Hazard Analysis of NextGen Arrival Phase of Flight Concepts: Interval Management – Spacing

Cody Fleming

March 26, 2014

MIT AEROASTRO

SYSTEMS ENGINEERING RESEARCH LABORATORY

Agenda

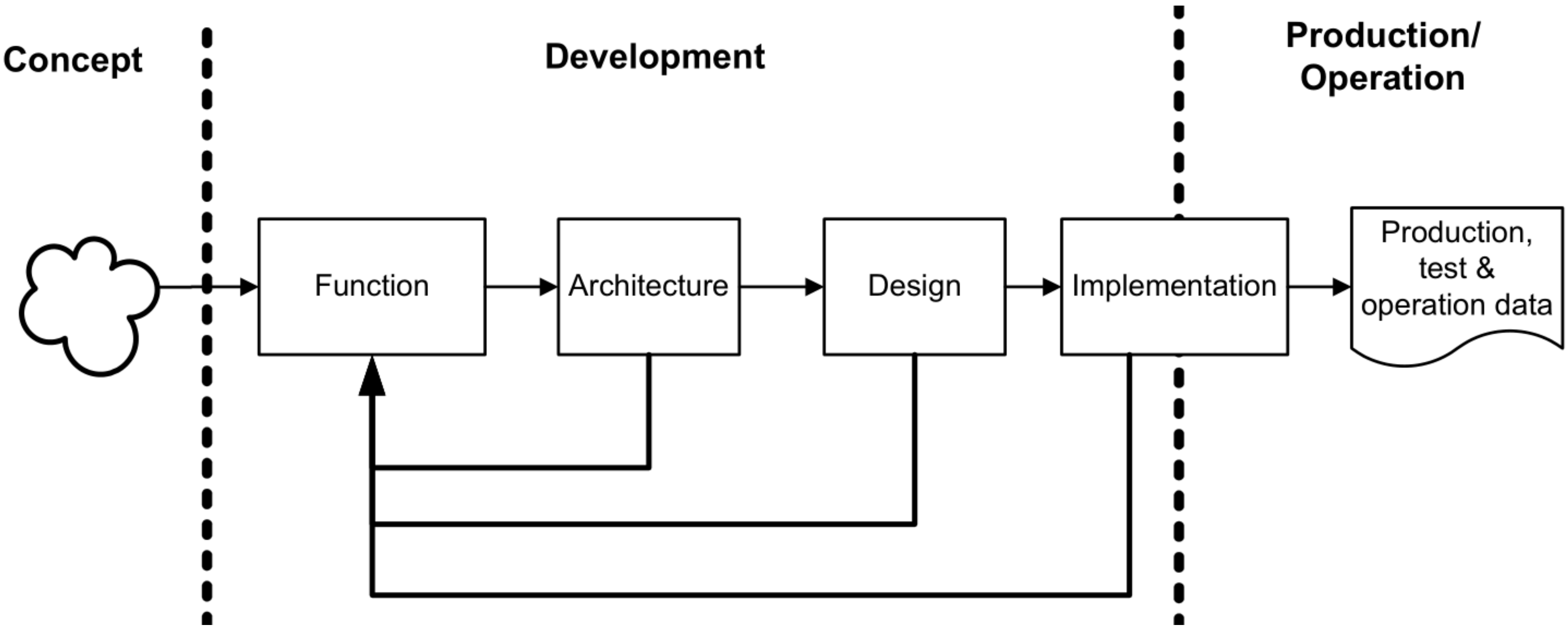
- Background
- NextGen Example
- Analysis
- Future

Motivation

- Shuttle
- B787

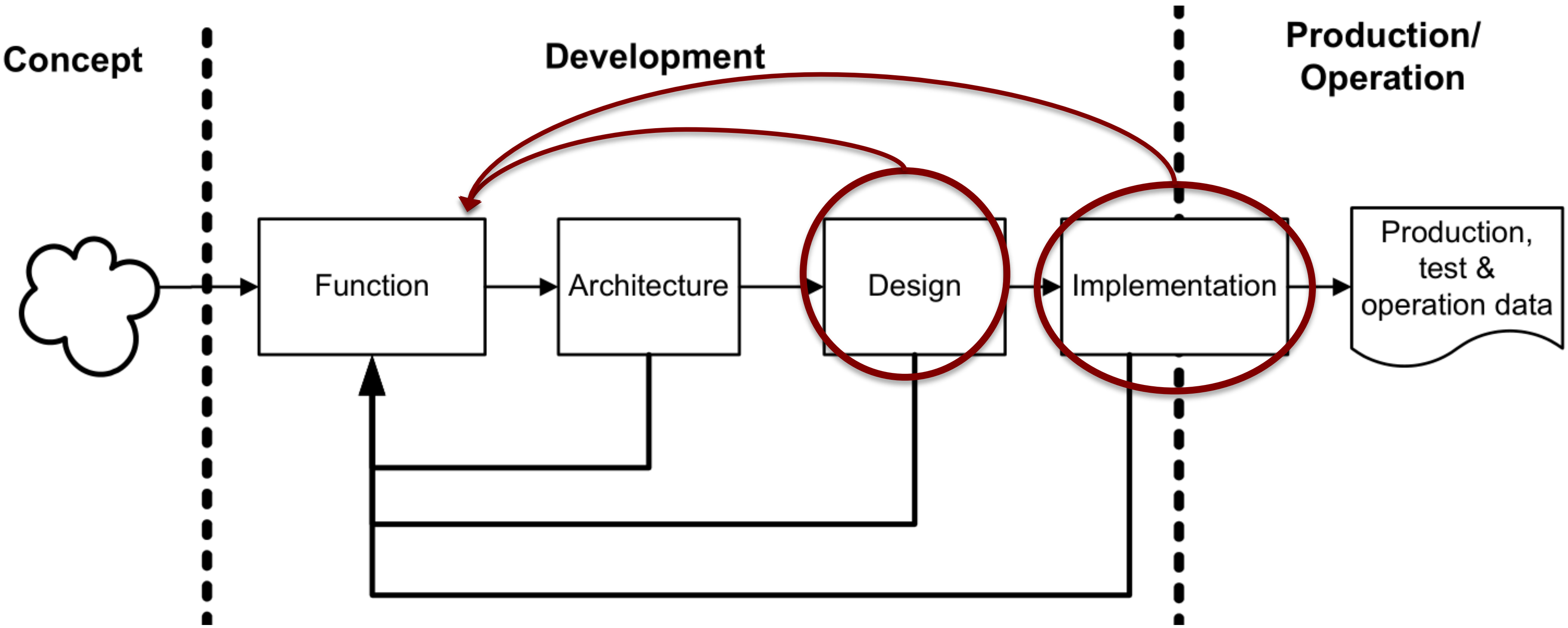
[Wiki Commons 1986, WSJ 2013, Guardian 2013]

Systems Engineering Timeline



[ARP-4754 2010]

Systems Engineering Timeline



[ARP-4754 2010]

National Airspace Safety

- Current flight-critical systems remarkably safe due to:

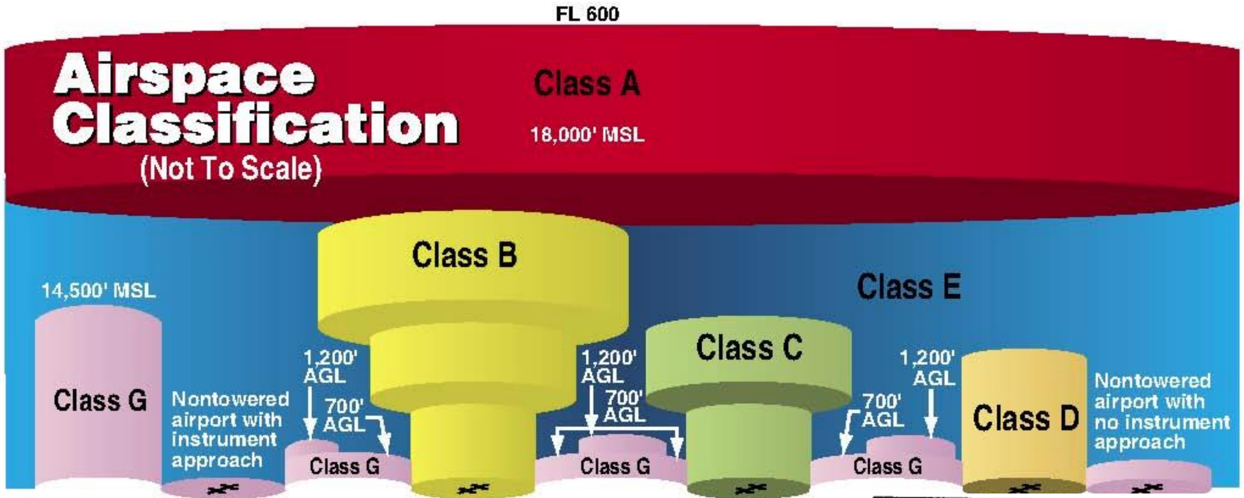
National Airspace Effectiveness

- Conservative adoption of new technologies

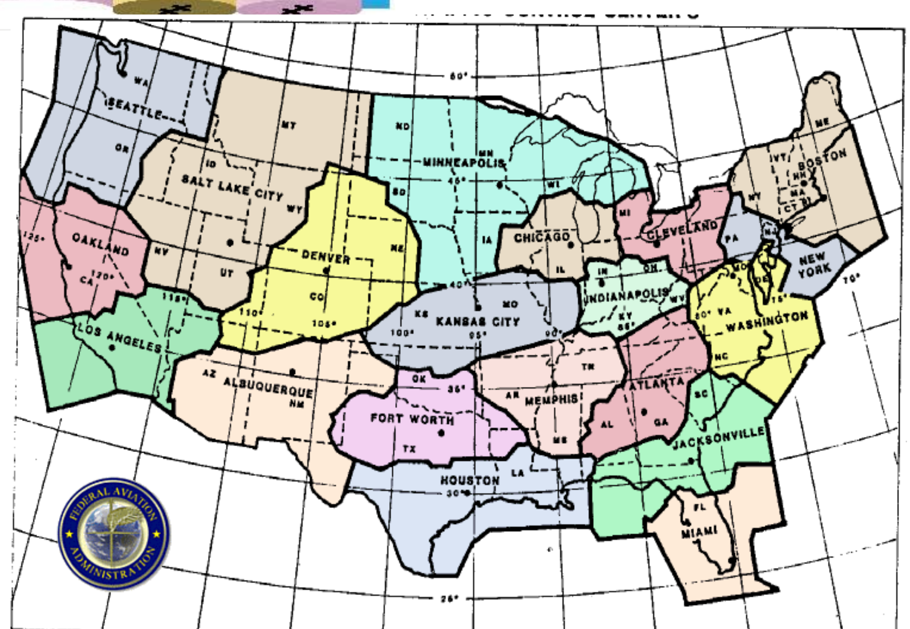
[Av News 2014]

National Airspace Safety

- Extensive decoupling of the system components



[Ascent 2013]



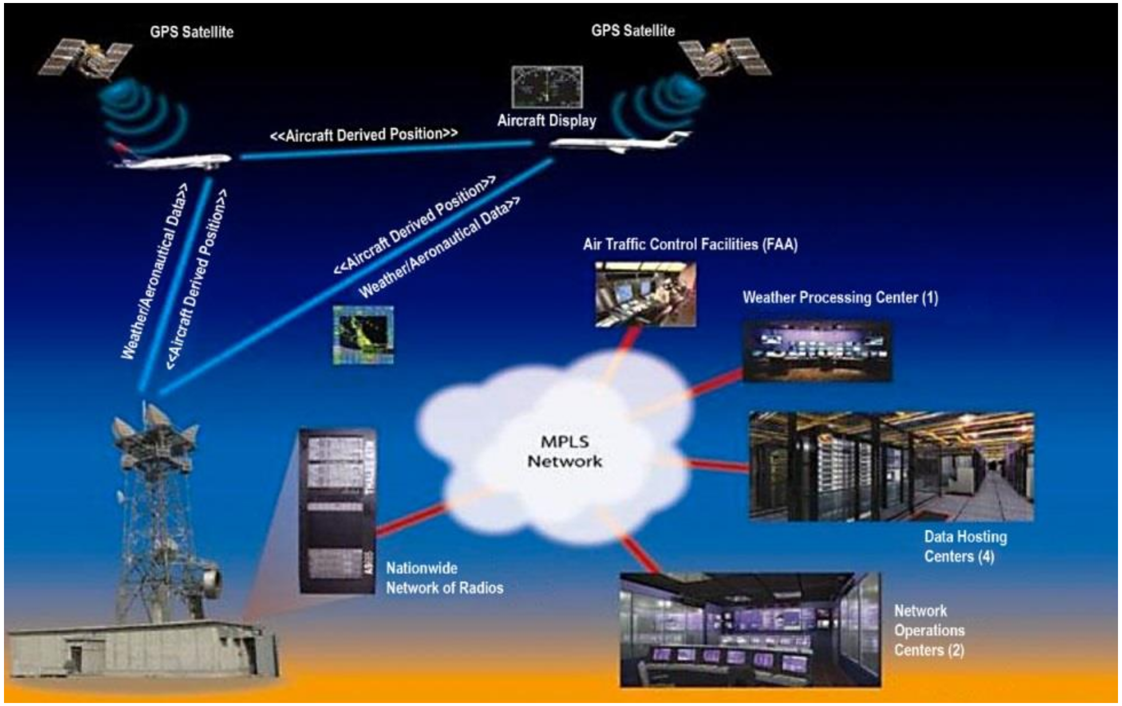
[IAC 2003]

National Airspace Safety

- Careful introduction of automation to augment human capabilities
- Reliance on experience and learning from the past

National Airspace Upgrades

- NextGen violates these assumptions -- more potential for component interaction accidents:

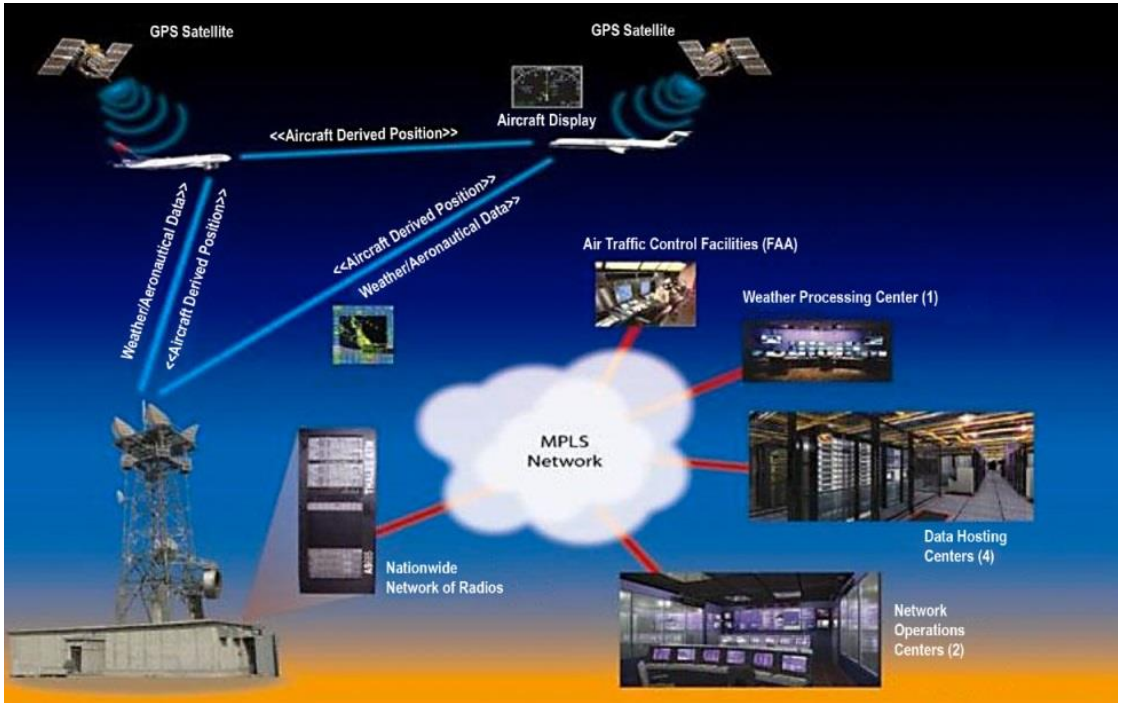


[IHO 2013]

National Airspace Upgrades

- Use of new technologies with little prior experience in this environment

- Reliance on software increasing and allowing greater system complexity



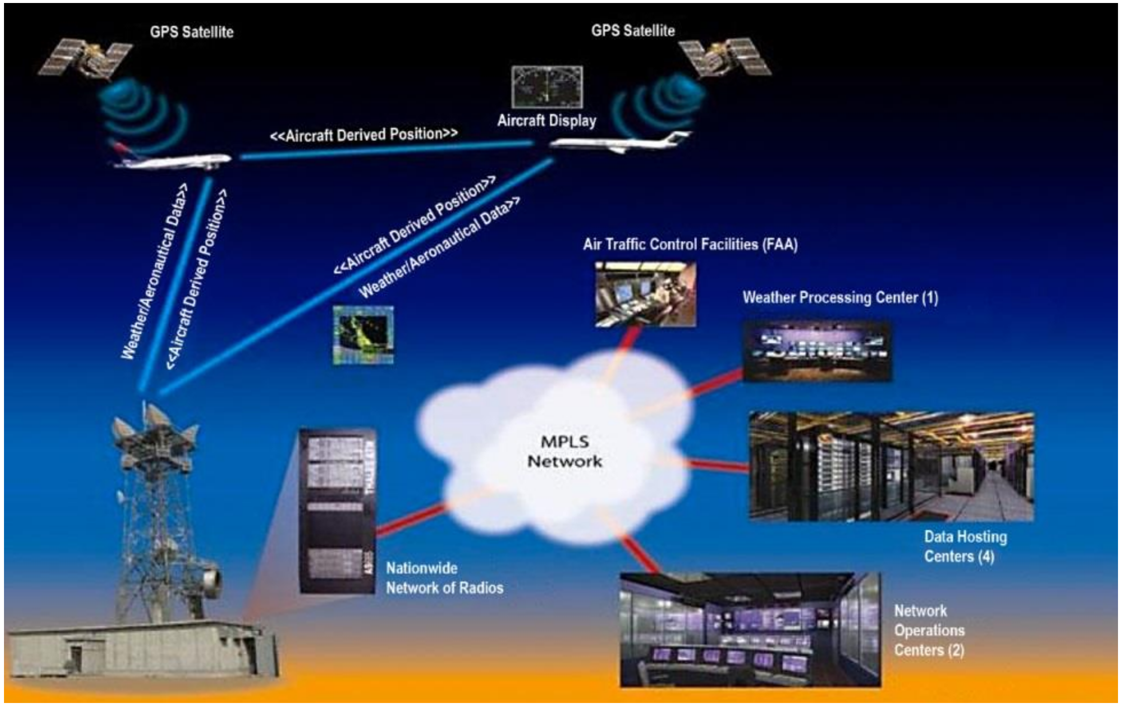
[IHO 2013]

- Human assuming more supervisory roles over automation, requiring more cognitively complex human decision making

National Airspace Upgrades

- Increased coupling and inter-connectivity among airborne, ground, and satellite systems

- Control shifting from ground to aircraft and shared responsibilities



[IHO 2013]

National Airspace Upgrades

- Attempts to re-engineer the NAS in the past have been not been terribly successful and have been very slow, partly due to inability to assure safety of the changes.

- Question: How can NAS be re-engineered incrementally without negatively impacting safety?

- Hypothesis:
  - Rethinking of how to do safety assurance required to successfully introduce NextGen concepts
  - Applying a new approach to safety based on systems theory can improve our ability to assure safety in these complex systems

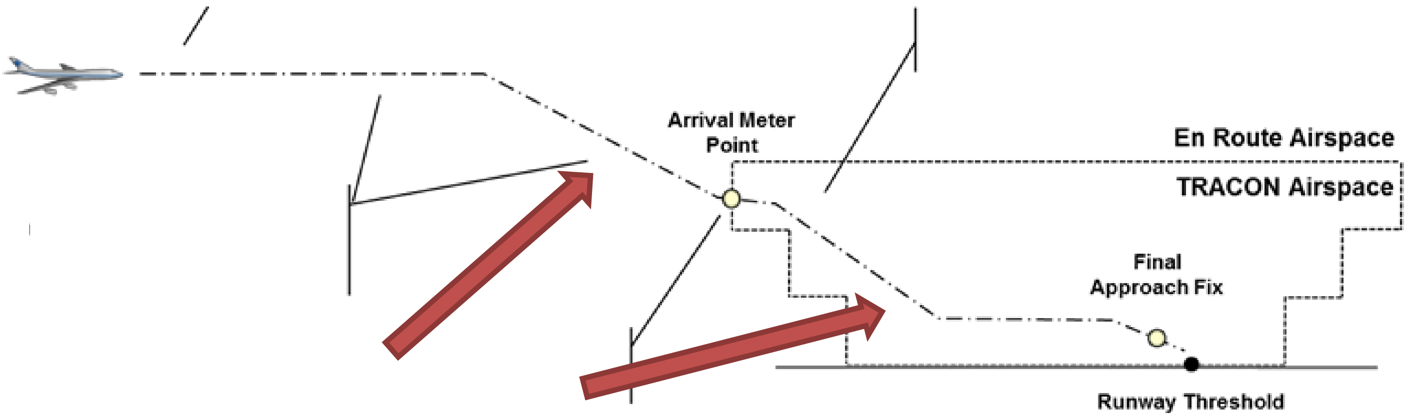
Agenda

- Background
- NextGen Example
- Analysis
- Future

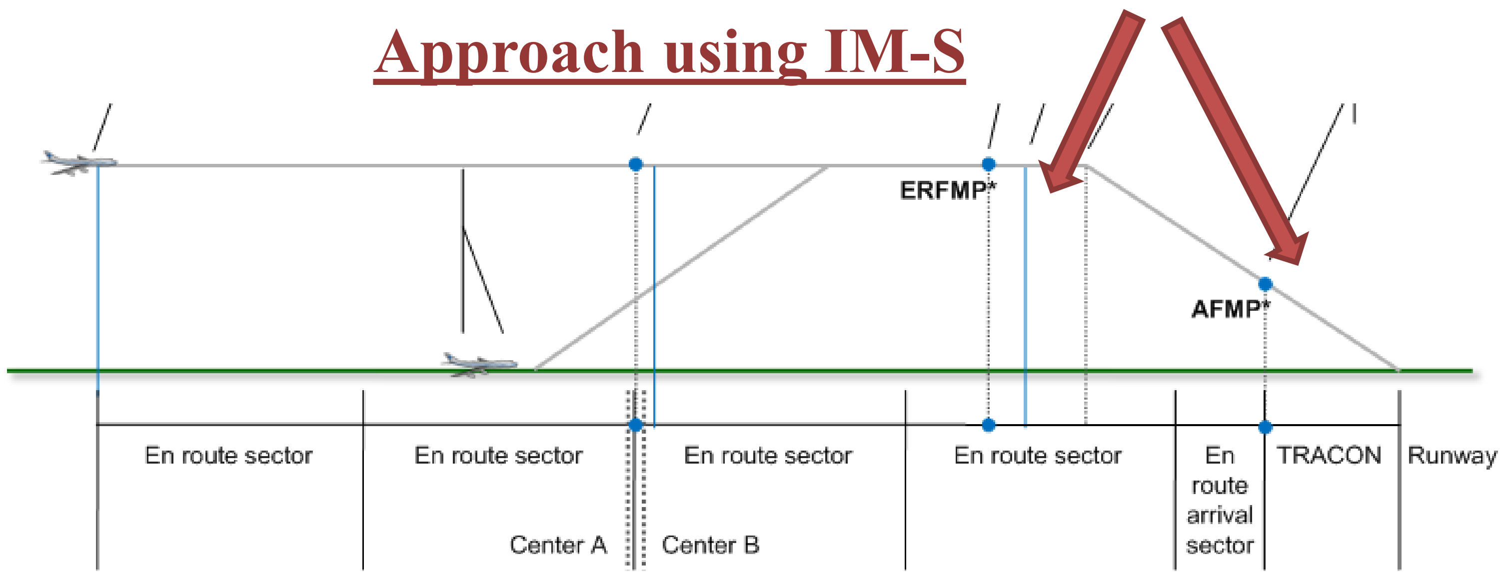
Interval Management – Spacing

- Arrival Interval Management – Spacing (IM-S) concept facilitates use of flow management constraints, while
  - Enabling efficient descent patterns (OPDs)
  - Reducing congestion in the arrival sector
  - Increasing throughput

Traditional Approach



Approach using IM-S



[FAA 2013]

2 Versions of IM-S

SERL MIT AEROASTRO

Ground-based (GIM-S)

Domain	Capability
Center TFM	• Trajectory modeling • CDT/FMT constraint assignment • Speed advisory generation and validation without sector-level problem status
En route ATC	Speed advisory • Notification • Indicators • Responses • Display control
Terminal ATC	Tower • Constraint List
Flight deck	ADS-B Out (optional)

[FAA 2013]

Flight Deck-Based (FIM-S)

Domain	Capability
Flight crew	• determining if an IM Operation is desirable; • determining the IM Aircraft, the Target Aircraft, the Assigned Spacing Goal and all other IM Clearance information; verifying that all initiation criteria are met … • communicating the IM Clearance to the IM Aircraft; • ensuring separation between the IM Aircraft and all other aircraft, including the Target Aircraft; • terminating the IM Operation if the ATM goal is no longer applicable or is not being met • resuming non-IM Operations whenever the IM Operation is terminated.

[RTCA 2011]

2 Versions of IM-S

SERL MIT AEROASTRO

Ground-based (GIM-S)

Domain	Capability
Center TFM	• Trajectory modeling • CDT/FMT constraint assignment • Speed advisory generation and validation without sector-level problem status
En route ATC	Speed advisory • Notification • Indicators • Responses • Display control
Terminal ATC	Tower • Constraint List
Flight deck	ADS-B Out (optional)

Flight Deck-Based (FIM-S)

Domain	Capability
Flight crew	• determining whether to accept or reject the IM Clearance; • making the IM Clearance information available to the FIM Equipment; confirming Target Aircraft Identification to the controller; • determining if ownship (i.e., IM Aircraft) is capable of performing the instructed maneuvers • informing the controller whether they accept or reject the IM Clearance; • following the IM Speed and IM Turn Point provided; • monitoring conformance with the IM Clearance; and • informing the controller when the flight crew wishes to terminate the IM Operation.

[FAA 2013]

Agenda

- Background
- NextGen Example
- Analysis
- Future

Analysis Process

- Identify accidents and hazards to be analyzed
- Systems-Theoretic Process Analysis (STPA)
  1. Draw the control structure
     - Identify major components and controllers
     - Label the control/feedback arrows
  2. Identify Unsafe Control Actions (UCAs)
     - Derive corresponding safety constraints
  3. Identify Causal Factors
     - Create controller process models
     - Analyze controller, control/feedback paths, process

Hazards Considered

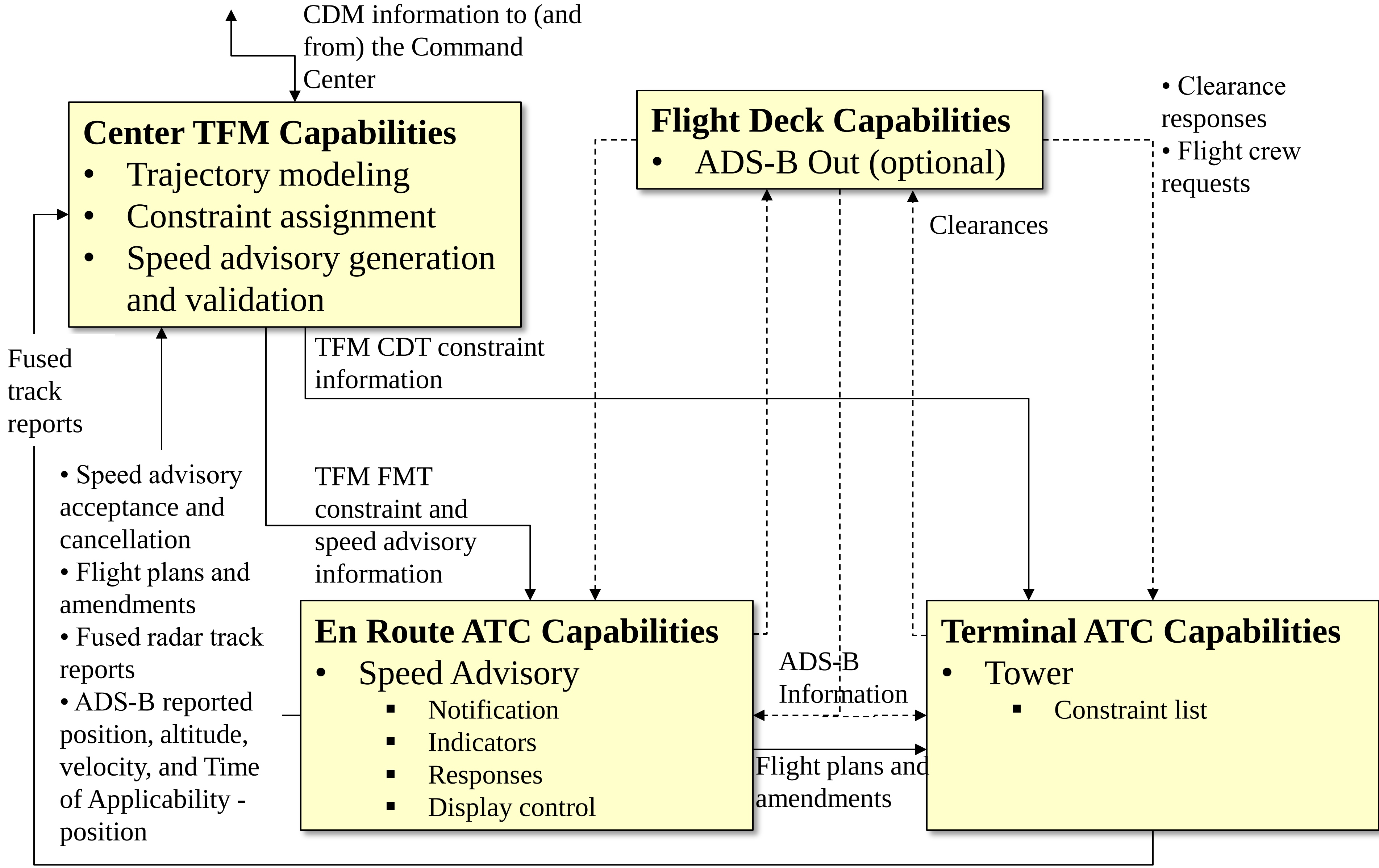
- H-1: A pair of controlled aircraft violate minimum separation standards (LOS)
- H-2: Aircraft enters unsafe atmospheric region
- H-3: Aircraft enters uncontrolled state
- H-4: Aircraft enters unsafe attitude
- H-5: Aircraft enters a prohibited area

Analysis Process

- Identify accidents and hazards to be analyzed
- Systems-Theoretic Process Analysis (STPA)

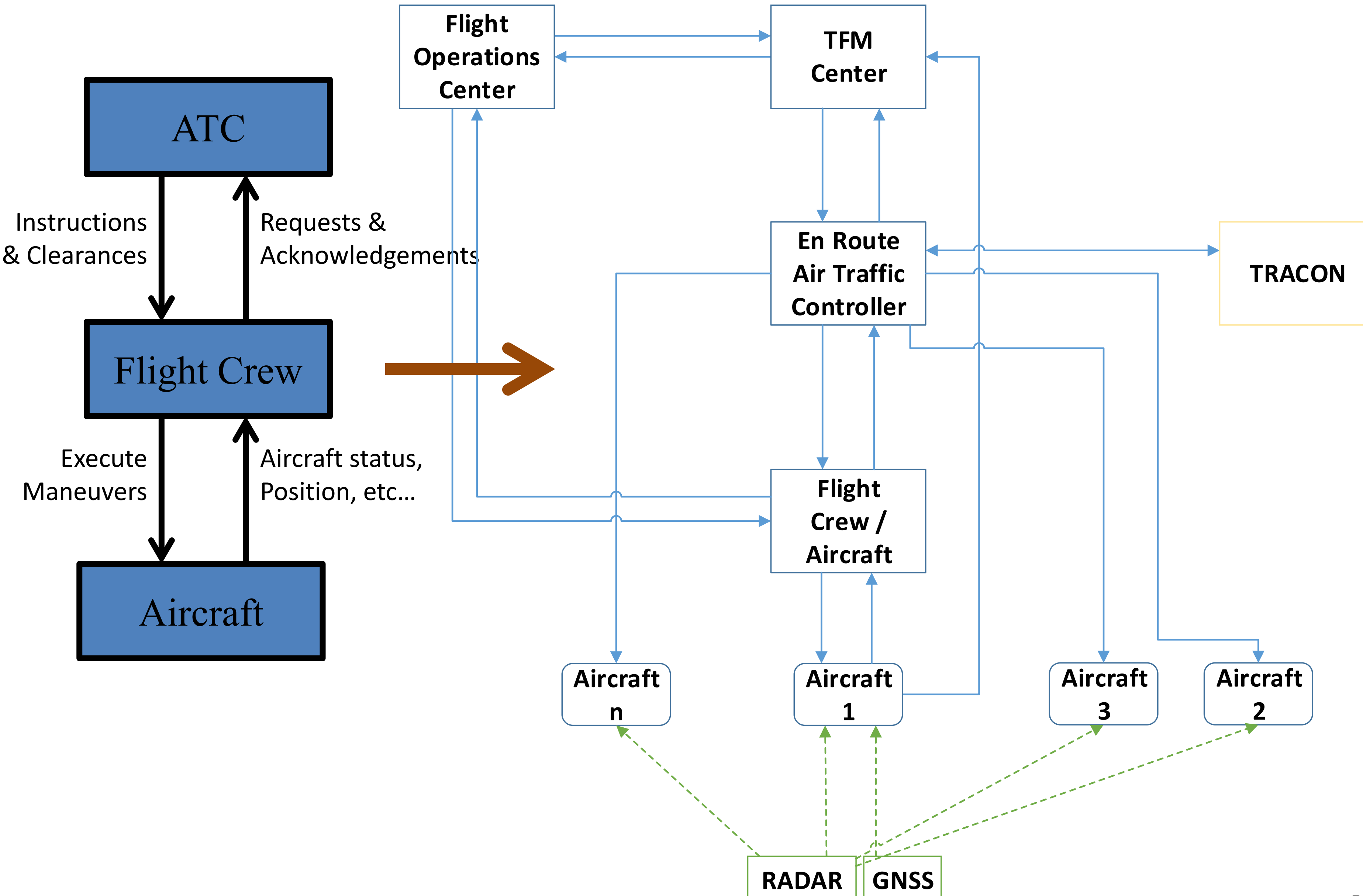
1. Draw the control structure
   - Identify major components and controllers
   - Label the control/feedback arrows
2. Identify Unsafe Control Actions (UCAs)
   - Derive corresponding safety constraints
3. Identify Causal Factors
   - Create controller process models
   - Analyze controller, control/feedback paths, process

Ground-based IM-S (GIM-S)



[IM-S ConOps]

GIM-S Control Structure



Analysis Process

- Identify accidents and hazards to be analyzed
- Systems-Theoretic Process Analysis (STPA)

1. Draw the control structure
   - Identify major components and controllers
   - Label the control/feedback arrows
2. Identify Unsafe Control Actions (UCAs)
   - Derive corresponding safety constraints
3. Identify Causal Factors
   - Create controller process models
   - Analyze controller, control/feedback paths, process

Unsafe Control Actions

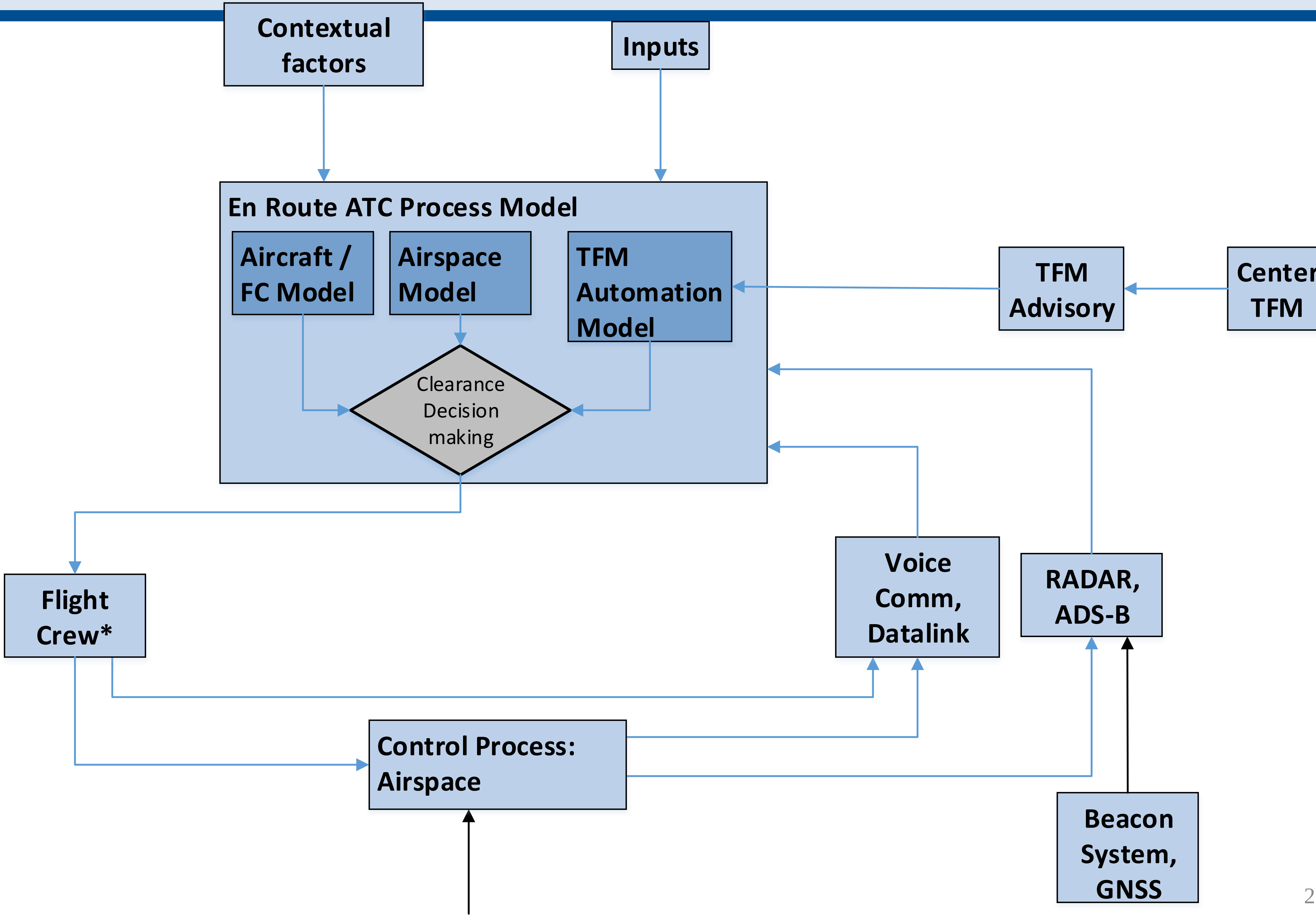
Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Modify Speed	Not providing a speed modification is hazardous when the current speed leads to LOS	Providing a speed modification is hazardous if it is the incorrect speed	Providing a speed modification to aircraft "i" is hazardous if given after (before) a related clearance* was already provided to aircraft "j"	
		Providing a speed modification is hazardous if it exceeds the aircraft capability (overspeed or stall)	Providing speed modification too late after conditions (e.g. weather, aircraft speed, heading, etc) in TBFM trajectory model have changed	

[Not a full table. Full table shown in backup slides]

Analysis Process

- Identify accidents and hazards to be analyzed
- Systems-Theoretic Process Analysis (STPA)
  1. Draw the control structure
     - Identify major components and controllers
     - Label the control/feedback arrows
  2. Identify Unsafe Control Actions (UCAs)
     - Derive corresponding safety constraints
  3. Identify Causal Factors
     - Create controller process models
     - Analyze controller, control/feedback paths, process

Create Controller Process Models



Controller Process Model Example

- OPDs are an increasingly important aspect of traffic mgmt
- En route interval management has different level of priority now than in the past
- Different downstream sectors might have different capacity constraints
- Own sector traffic demands vs up/down stream demands

Contextual factors

Inputs

- Procedures from FAA (?)
- Downstream capacity updates
- Upstream traffic constraints

En Route ATC Process Model

Aircraft / FC Model
- Aircraft type
- Aircraft capability (ascent/ descent rate, stall speed)
- Aircraft ID
- Current location
- Current airspeed, vertical speed,
- Current altitude
- Current advisory(ies)

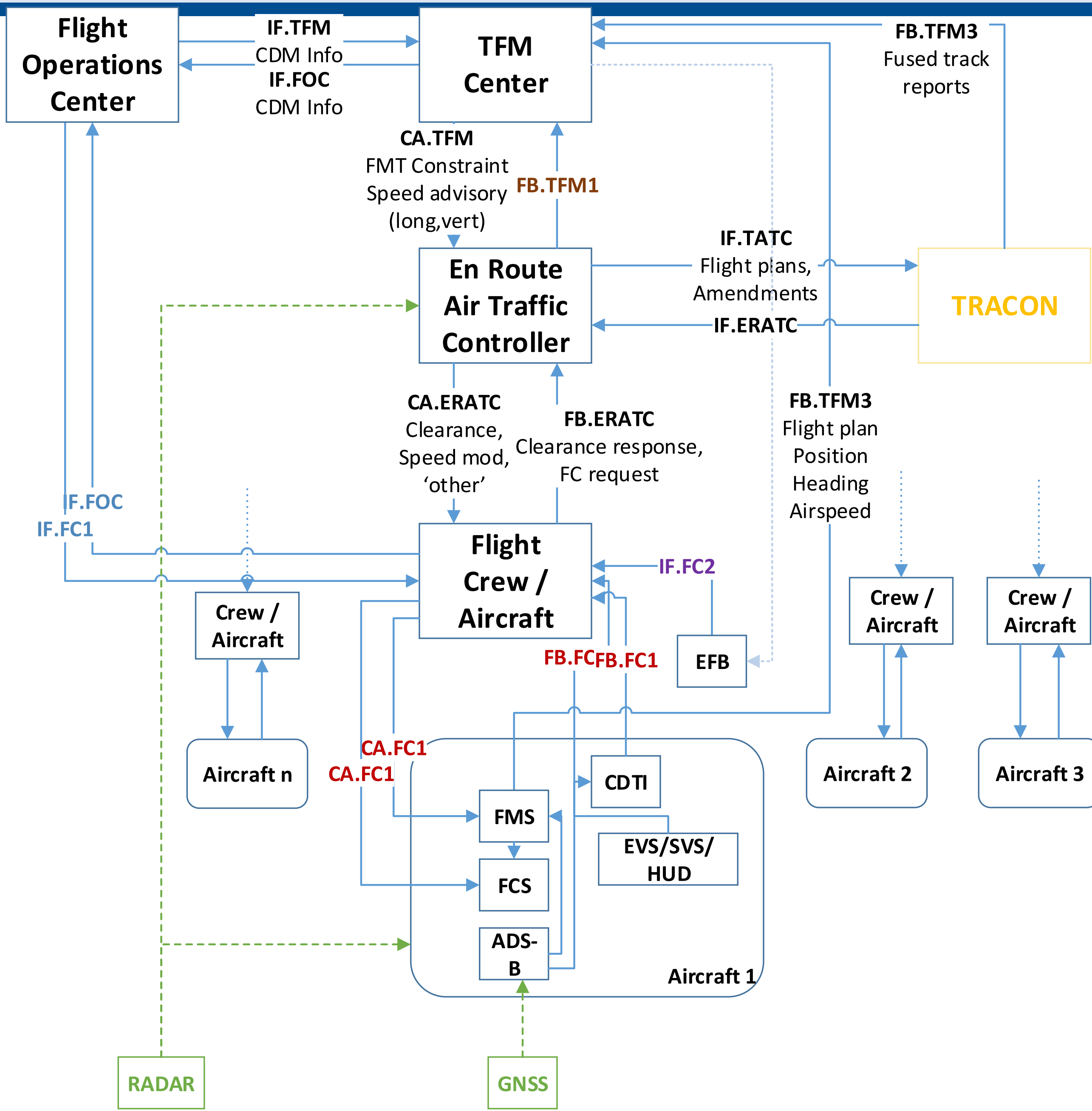
Airspace Model
- Separation requirement
- Current separation, own airspace
- Predicted separation, own airspace
- Current downstream sector (TRACON) capacity
- Predicted downstream sector (TRACON) capacity
- Environment (wind, convective weather)

TFM Automation Model
- Sequence algorithm (how it decides which aircraft go first in flow)
- Trajectory model
- CDT / FMT constraint assignment, list
- User interface (how information is displayed, user options, modifications

TFM Advisory

Clearance decision making

Overall GIM-S Control Structure



CA.FC1
- Input flight plan
- Modify flight plan

CA.FC1
- Modify airspeed
- Modify altitude
- Modify heading

FB.TFM1
- Speed advisory acceptance & cancellation
- Flight plans and amendments
- Fused radar track reports
- ADS-B reported position, alt, speed, and Time of Applicability (position)

IF.FC2
- Nav charts
- Op manual for a/c

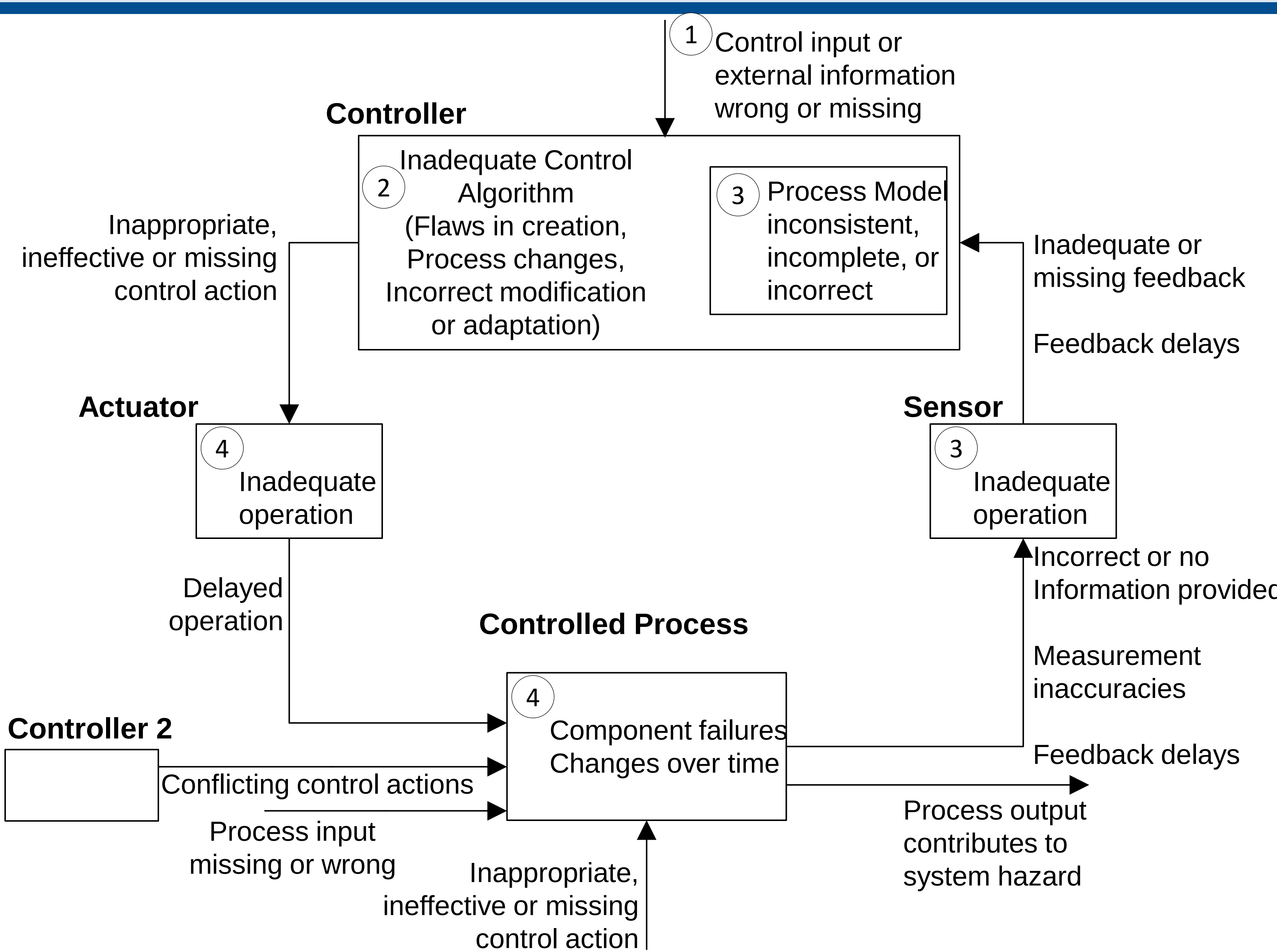
FB.FC1
- Ownship position
- Other a/c position
- Weather

FB.FC1
- Heading
- Angle of attack
- Airspeed

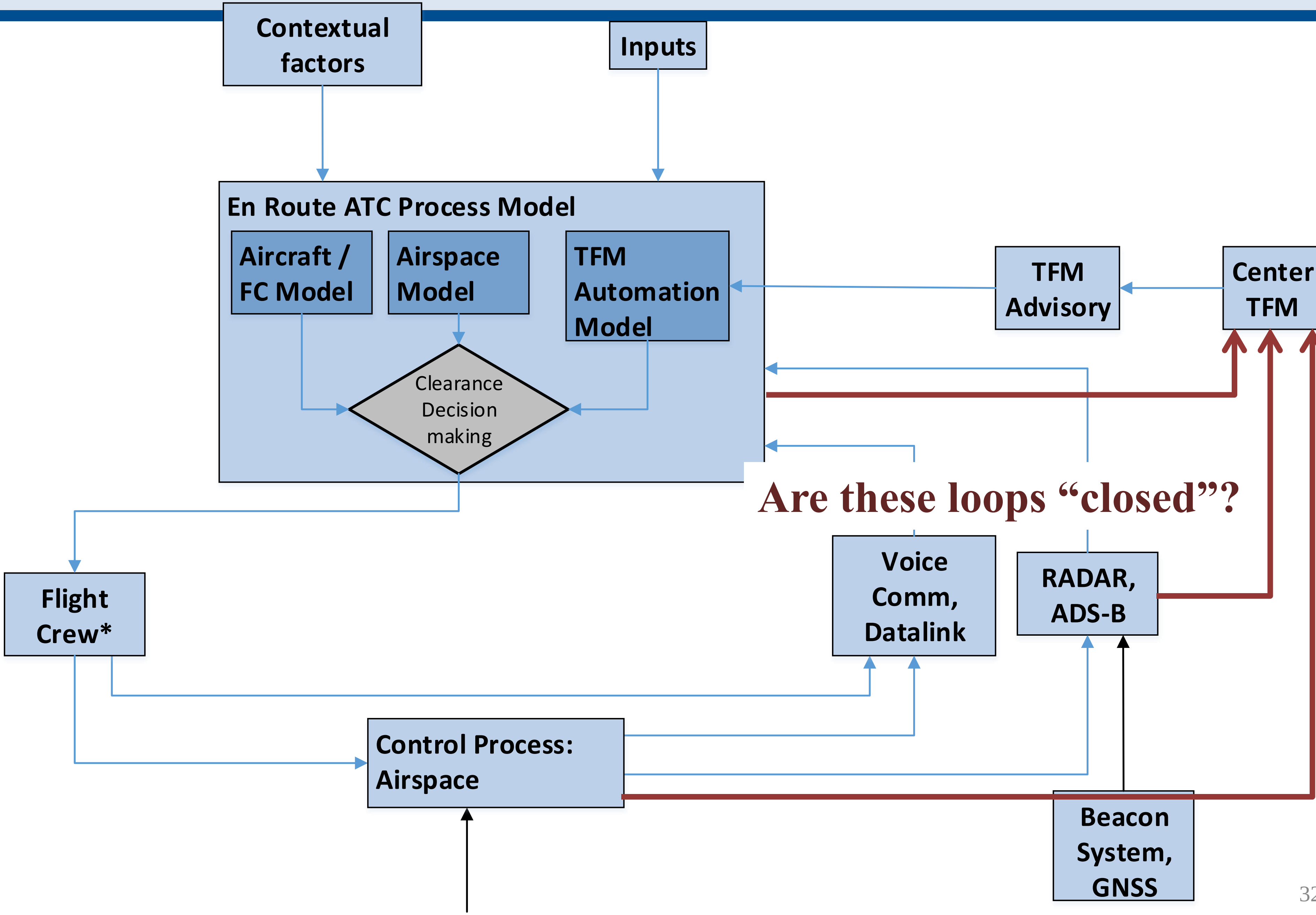
Analysis Process

- Identify accidents and hazards to be analyzed
- Systems-Theoretic Process Analysis (STPA)
  1. Draw the control structure
     - Identify major components and controllers
     - Label the control/feedback arrows
  2. Identify Unsafe Control Actions (UCAs)
     - Derive corresponding safety constraints
  3. Identify Causal Factors
     - Create controller process models
     - Analyze controller, control/feedback paths, process

Identifying Causal Factors



Checking for Missing Feedback



Are these loops "closed"?

Example from IM-S ConOps

- "In some cases, operational conditions in the sector may not support the controller's acceptance of a speed advisory. For these cases, controllers can enter the advisory rejection into the automation, allow the advisory to time out, or choose a different speed (these responses are not sent to the TFM automation)"
  [SBS IM-S ConOps, 2013]

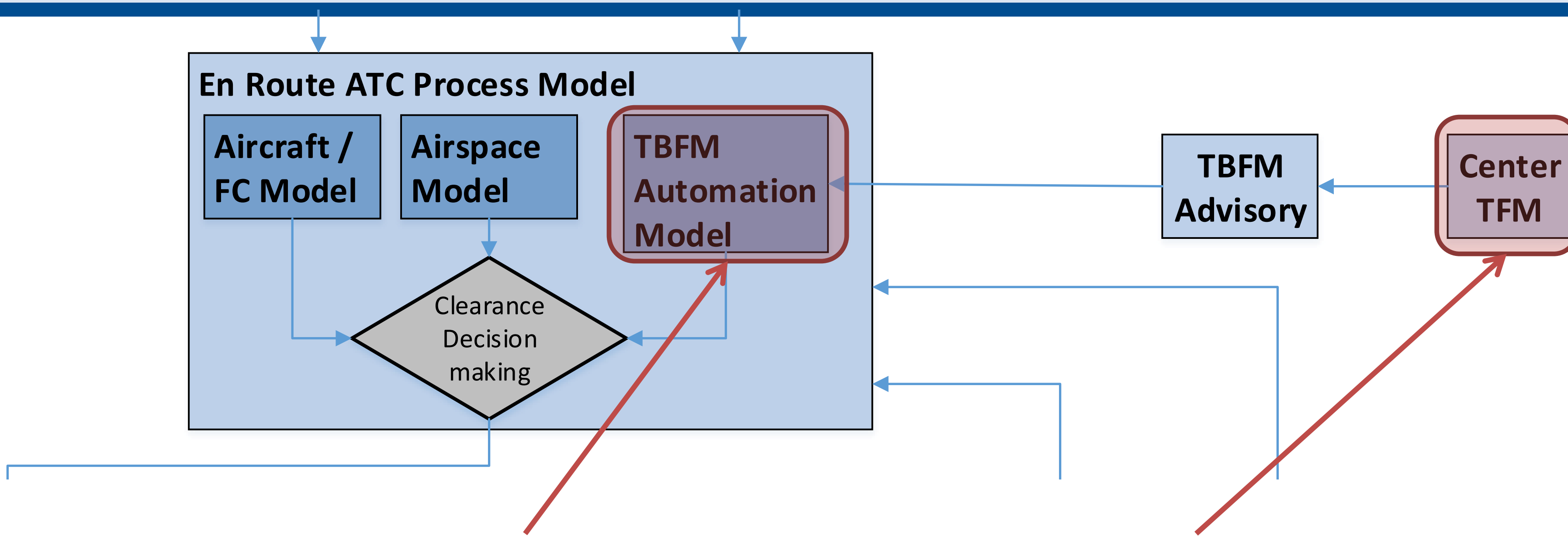
Example from IM-S ConOps

- "In some cases, operational conditions in the sector may not support the controller's acceptance of a speed advisory. For these cases, controllers can enter the advisory rejection into the automation, allow the advisory to time out, or choose a different speed (*these responses are not sent to the TFM automation*)"

  [SBS IM-S ConOps, March 2013, emphasis added]

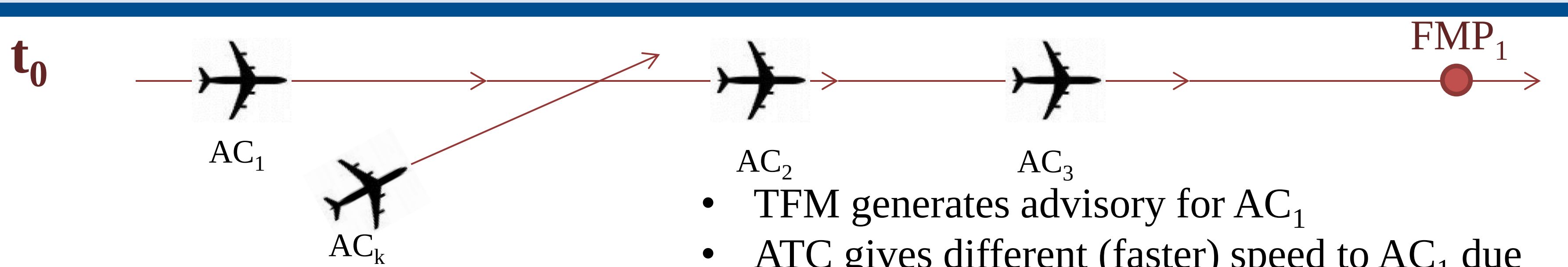
Potential question about design:
Is feedback missing for TFM automation?

Example Causal Factor



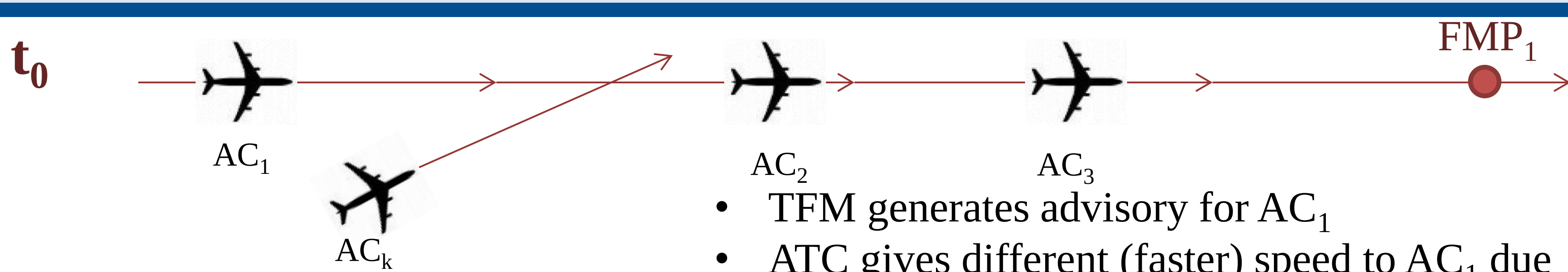
- ATC process model flaw
  - ATC believes that TFM automation is using same data as he/she sees
  - ATC believes TFM uses same 'algorithm' (procedure) to determine advisories
- TFM process model flaw
  - Inaccurate information about airspace
  - e.g. Amended flight plan not provided for trajectory modeling
  - e.g. Aircraft 1 in scenario (following slides) not ADS-B equipped, or ADS-B not updated correctly

Scenario

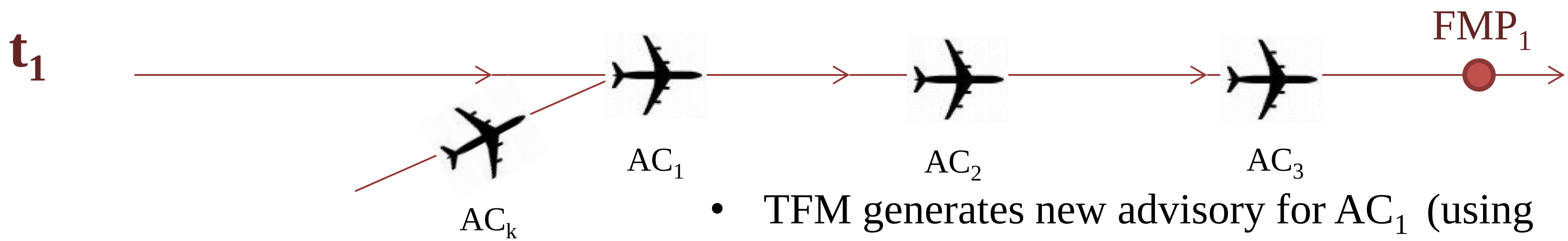


- TFM generates advisory for AC$_1$
- ATC gives different (faster) speed to AC$_1$ due to conflict with AC$_k$
- ATC lets TFM advisory time out

Scenario

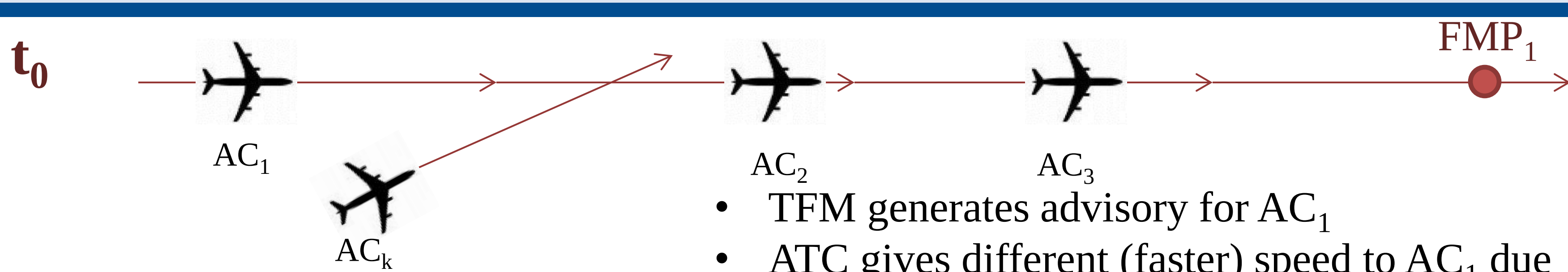


- TFM generates advisory for AC$_1$
- ATC gives different (faster) speed to AC$_1$ due to conflict with AC$_k$
- ATC lets TFM advisory time out

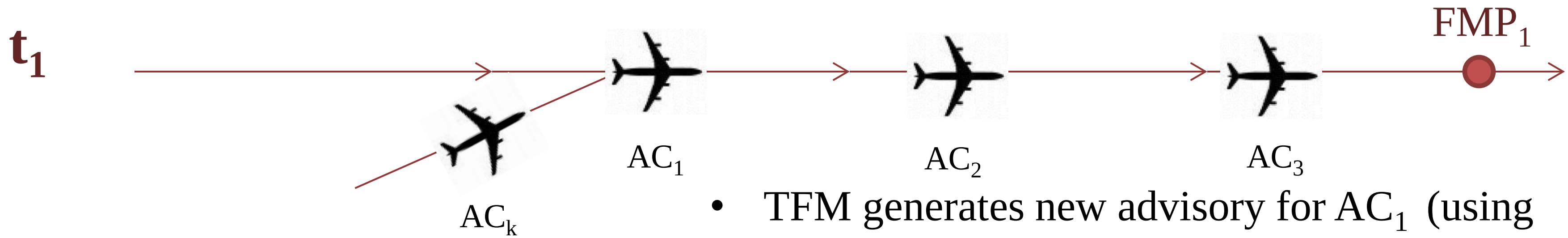


- TFM generates new advisory for AC$_1$ (using assumptions based on t_0 condition)
- ATC accepts advisory

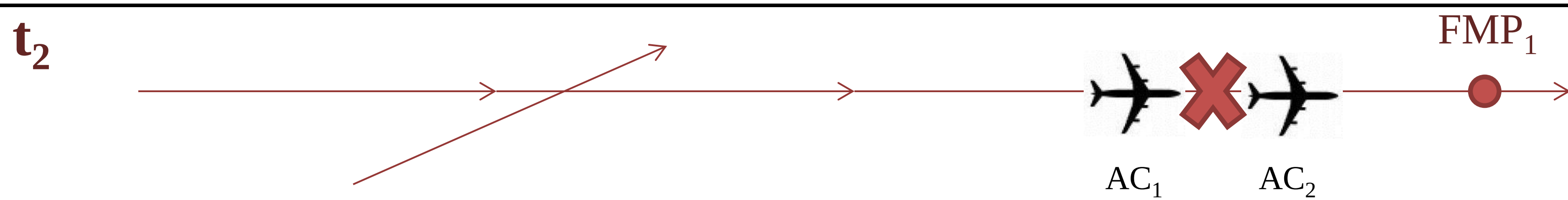
Scenario



- TFM generates advisory for AC_1
- ATC gives different (faster) speed to AC_1 due to conflict with AC_k
- ATC lets TFM advisory time out

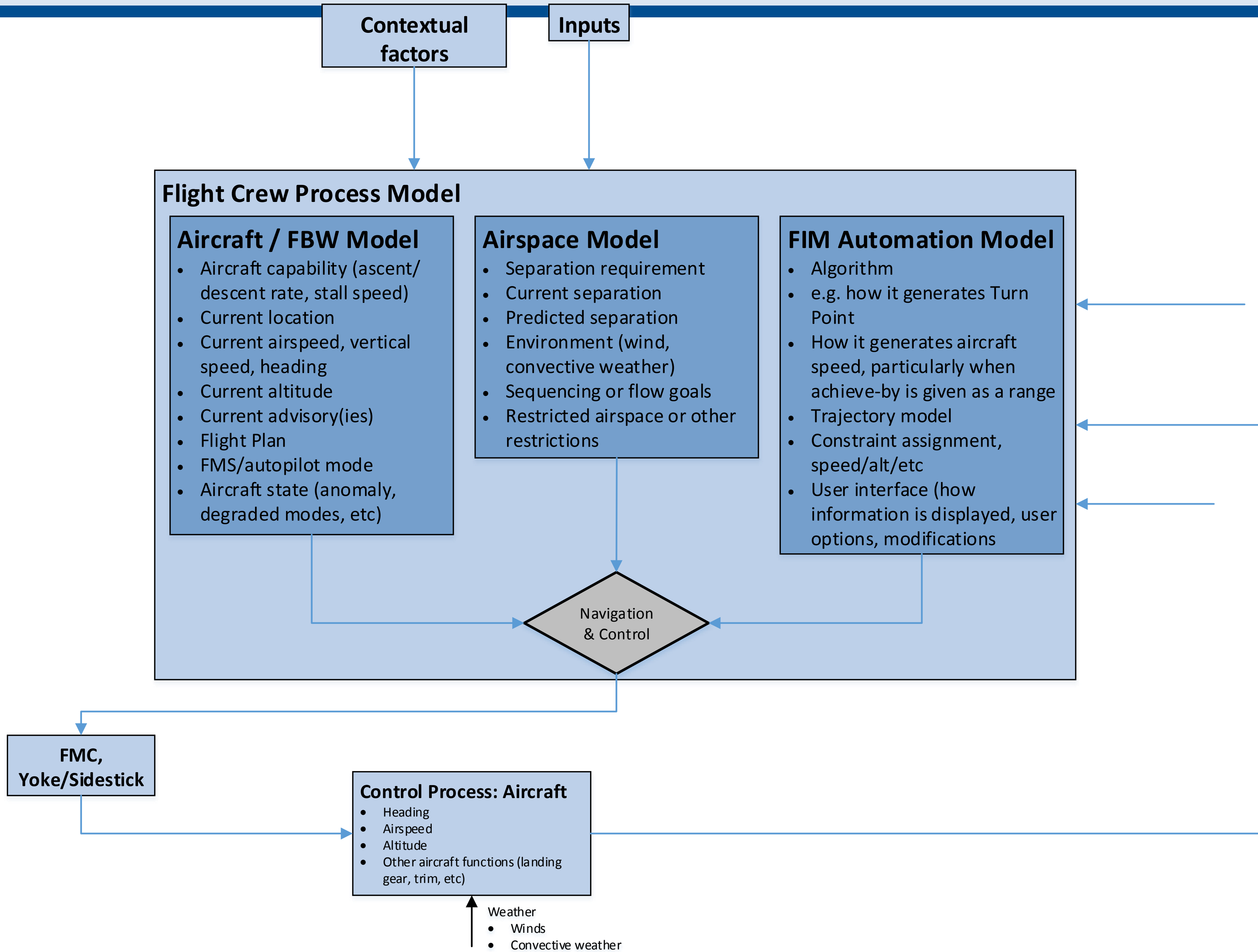


- TFM generates new advisory for AC_1 (using assumptions based on t_0 condition)
- ATC accepts advisory



- At t_1, TFM did not have updated model of aircraft position
- ATC did not update flight plan due to concentration on conflict

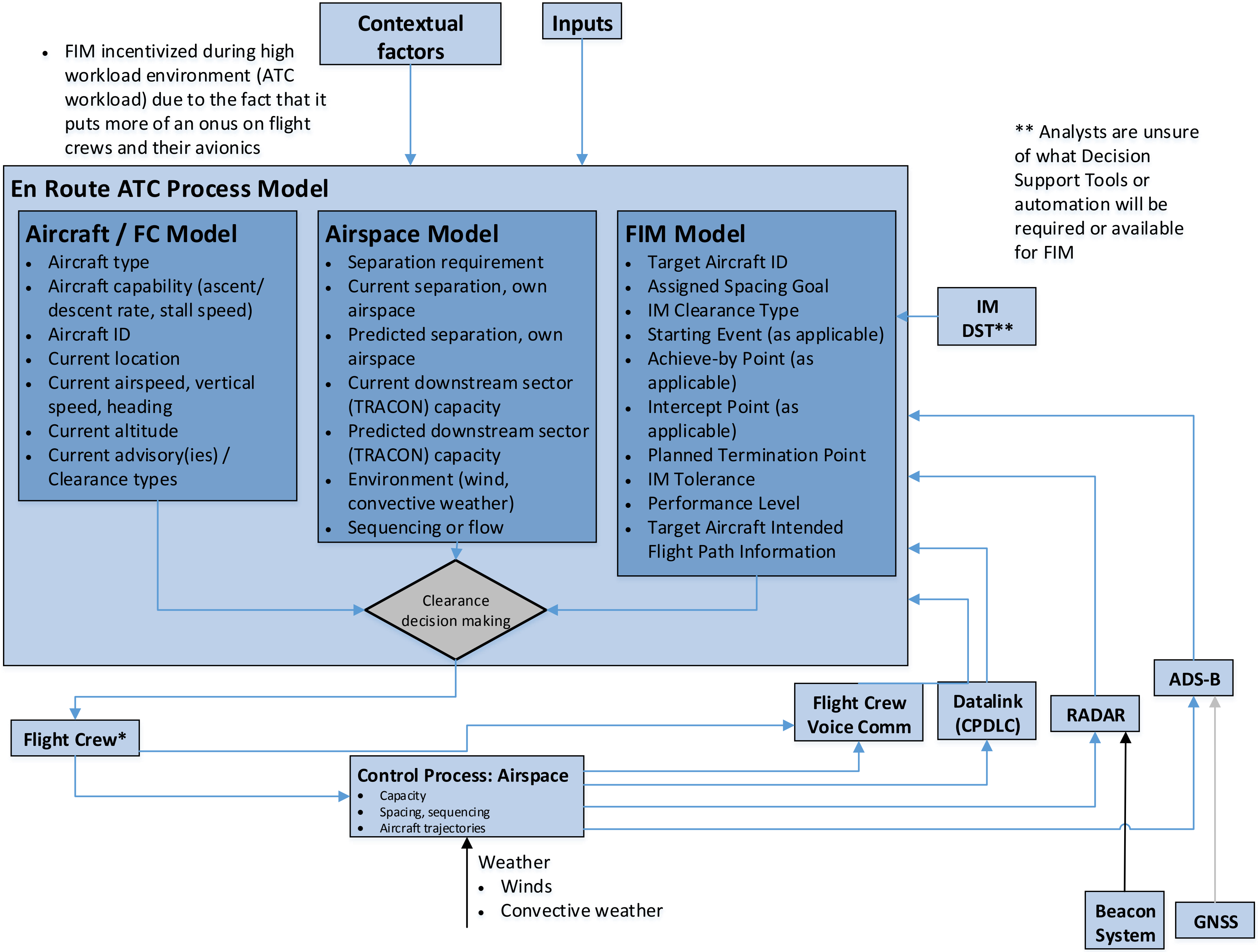
FIM Analysis – Flight Crew



FIM Analysis – ATC

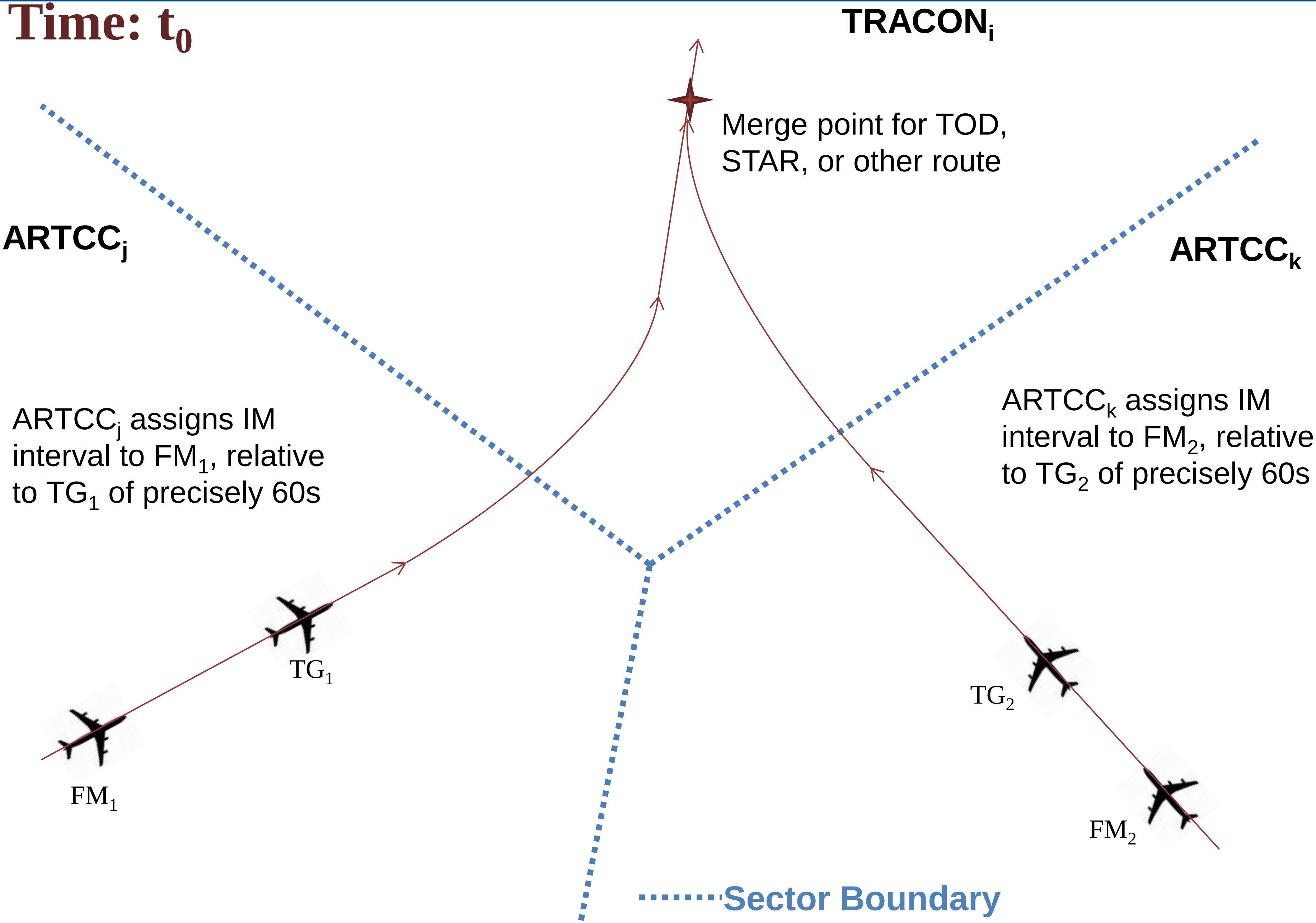
- FIM incentivized during high workload environment (ATC workload) due to the fact that it puts more of an onus on flight crews and their avionics

** Analysts are unsure of what Decision Support Tools or automation will be required or available for FIM

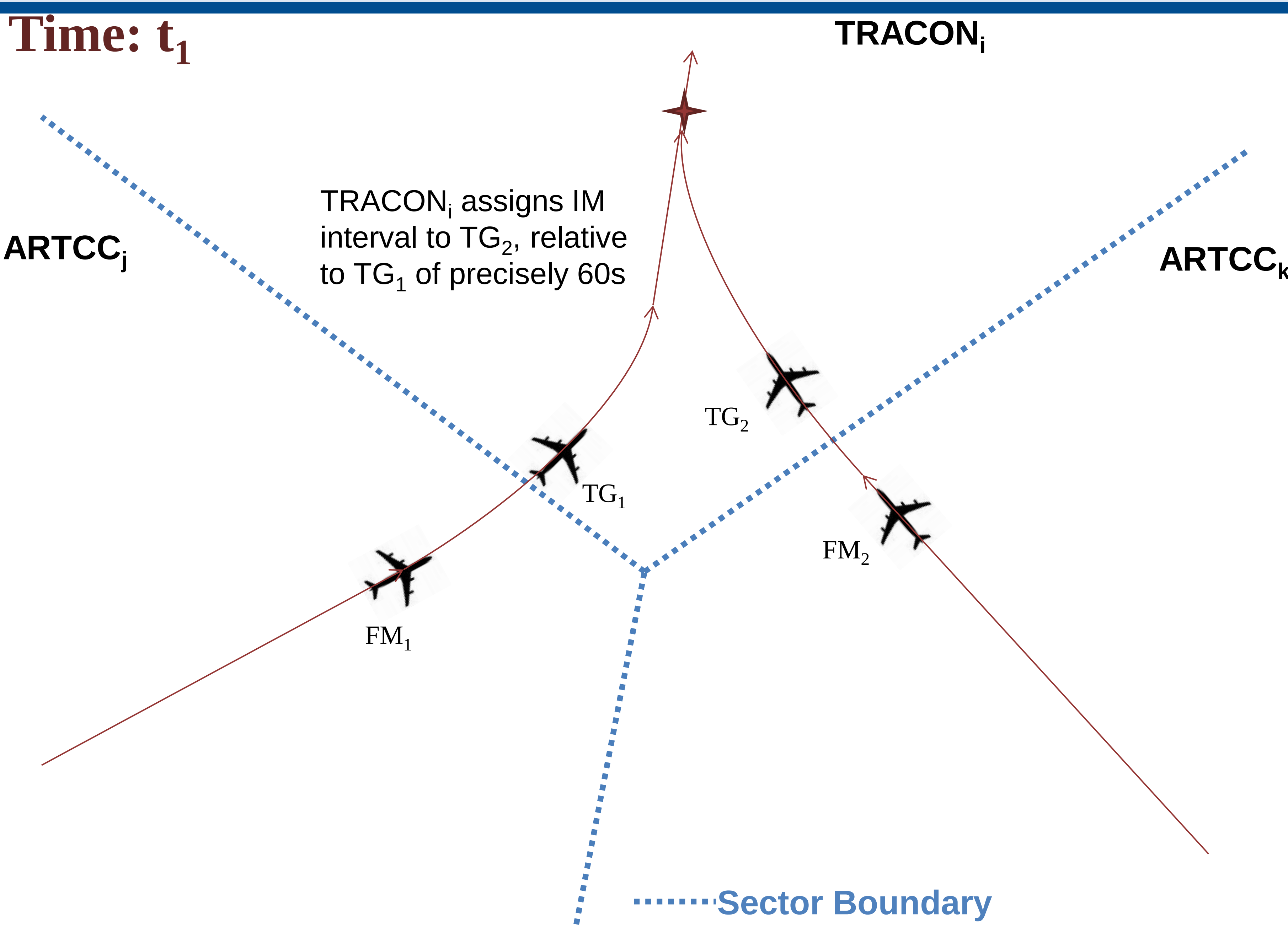


Scenario

Time: t_0

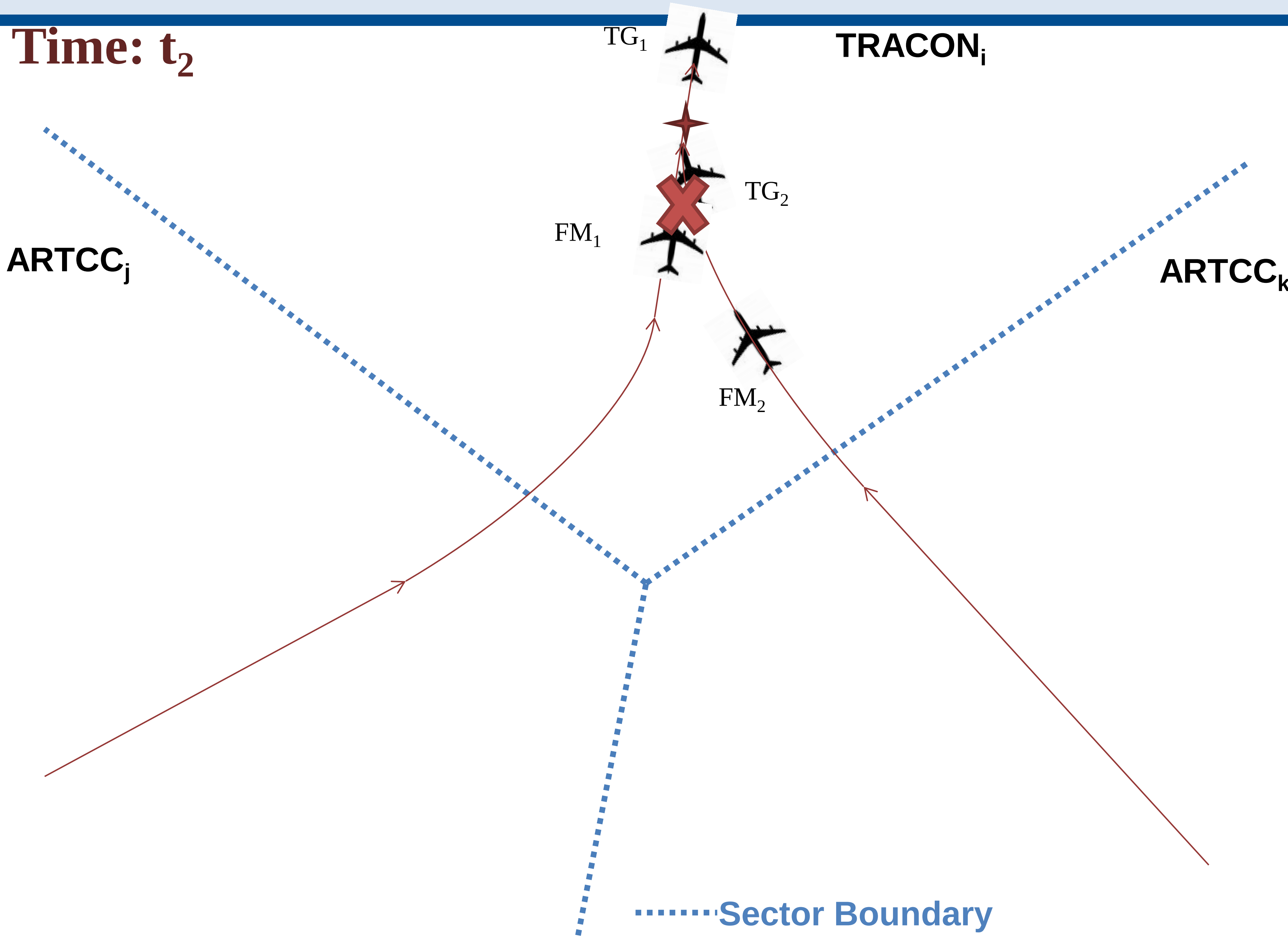


Scenario



Time: t_1
TRACON$_i$
TRACON$_i$ assigns IM interval to TG$_2$, relative to TG$_1$ of precisely 60s
ARTCC$_j$
ARTCC$_k$
TG$_2$
TG$_1$
FM$_2$
FM$_1$
Sector Boundary

Scenario



Time: t_2
TG_1
$TRACON_i$
TG_2
FM_1
$ARTCC_j$
$ARTCC_k$
FM_2
Sector Boundary

Agenda

- Background
- NextGen Example
- Analysis
- Future

Current & Future Work

- Can we do the analysis even *earlier*?
  - Analyze concepts with less maturity
  - Assist decision-makers in design
  - Actually develop concepts?

References

1. AO-2010-089, In-flight uncontained engine failure Airbus A380-842, VH-OQA, overhead Batam Island, Indonesia, Australian Transporation Safety Board, 4 November 2010
2. Rushe, D. Boeing 787 Dreamliner's failed battery was wired incorrectly, Japan says, 20 February, 2013. http://www.theguardian.com/business/2013/feb/20/boeing-dreamliner-failed-battery-wired
3. Gara, T. FAA Statement: Boeing 787 Dreamliner Grounded, For Now, Wall Street Journal Blog, 16 January 2013.
4. Society of Automotive Engineers, SAE International. Guidelines for Development of Civil Aircraft and Systems, Aerospace Recommended Practice, ARP4754 REV. A, Issued 1996-11, Revised 2010-12
5. Kapurch, Stephen J., ed. NASA Systems Engineering Handbook. DIANE Publishing, 2010.
6. Surveillance and Broadcast Services (SBS) Concept of Operations Arrival Interval Management – Spacing (IM-S), PMO-010, Revision 02, Final March 1, 2013
7. IHO blog, http://iho.hu/blogpost/jelek-a-magasbol-1-radarokrol-transzponderekrol-131105, 11/6/2013, accessed 17 March 2014
8. FAA Surveillance and Broadcast Services (SBS) Concept of Operations. Arrival Interval Management – Spacing (IM-S) Concept of Operations for the Mid-Term Timeframe, PMO-010, Revision 02 Final March 1, 2013
9. RTCA. Safety, Performance and Interoperability Requirements Document for Airborne Spacing – Flight Deck Interval Management (ASPA-FIM), RTCA DO-328 Prepared by: SC-186, June 22, 2011
10. Interagency Airpsace Coordination, FAA and USDA, http://airspacecoordination.org/guide/index.html, accessed 22 March 2014
11. Ascent Ground School, http://www.ascentgroundschool.com/index.php/faa-references/instrument-flying-handbook/151-chapter-8-the-national-airspace-system, copyright 2013, accessed 22 March 2014
12. Aviation News, http://www.aviationnews.eu/2011/09/08/lockheed-martin-upgrades-air-traffic-control-system-in-nation%E2%80%99s-second-busiest-airspace/, Copyright 2014, accessed 23 March 2014