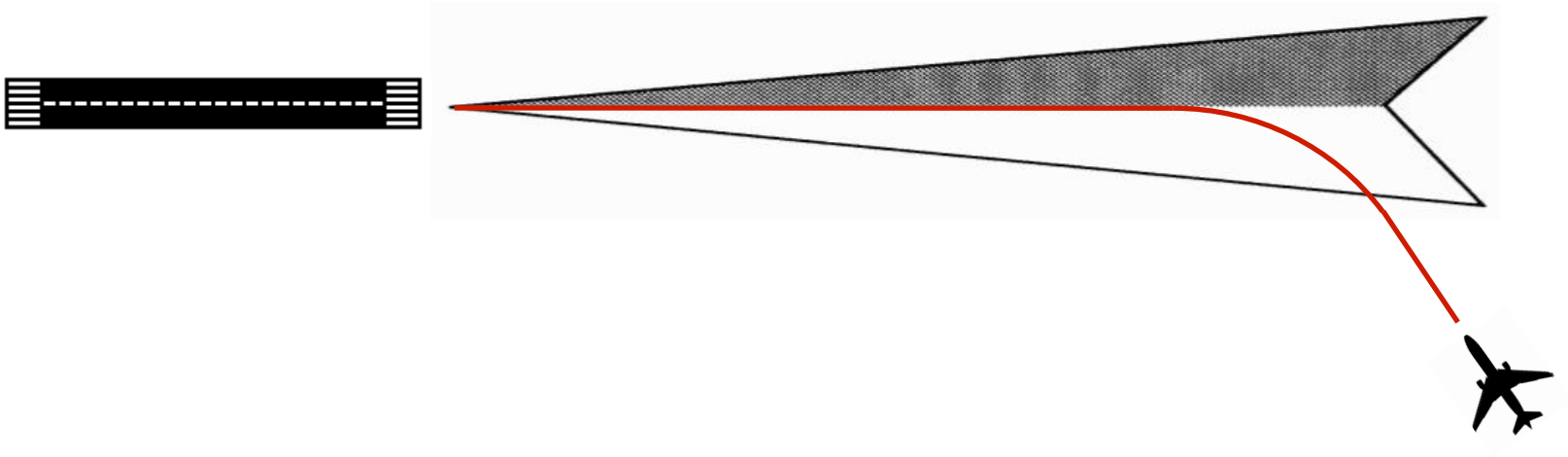
Commercial aircraft approaching for landing

Controllers

- ATC
- The crew
- Crew of other aircraft or drone



STPA Indicators for SMS



Original STPA

Controller	Process	Switch / Selector	Control Actions	Unsafe Control Actions											
				Provided causes Hazard			Not Provided causes Hazard			Applied for too long or too short			Wrong timing or order		
				UCA	H*	Description	UCA	H*	Description	UCA	H*	Description	UCA	H*	Description
Crew	AP	LOC	Engage LOC	23	H3 H4	Engage Loc when AC is under vectors flying outbound	24	H1.1 H3	Not engaged when AC passes ideal turning point			N/A	25	H1.1 H3	Engage too late when AP is unable to capture without overshoot

STPA Indicators for SMS

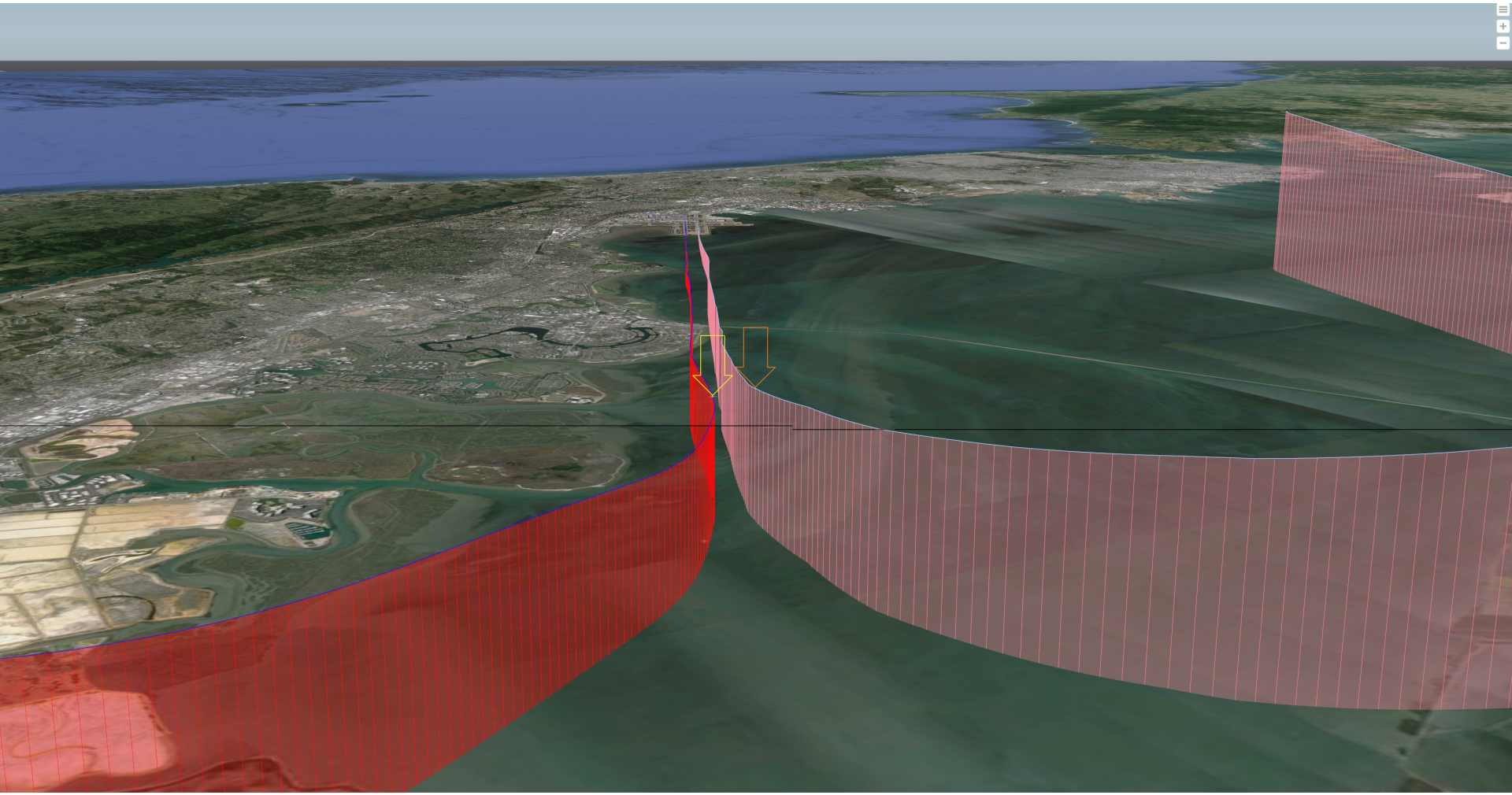
UCA	H*	Description
25	H1.1 H3	Engaged too late when AP is unable to capture without overshoot

Scenario	Constraint
PM shares attention with phraseology and reading IFR procedures and forgets to press LOC before ideal turning point	LOC must be selected with anticipation enough to avoid overshoot of Localizer by more than 1 dot

Assumption	Measure	Leading Indicator	Monitor	Frequency
If landing briefing happens above 5000 ft, workload level is not a reason to forget selecting LOC	Training procedure: App briefing during descent must initiate above 7000 ft	Measure dots of LOC overshoot	FOQA (FDM)	Every flight

SPI	SPT
# of dots of LOC overshoot	Less than 1 dot

FOQA Data of Real Event



Event Investigation

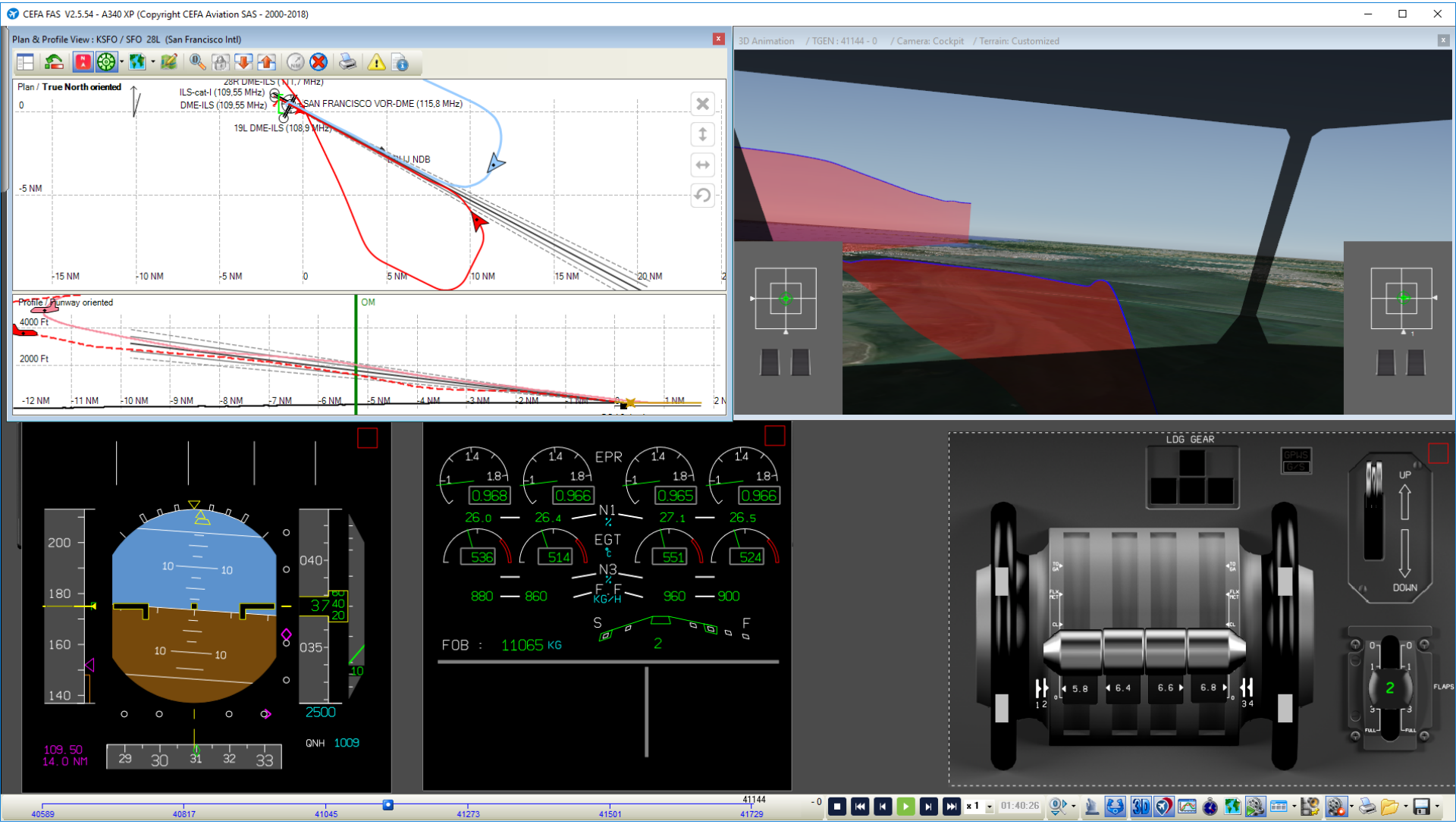
Title	TA ON APPROACH - SFO
Pilot Description	Intruder aircraft TA at 1200' TCAS showing relative position 10 o'clock 200' above. No VIS contact. At 1000' RA to descend received. F/O carried out maneuver CPT told ATC "RA". Traffic became visual for us at approx 700'. Until then TCAS was showing on top of us. I made decision not to go around as this would have jeopardized our safety since we had no idea of the exact proximity of the traffic. Once we had him in sight we stabilized at 600'. As we were visual to the ground and could not at first see the traffic and once we saw him he was to close for a go around. I decided the safest course of action was to continue to land.
Flight Data Analysis	At 1310 ft TCAS RA 1500 FPM descent was activated for 16 seconds and the aircraft descent to 928 ft. the aircraft levelled off at about 740 ft at 3.3 DME and climbed to 790 ft at 2.8 DME. A/P was immediately off when the RA was activated.
Flight Ops Risk Analysis	This was a well handled event given the conflict of SOP and safety constraints that the crew found themselves experiencing. The Captain was interviewed and it was evident that his actions were correct given the information he was processing at the time of the event. Although stabilized approach criteria were not met, safety was maintained through the see and avoid philosophy. Animation was created and reviewed. 1 high rate of descent FDAP was triggered as a response to the RA descend command at 1300'. Aircraft was stabile on flight path by 750'.

- **Intruder 10 o'clock 200ft above**
- **No VIS contact**
- **TCAS RA to descend**
- **I made decision not to go around**
- **I decided to land**

- **At 1310 ft TCAS RA 1500 FPM**
- **Aircraft levelled off at about 740 ft**
- **A/P off at RA**

- **Well handled event given the conflict of SOP and safety constraints**
- **Safety was maintained through the see and avoid philosophy**

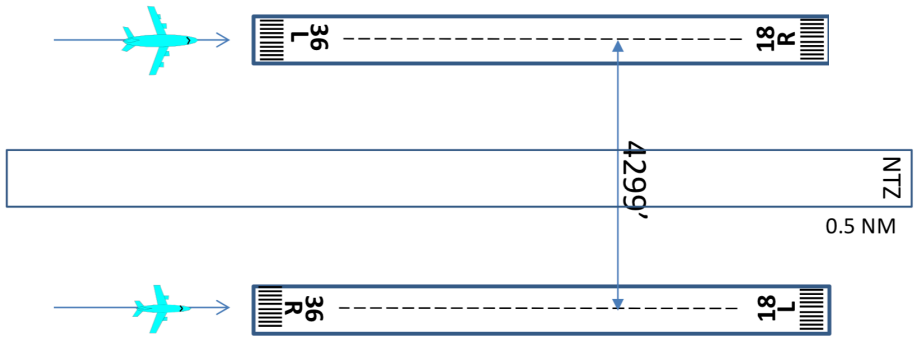
FOQA Data from Partners



AHAI – Active Hazard Analysis Input

Description after FOQA

During simultaneous parallel approach to SFO (A-340 of A to 28L and B-737 of B to 28R), the B-737 overshot the localizer, entering the NTZ, 200ft above and 1000ft behind the A-340. The Tower did not complain or correct the 737.



3 Cases

- **B737 - Why one aircraft overshot the localizer and entered the NTZ?**
- ATC - Why the ATC did not command one of the aircraft to go around?
- A340 - Why the correct decision of the captain is not part of the procedures?

Phases of an Active STPA

1. Identify Control Relations
2. Diagnose
3. Reason on Assumptions
4. Solution
5. Update

Active STPA Phase 1 - Tasks

1. **Indentify Control Relations**
2. Diagnose
3. Reason on Assumptions
4. Solution
5. Update

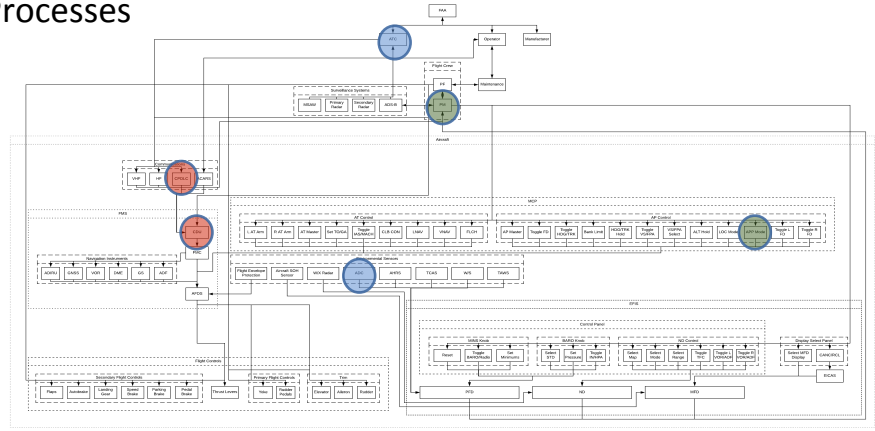
1.1 - Search in Control Structure

1.2 - Identify Controllers

1.3 - Identify Controlled Processes

1.4 - Find Control Actions

1.5 - Highlight UCAs



Original STPA

Controller	Process	Switch / Selector	Control Actions	Unsafe Control Actions											
				Provided causes Hazard			Not Provided causes Hazard			Applied for too long or too short			Wrong timing or order		
				UCA	H*	Description	UCA	H*	Description	UCA	H*	Description	UCA	H*	Description
Crew	AP	LOC	Engage LOC	23	H3 H4	Engage Loc when AC is under vectors flying outbound	24	H1.1 H3	Not engaged when AC passes ideal turning point			N/A	25	H1.1 H3	Engaged too late when there is high intercept angle and AP is unable to capture without overshoot

Active STPA Phase 2 - Tasks

1. Identify Control Relations
2. **Diagnose**
3. Reason on Assumptions
4. Solution
5. Update

2.1 – Search training manuals and procedures

2.2 – Search for constraints in all levels

2.3 – Identify scenarios

2.4 – Identify Control Actions and UCAs

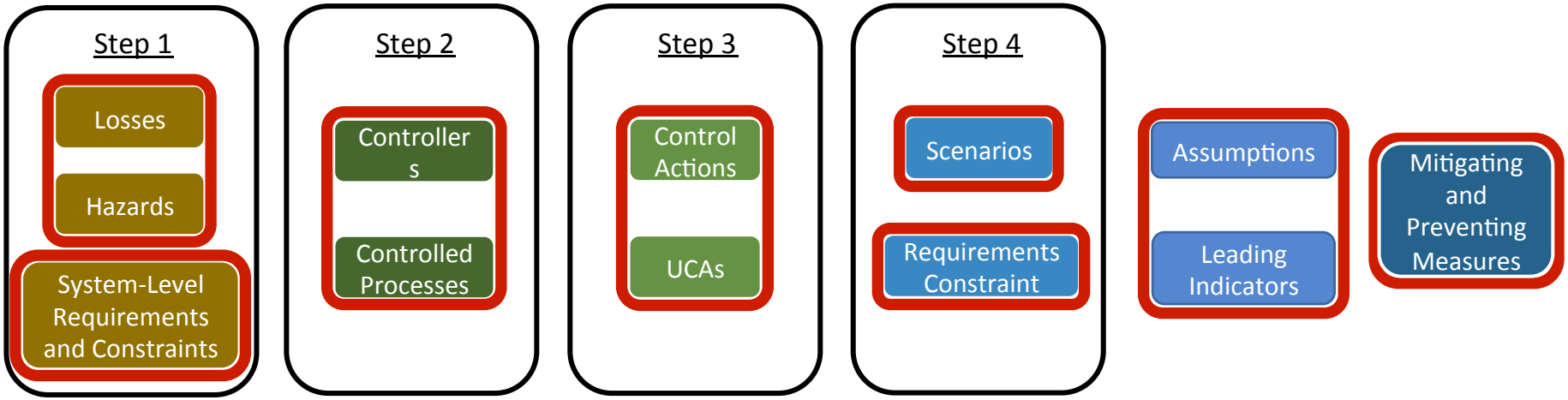
2.5 – Verify validity of Control Structure

2.6 – Verify validity of fundamentals

2.7 – List pertinent assumptions and L.I.

Parallel App example

- There was a scenario
- Assumption on workload that pilots would not forget to press LOC before ideal turning point was flawed
- CRM procedure was not followed



Active STPA Phase 3 - Tasks

1. Identify Control Relations
2. Diagnose
3. **Reason on Assumptions**
4. Decide on a Solution
5. Update

3.1 – Identify violated assumptions

3.2 - Verify if Hedging Actions worked

3.3 – Investigate causal and contributing factors

3.4 – State why each assumption was wrong

3.5 – Evaluate trends or changes

3.6 – Register new assumptions

Parallel App example

3.1 – Violated assumption: If procedure is briefed before initial point, workload level is not a reason to forget selecting LOC

3.2 – ATC order to B737 was late

3.3 – Memory error caused by distraction or high workload

3.4 – The assumption that the PM had time enough to engage the LOC when under vectors was correct for regular app, not necessarily for parallel app

3.5 – Change: There is a new responsibility for the PM, check visually for separation with the other AC in parallel App

3.6 – The higher workload on parallel app requires that the final setup of AP occurs before the visual scan for other AC

Active STPA Phase 4 - Tasks

1. Identify Control Relations
2. Diagnose
3. Reason on Assumptions
4. **Solution**
5. Update

4.1 – List possible solutions

4.2 - Analyze tradeoffs

4.3 - Determine optimum solution

Parallel App example

4.1 – Solutions:

I. Transfer responsibility to select LOC to PF

II. Eliminate requirement that PM acquire and maintain visual contact with other AC

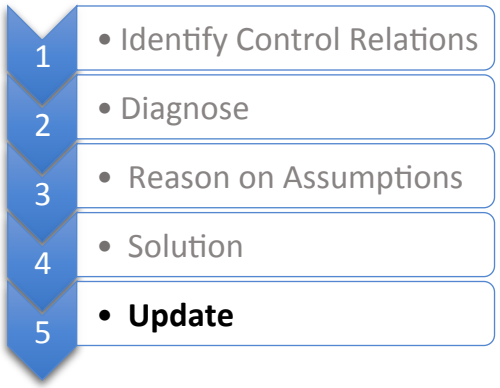
III. Determine that PM should start visual search only after setup of AP and call out to PF

4.2 – (I) PF has other responsibilities and high workload

(II) This responsibility is a Hedging Action for another assumption

4.3 – Solution III

Active STPA Phase 5 - Tasks



5.1 – STPA

5.2 – Measures

5.3 – Hedging Actions

5.4 – SPIs and SPTs

5.5 – Trends

Parallel App example

5.1 – No changes – low level constraint is valid

5.2 – Communicate new CRM procedure to all pilots:

PM should start visual search only after setup of AP and call out to PF on parallel App

5.3 – PF checks if LOC is engaged before ideal turning point

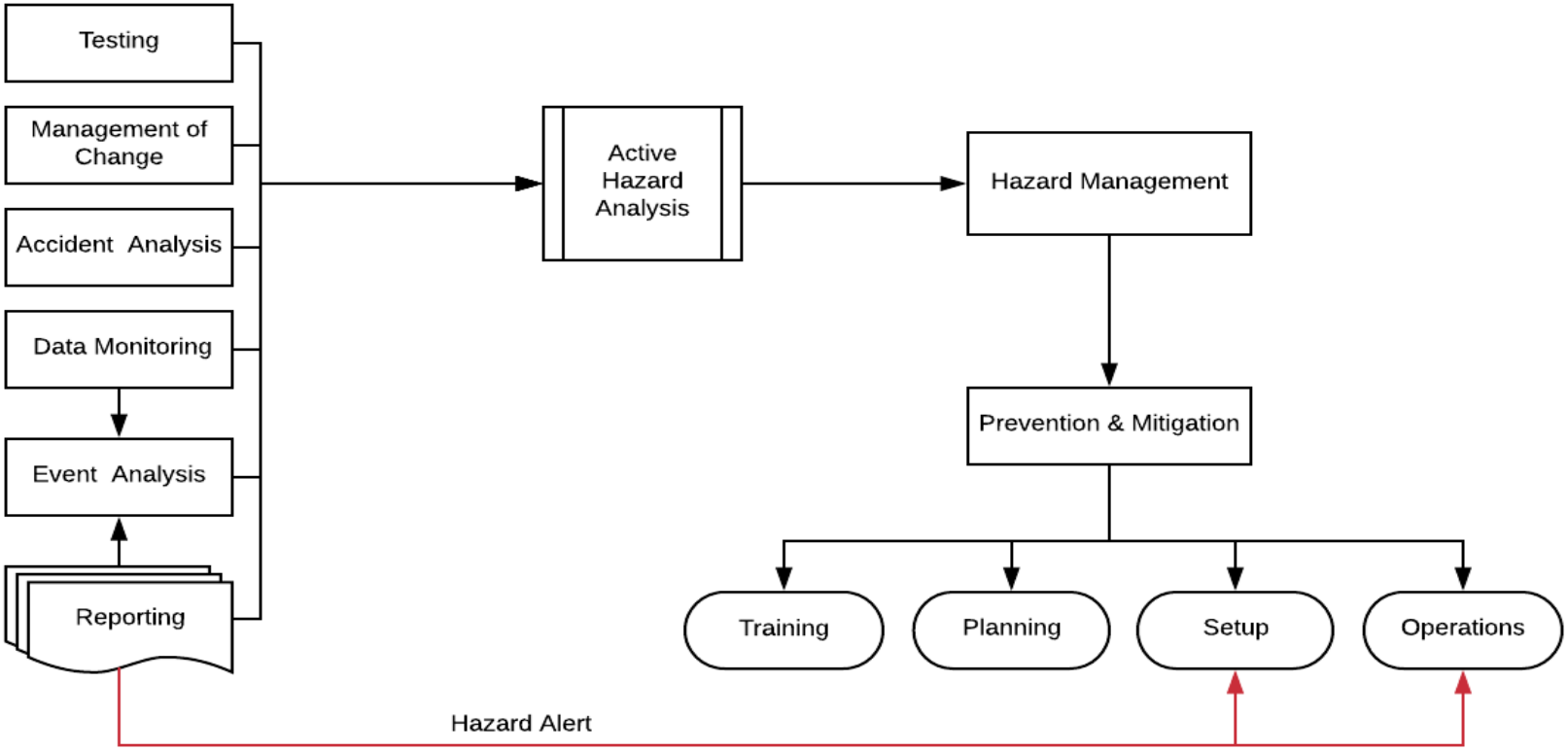
Set observation flights to verify if new CRM procedures are followed

5.4 – New SPI: Observe in FOQA window in seconds for LOC selection

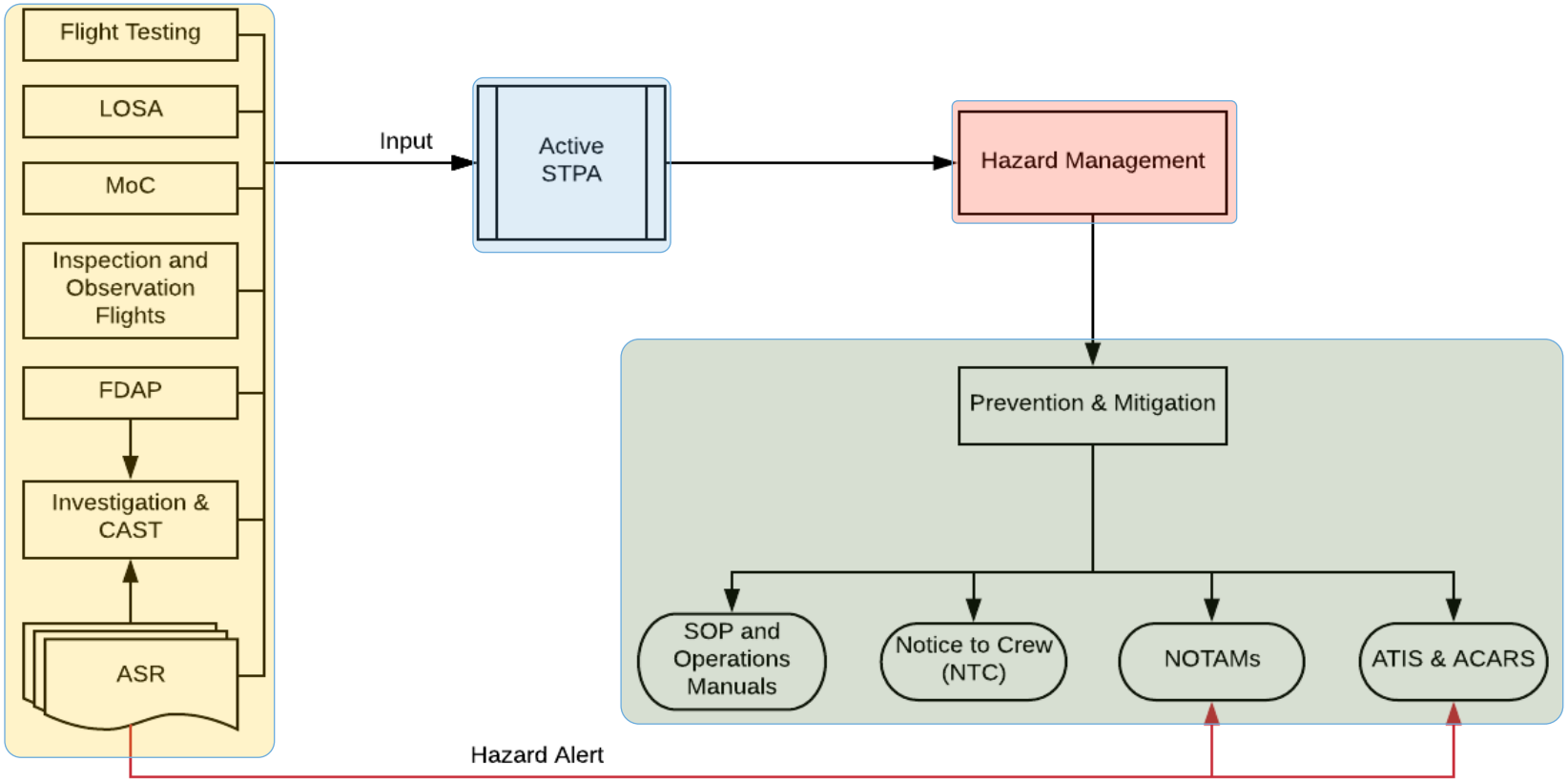
Observe how many seconds LOC has been selected before ideal turning point (SPT: above 30s)

5.5 – Include data in cockpit workload trend

I-SMS General Framework



I-SMS - Application for Commercial Aviation



Four Processes:

- P1 - Communication protocol for sensitive data
- P2 - Active Hazard Analysis update
- P3 – Hazard Management
- P4 – Prevention & Mitigation

Potential Outcomes

- Trends to answer if system is drifting in safety status
- More complete STPA
  - Organized update of assumptions
  - Additional enforcement mechanisms for constraints
- Clearer allocation of responsibilities
  - Foster initiative and safety awareness attitude (Safety Promotion)
- Security: Address vulnerability against adversaries
- Enhanced knowledge about system and environment
- More robust training procedures
- Support management long time planning and decision making (provided by more meaningful trends)

Thank you!

Questions?



Diogo Castilho

castilho@mit.edu

castilhods@msn.com

diogo-castilho-1ab66034

Accidents in Aviation

Wednesday Mar 20th 2019

- I Envoy E135 at Mc Allen on Mar 18th 2019, smoke on board
- I Jetblue E190 at Boston on Mar 19th 2019, bird strike
- I Austral E190 near Posadas on Mar 20th 2018, smoke in cabin
- A THY B773 near Boston on Mar 9th 2019 turbulence injures 29 people on board
- I KLM B773 near Shannon on Mar 19th 2019, engine oil problem

Thursday Mar 21st 2019

- A Commutair E145 at Presque Isle on Mar 4th 2019, runway excursion, hard landing and gear collapse
- A Spirit A319 near Las Vegas on Feb 27th 2019, smoke in cockpit
- I Westjet B737 enroute on Mar 16th 2019, pilot incapacited
- A Iran F100 at Tehran on Mar 19th 2019 main gear did not extend

Saturday Mar 23rd 2019

- I American A332 at Munich on Mar 22nd 2019, pack problem
- I Iran Aseman F100 at Ilaam and Tehran on Mar 22nd 2019, right main gear did not extend, then by luck extended one last time
- I BoA B737 near Cochabamba on Mar 22nd 2019, engine shut down in flight
- I Cathay Pacific A333 at Jakarta on Mar 22nd 2019, hydraulic failure

Source: Aviation Herald