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

Cody Fleming

March 26, 2014
Agenda

• Background
• NextGen Example
• Analysis
• Future
Motivation

• Shuttle

• B787

[Wiki Commons 1986, WSJ 2013, Guardian 2013]
Systems Engineering Timeline

Concept → Function → Architecture → Design → Implementation → Production, test & operation data

[ARP-4754 2010]
Systems Engineering Timeline

Concept

Function → Architecture → Design → Implementation → Production, test & operation data

Development

Production/Operation

[ARP-4754 2010]
Current flight-critical systems remarkably safe due to:
National Airspace Effectiveness

• Conservative adoption of new technologies
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

- 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
Interval Management – Spacing

Traditional Approach

Approach using IM-S

[FAA 2013]
## 2 Versions of IM-S

### Ground-based (GIM-S)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center TFM</td>
<td>• Trajectory modeling&lt;br&gt;• CDT/FMT constraint assignment&lt;br&gt;• Speed advisory generation and validation without sector-level problem status</td>
</tr>
<tr>
<td>En route ATC</td>
<td>Speed advisory&lt;br&gt;• Notification&lt;br&gt;• Indicators&lt;br&gt;• Responses&lt;br&gt;• Display control</td>
</tr>
<tr>
<td>Terminal ATC</td>
<td>Tower&lt;br&gt;• Constraint List</td>
</tr>
<tr>
<td>Flight deck</td>
<td>ADS-B Out (optional)</td>
</tr>
</tbody>
</table>

### Flight Deck-Based (FIM-S)

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and all other aircraft, including the Target Aircraft;&lt;br&gt;• terminating the IM Operation if the ATM goal is no longer applicable or is not being met&lt;br&gt;• resuming non-IM Operations whenever the IM Operation is terminated.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

[FAA 2013]

[RTCA 2011]
## 2 Versions of IM-S

### Ground-based (GIM-S)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center TFM</td>
<td>• Trajectory modeling&lt;br&gt;• CDT/FMT constraint assignment&lt;br&gt;• Speed advisory generation and validation without sector-level problem status</td>
</tr>
<tr>
<td>En route ATC</td>
<td>Speed advisory&lt;br&gt;• Notification&lt;br&gt;• Indicators&lt;br&gt;• Responses&lt;br&gt;• Display control</td>
</tr>
<tr>
<td>Terminal ATC</td>
<td>Tower&lt;br&gt;• Constraint List</td>
</tr>
<tr>
<td>Flight deck</td>
<td>ADS-B Out (optional)</td>
</tr>
</tbody>
</table>

### Flight Deck-Based (FIM-S)

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

[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)

**Center TFM Capabilities**
- Trajectory modeling
- Constraint assignment
- Speed advisory generation and validation

**Flight Deck Capabilities**
- ADS-B Out (optional)

**En Route ATC Capabilities**
- Speed Advisory
  - Notification
  - Indicators
  - Responses
  - Display control

**Terminal ATC Capabilities**
- Tower
  - Constraint list

**Clearances**
- Clearance responses
- Flight crew requests

**Fused track reports**
- Speed advisory acceptance and cancellation
- Flight plans and amendments
- Fused radar track reports
- ADS-B reported position, altitude, velocity, and Time of Applicability - position

**TFM CDT constraint information**

**TFM FMT constraint and speed advisory information**

**CDM information to (and from) the Command Center**

[IM-S ConOps]
GIM-S Control Structure

ATC

Instructions & Clearances

Requests & Acknowledgements

Flight Crew

Execute Maneuvers

Aircraft status, Position, etc...

Aircraft

Flight Operations Center

TFM Center

En Route Air Traffic Controller

Flight Crew / Aircraft

Aircraft 1

Aircraft 3

Aircraft 2

Aircraft n

RADAR

GNSS

TRACON
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

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

**Contextual factors**

- **En Route ATC Process Model**
  - Aircraft / FC Model
  - Airspace Model
  - TFM Automation Model
  - Clearance Decision making

**Inputs**

- **Control Process: Airspace**
  - Flight Crew*

**Outputs**

- **TFM Advisory**
- **Center TFM**
- **Voice Comm, Datalink**
- **RADAR, ADS-B**
- **Beacon System, GNSS**
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

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)

Clearance decision making

Contextual factors

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

TFM Advisory

Datalink (CPDLC)

ADS-B

Flight Crew Voice Comm
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

1. Control input or external information wrong or missing

2. Inadequate Control Algorithm (Flaws in creation, Process changes, Incorrect modification or adaptation)

3. Process Model inconsistent, incomplete, or incorrect

Controller

Actuator

Inappropriate, ineffective or missing control action

Inadequate operation

Delayed operation

Conflicting control actions

Process input missing or wrong

Inappropriate, ineffective or missing control action

Sensor

Controller 2

Inadequate operation

Process input missing or wrong

Information provided

Measurement inaccuracies

Incorrect or no Information provided

Feedback delays

Inadequate or missing feedback

Process output contributes to system hazard

Controlled Process

Component failures

Changes over time
Checking for Missing Feedback

Are these loops “closed”?

Contextual factors

En Route ATC Process Model

Aircraft / FC Model
Airspace Model
TFM Automation Model

Clearance Decision making

Inputs

Control Process: Airspace

Flight Crew*

Voice Comm, Datalink

RADAR, ADS-B

Beacon System, GNSS

TFM Advisory

Center TFM
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
• 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

$t_0$  
- 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

$t_1$  
- TFM generates new advisory for $AC_1$ (using assumptions based on $t_0$ condition)
- ATC accepts advisory
Scenario

\[ t_0 \]

\[ AC_1 \]

\[ AC_k \]

\[ AC_2 \]

\[ AC_3 \]

- 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

\[ t_1 \]

\[ AC_1 \]

\[ AC_k \]

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

\[ t_2 \]

\[ AC_1 \]

\[ AC_2 \]

- 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

**Flight Crew Process Model**

**Aircraft / FBW Model**
- Aircraft capability (ascent/descent rate, stall speed)
- Current location
- Current airspeed, vertical speed, heading
- Current altitude
- Current advisory(ies)
- Flight Plan
- FMS/autopilot mode
- Aircraft state (anomaly, degraded modes, etc)

**Airspace Model**
- Separation requirement
- Current separation
- Predicted separation
- Environment (wind, convective weather)
- Sequencing or flow goals
- Restricted airspace or other restrictions

**FIM Automation Model**
- Algorithm
  - e.g. how it generates Turn Point
  - How it generates aircraft speed, particularly when achieve-by is given as a range
  - Trajectory model
  - Constraint assignment, speed/alt/etc
  - User interface (how information is displayed, user options, modifications)

**Contextual factors**

**Inputs**

**Navigation & Control**

**Control Process: Aircraft**
- Heading
- Airspeed
- Altitude
- Other aircraft functions (landing gear, trim, etc)

**FMC, Yoke/Sidestick**

**Weather**
- Winds
- Convective weather
**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

**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, heading
- Current altitude
- Current advisory(ies) / Clearance types

**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)
- Sequencing or flow

**FIM Model**
- Target Aircraft ID
- Assigned Spacing Goal
- IM Clearance Type
- Starting Event (as applicable)
- Achieve-by Point (as applicable)
- Intercept Point (as applicable)
- Planned Termination Point
- IM Tolerance
- Performance Level
- Target Aircraft Intended Flight Path Information

**Clearance decision making**

**Contextual factors**

**Inputs**

**Control Process: Airspace**
- Capacity
- Spacing, sequencing
- Aircraft trajectories

**Weather**
- Winds
- Convective weather

**Flight Crew**

**Flight Crew Voice Comm**

**Datalink (CPDLC)**

**RADAR**

**Beacon System**

**GNSS**

**IM DST**

**ADS-B**

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

Time: $t_0$

TRACON$_i$

Merge point for TOD, STAR, or other route

ARTCC$_j$

ARTCC$_k$

ARTCC$_j$ assigns IM interval to FM$_1$, relative to TG$_1$ of precisely 60s

ARTCC$_k$ assigns IM interval to FM$_2$, relative to TG$_2$ of precisely 60s

Sector Boundary
Scenario

Time: \( t_1 \)

TRACON_i assigns IM interval to TG_2, relative to TG_1 of precisely 60s
Scenario

Time: $t_2$

ARTCC$_j$  TRACON$_i$  ARTCC$_k$

Sector Boundary

FM$_1$  TG$_1$  TG$_2$  FM$_2$
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
6. Surveillance and Broadcast Services (SBS) Concept of Operations Arrival Interval Management – Spacing (IM-S), PMO-010, Revision 02, Final March 1, 2013
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