Including Safety during Early Development Phases of Future ATM Concepts

Cody H. Fleming & Nancy G. Leveson

23 June 2015
11th USA/EUROPE ATM R&D Seminar
Motivation

1. Ability to impact cost and performance

2. Cost of design changes

80% of Safety Decisions [Frola and Miller, 1984]
General Challenges

- limited design information
- no specification
- informal documentation
- concept of operations ≡ “ConOps”

Concept → Requirements → Design → Build → Operate

- Preliminary Hazard Analysis
- System & Sub-system Hazard Analysis
- Accident Analysis

© Fleming ‘15
Goals

1. use rigorous, systematic tools for identifying hazardous scenarios and undocumented assumptions

2. supplement existing (early) SE activities such as requirements definition, architectural and design studies

Especially when tradespace includes: human operation, automation or decision support tools, and the coordination of decision making agents
Table of Contents

1. Theory
2. STECA
3. Application-TBO
4. Early Eng
Current State of the Art

- Concept
- Requirements
- Design
- Build
- Operate

- Preliminary Hazard Analysis
- System & Sub-system Hazard Analysis
- Accident Analysis
# Preliminary Hazard Analysis

<table>
<thead>
<tr>
<th>ITEM</th>
<th>HAZARD COND</th>
<th>CAUSE</th>
<th>EFFECTS</th>
<th>RAC</th>
<th>ASSESSMENTS</th>
<th>RECOMMENDATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned number</td>
<td>List the nature of the condition</td>
<td>Describe what is causing the stated condition to exist</td>
<td>If allowed to go uncorrected, what will be the effect or effects of the hazardous condition</td>
<td>Hazard Level assignment</td>
<td>Probability, possibility of occurrence: -Likelihood -Exposure -Magnitude</td>
<td>Recommended actions to eliminate or control the hazard</td>
</tr>
</tbody>
</table>

[Vincoli, 2005]
## Limitations of PHA

PHA tends to identify the following hazard causes:

<table>
<thead>
<tr>
<th>Causes</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment Failure</td>
<td>Self explanatory</td>
</tr>
<tr>
<td>Design error, coding error, insufficient software testing, software operating system problem</td>
<td>Medium</td>
</tr>
<tr>
<td>Human error</td>
<td></td>
</tr>
</tbody>
</table>

This is true:

**ALL accidents are caused by hardware failure, software flaws, or human error**

But is the information coming from PHA useful for systems engineering?

[JPDO, 2012]
Safety $\Rightarrow$ Control Problem

Systems-Theoretic Accident Model and Process (STAMP)

- Accidents are more than a chain of events, they involve complex dynamic processes
- Treat accidents as a control problem, not a failure problem
- Prevent accidents by enforcing constraints on component behavior and interactions
Systems Theory
Emergence

Organized complexity as a hierarchy of levels, “each more complex than the one below, a level being characterized by emergent properties which do not exist at the lower level” [Checkland, 1999]
Hierarchy

Level 1 Subsystem

Input

Intervention

Feedback

Input

Output

Level \( n \) Subsystem

Intervention

Feedback

Input

Output

Level \( n - 1 \) Subsystem

Input

Feedback

Output

Level 1 Subsystem

Input

Output

[Mesarovic, 1970]
Four conditions are required for process control:

1. *Goal* condition: the controller must have a goal or goals

2. *Action* condition: the controller must be able to affect the state of the system, typically by means of an actuator or actuators

3. *Model* condition: the controller must contain a model of the system

4. *Observability* condition: the controller must be able to ascertain the state of the system, typically by feedback from a sensor

[Ashby, 1957]
Table of Contents

1. Theory

2. STECA

3. Application-TBO

4. Early Eng
Approach

Systems-theoretic Early Concept Analysis—STECA
Approach

Concept

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
Control Elements

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
Control Elements

Controller
- Inadequate Control Algorithm (Flaws in creation, Process changes, Incorrect modification or adaptation)
- Process Model inconsistent, incomplete, or incorrect
- Inadequate or missing feedback
- Feedback delays

Actuator
- Inadequate Operation
- Delayed operation

Controller 2
- Conflicting control actions
- Process input missing or wrong

Sensor
- Inadequate Operation
- Incorrect or no information provided
- Measurement inaccuracies
- Feedback delays

Controlled Process
- Component failures
- Changes over time
- Unidentified or out-of-range disturbance
- Process output contributes to hazard

Controller input or external information wrong or missing

[Leveson, 2012]
Control Elements

1. Controller
   - 5. Process Model
   - 6. Control Algorithm
   - 7. Control Action

2. Actuator

3. Controlled Process
   - 12. Alternate control actions
   - 13. External process input

4. Sensor

9. Control input (setpoint) or other commands
10. Controller output
11. External input
14. Process Disturbance
15. Process Output
8. Feedback to higher level controller

Theory
STECA
Application-TBO
©Fleming '15
Roles in Control Loop

What kinds of things can an “entity” do within a control structure, and more particularly within a control loop?
Roles in Control Loop

What kinds of things can an “entity” do within a control structure, and more particularly within a control loop?

**Controller**

- Enforces safety constraints
- Creates, generates, or modifies control actions based on algorithm or procedure and perceived model of system
- Processes inputs from sensors to form and update process model
- Processes inputs from external sources to form and update process model
- Transmits instructions or status to other controllers
Roles in Control Loop

What kinds of things can an “entity” do within a control structure, and more particularly within a control loop?

**Actuator**

- Translates controller-generated action into process-specific instruction, force, heat, etc
Roles in Control Loop

What kinds of things can an “entity” do within a control structure, and more particularly within a control loop?

**Controlled Process**

- Interacts with environment via forces, heat transfer, chemical reactions, etc.
- Translates higher level control actions into control actions directed at lower level processes
Roles in Control Loop

What kinds of things can an “entity” do within a control structure, and more particularly within a control loop?

Sensor

- Transmits continuous dynamic state measurements to controller (i.e. measures the behavior of controlled process via continuous or semi-continuous [digital] data)
- Transmits binary or discretized state data to controller (i.e. measures behavior of process relative to thresholds; has algorithm built-in but no cntl authority)
- Synthesizes and integrates measurement data
1. Controller

2. Actuator

3. Controlled Process

4. Sensor

5. Process Model

6. Control Algorithm

7. Control Action

8. Feedback to higher level controller

9. Control input (setpoint) or other commands

10. Controller output

11. External input

12. Alternate control actions

13. External process input

14. Process Disturbance

15. Process Output

© Fleming ‘15
Analysis

ConOps

Model Generation

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

Model-based Analysis
Analysis

“Completeness”

“Analyzing Safety-related Responsibilities”

“Coordination & Consistency”
Early Systems Engineering

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
Early Systems Engineering

Constraints on control loop behavior

Model-Based Analysis

Change the control structure
Table of Contents

1. Theory
2. STECA
3. Application-TBO
4. Early Eng
Application—TBO

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
As the aircraft approaches level-off and cruise, the shape of the protected airspace morphs into more of an elliptical 3-D shape, where the aircraft is positioned in the narrow end of the elliptical shape, with the wake vortex "tail" as its aft bound and vertical, lateral, and longitudinal uncertainty defining the flexible airspace. No two elliptical shapes can overlap if separation is to be assured. In this case, Aircraft A and Aircraft B have crossing trajectories. Aircraft A's protected space is smaller because it has less uncertainty than Aircraft B. The trailing area of protection may reflect wake turbulence requirements. The lateral protection is the uncertainty in navigation performance, while the leading distance along the flight path represents the time uncertainty. In level flight, the vertical altitude dimension is quite small.

[JPDO, 2011]
As the aircraft approaches level-off and cruise, the shape of the protected airspace morphs into more of an elliptical 3-D shape, where the aircraft is positioned in the narrow end of the elliptical shape, with the wake vortex "tail" as its aft bound and vertically, lateral, and longitudinal uncertainty defining the flexible airspace. No two elliptical shapes can overlap if separation is to be assured. In this case, Aircraft A and Aircraft B have crossing trajectories. Aircraft A's protected space is smaller because it has less uncertainty than Aircraft B. The trailing area of protection may reflect wake turbulence requirements. The lateral protection is the uncertainty in navigation performance, while the leading distance along the flight path represents the time uncertainty. In level flight, the vertical altitude dimension is quite small.

On arrival, the shape of uncertainty projects downward, based on the descent profile. RNP controls lateral displacement, and time is projected forward to points in space for metering, merging, or initiating the approach as needed for separation, sequencing, merging, and spacing. As the aircraft moves closer to the airport and landing, the uncertainty of vertical profile decreases and the aircraft is now flying in more of a tube-shaped bounded uncertainty, defined laterally by RNP and vertically by the altitude restrictions for the arrival.

[JPDO, 2011]
System-Level Hazards

[H-1] Aircraft violate minimum separation (LOS or loss of separation, NMAC or Near midair collision)

[H-2] Aircraft enters uncontrolled state

[H-3] Aircraft performs controlled maneuver into ground (CFIT, controlled flight into terrain)

[SC-1] Aircraft must remain at least TBD nautical miles apart en route* ↑[H-1]

[SC-2] Aircraft position, velocity must remain within airframe manufacturer defined flight envelope ↑[H-2]

[SC-3] Aircraft must maintain positive clearance with all terrain (This constraint does not include runways and taxiways) ↑[H-3]
Identify Control Concepts

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
Identify Control Concepts

TBO conformance is monitored both in the aircraft and on the ground against the agreed-upon 4DT. In the air, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other “time to go” aids. [JPDO, 2011]
Identify Control Concepts

TBO conformance is monitored both in the aircraft and on the ground against the agreed-upon 4DT. In the air, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other “time to go” aids. [JPDO, 2011]

<table>
<thead>
<tr>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
</tr>
<tr>
<td>Behavior Type</td>
</tr>
<tr>
<td>Context</td>
</tr>
</tbody>
</table>
**Identify Control Concepts**

\textit{TBO conformance is monitored both in the aircraft and on the ground against the agreed-upon 4DT. In the air, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other “time to go” aids. [JPDO, 2011]}

<table>
<thead>
<tr>
<th>Subject</th>
<th>Conformance monitoring, Air automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Sensor</td>
</tr>
<tr>
<td>Behavior Type</td>
<td>Transmits binary or discretized state data to controller (i.e. measures behavior of process relative to thresholds; has algorithm built-in but no cntl authority)</td>
</tr>
<tr>
<td></td>
<td>Synthesizes and integrates measurement data</td>
</tr>
<tr>
<td>Context</td>
<td>This is a decision support tool that contains algorithms to synthesize information and provide alerting based on some criteria.</td>
</tr>
</tbody>
</table>
Identify Control Concepts

TBO conformance is monitored both in the aircraft and on the ground against the agreed-upon 4DT. In the air, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other “time to go” aids. [JPDO, 2011]
Identify Control Concepts

TBO conformance is monitored both in the **aircraft** and on the **ground** against the agreed-upon 4DT. In the **air**, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other “time to go” aids. [JPDO, 2011]

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Controller</td>
<td>Piloting function</td>
</tr>
<tr>
<td>2. Actuator</td>
<td></td>
</tr>
<tr>
<td>3 Cntl’d Process</td>
<td>Aircraft</td>
</tr>
<tr>
<td>4. Sensor</td>
<td>Altimeter, FMS, Aircraft conformance monitor</td>
</tr>
<tr>
<td>5. Process Model</td>
<td>Intended latitude, longitude, altitude, time; Actual latitude, longitude, altitude, time</td>
</tr>
<tr>
<td>6. Cntl Algorithm</td>
<td></td>
</tr>
<tr>
<td>7. Control Actions</td>
<td></td>
</tr>
<tr>
<td>8. Controller Status</td>
<td></td>
</tr>
<tr>
<td>9. Control Input</td>
<td></td>
</tr>
<tr>
<td>10. Controller Output</td>
<td></td>
</tr>
<tr>
<td>11. External Input</td>
<td></td>
</tr>
<tr>
<td>12. Alt Controller</td>
<td></td>
</tr>
<tr>
<td>13. Process Input</td>
<td></td>
</tr>
<tr>
<td>14. Proc Disturbance</td>
<td></td>
</tr>
<tr>
<td>15. Process Output</td>
<td></td>
</tr>
</tbody>
</table>
Conf Monitoring Control Loops

“Air”

AIR (Flight Crew)

CA_A PM_A

Alert parameter (A)

FMS

Conformance Monitor [Air]

CDTI

{x,y,h,t}

Aircraft

ADS-B

GNSS

{x,y,h,t}all

©Fleming ‘15
Conf Monitoring Control Loops

“Air”

- AIR (Flight Crew)
  - CA_A
  - PM_A
- FMS
- Aircraft
  - ADS-B
- GNSS
- Alert parameter (A)

“Ground”¹

- GROUND (ANSP / ATC)
  - CA_G
  - PM_G
- TBO Strategic Evaluation
- TBO Automation
- Conformance Monitor [Gnd]
- Data Link
- Altitude Report
- {4DT}_i
- {x,y,h,t}_i
- {h}_i

- AIRSPACE
- GNSS

¹Examples of model development for ground component included in backup slides
Hierarchical Control Structure

How to Establish Hierarchy?

- Higher level of systems:
  - Decision Making Priority
  - Decision Complexity, ↑
  - Time Scale between decisions, ↑
  - Dynamics of controlled system, ↓
Hierarchical Control Structure

Function

Route Planning*

Piloting*

Aircraft

Environment

Safety-Related Responsibilities

- Provide conflict-free clearances & trajectories
- Merge, sequence, space the flow of aircraft
- Navigate the aircraft
- Provide aircraft state information to rte planner
- Avoid conflicts with other aircraft, terrain, weather
- Ensure that trajectory is within aircraft flight envelope
- Provide lift
- Provide propulsion (thrust)
- Orient and maintain control surfaces
Hierarchical Control Structure

Route Planning

Piloting

Aircraft

Environment

Route, Trajectory Management Function

GROUND (ANSP / ATC)

Alert parameter (G)

AIR (Flight Crew)

Alert parameter (A)

FMS; Manual

Aircraft

ADS-B

GNSS

Data Link

Conformance Monitor [Gnd]

Conformance Monitor [Air]

Altitude Report

{4DT} (Intent)

{h}

{x,y,h,t}

{x,y,h,t}
Hierarchical Control Structure

Route Planning*

Piloting*

Aircraft

Environment

**Route, Trajectory Management Function**

- GROUND (ANSP / ATC)
  - Alert parameter (G)
  - Data Link
  - Conformance Monitor [Gnd]
  - Altitude Report

**Piloting Function**

- 4DT; Clearance
- AIR (Flight Crew)
  - Alert parameter (A)
  - Conformance Monitor [Air]
- FMS; Manual
- CDTI

**Aircraft**

- ADS-B
  - Alert parameter [x,y,h,t]
- GNSS

**Alert parameter**

- (A) {x,y,h,t}
- (G) 4DT

**Theory**

- STECA
- Application-TBO

©Fleming ‘15
ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis
1. Are the control loops complete?
2. Are the system-level safety responsibilities accounted for?
3. Do control agent responsibilities conflict with safety responsibilities?
4. Do multiple control agents have the same safety responsibility(ies)?
5. Do multiple control agents have or require process model(s) of the same process(es)?
6. Is a control agent responsible for multiple processes? If so, how are the process dynamics (de)coupled?
4. Do multiple control agents have the same safety responsibility(ies)?

5. Do multiple control agents have or require process model(s) of the same process(es)?

6. Is a control agent responsible for multiple processes? If so, how are the process dynamics (de)coupled?

²Example of “Analyzing Safety-related Responsibilities” included in Backup Slides on page 43
Coordination & Consistency

- Coordination Principle (4)
- Consistency Principle (5)

\[
(\forall c \in C_i)(\forall d \in C_j) \exists (P(c,d) \lor P(d,c))[A(c,V_p) \land A(d,V_p)], \quad (4)
\]

\[
(\forall v \in V, \forall c \in C_i, \forall d \in C_j | A(c,v) \land A(d,v))
\]
\[
[\rho_i(a,v) \equiv \rho_j(a,v) \land G_i \equiv G_j] \quad (5)
\]
Aircraft
ADS-B
Conformance Monitor [Gnd]
Conformance Monitor [Air]
Alert parameter (A)
{x,y,h,t}
GNSS
Alert parameter (G)
{4DT}
(Intent)

Route, Trajectory Management Function

4DT; Clearance

Piloting Function

AIR (Flight Crew)

FMS; Manual

Piloting Function

Aircraft
ADS-B

Conformance Monitor [Air]
CDTI

Altitude Report

Ground (ANSP / ATC)

4DT; Clearance

Theory
STECA
Application-TBO
Early Eng
©Fleming ‘15
\[ B_{cm} := \mathcal{L}_{cm} \times D_{cm} \rightarrow I_{cm}, \] (6)

- \( \mathcal{L}_{cm} \) is a model of the airspace state and
- \( D_{cm} \) is the decision criteria regarding conformance.
Coordination & Consistency

\[ \mathcal{L}_{cm} := \{z_{int}, z_{act}, \rho, T, P_r, W, E_{cm}, F_D\} \]  \tag{7}

\[ z_{int} := \{G, C, t\}_{int} \]

\[ z_{act} := \{G, C, t\}_{act} \]

\[ \rho := \text{Traffic density} \]

\[ \tau := \text{Operation type} \]

\[ P_r := \{\text{RNP, RTP}\} \]

\[ W := \text{Wake turbulence model} \]

\[ E_{cm} := \text{Elliptical conformance model} \]

\[ F_D := \{F, z_{int}\} \]

\[ D_{cm} = \{z_{act} \mid z_{act} \notin \bar{Z}(z_{int}, E_{cm}, a_{cm}) \} \]  \tag{8}
Coordination & Consistency

Route, Trajectory Management Function

GROUND (ANSP/ATC)

4DT; Clearance

Altitude Report

Data Link

Conformance Monitor [Gnd]

Alert parameter (G)

Gnd

Conformance Monitor [Air]

Alert parameter (A)

Air

{4DT}
(Intent)

{h}

FMS; Manual

Piloting Function

AIR (Flight Crew)

Alert parameter (A)

CA_{G}, PM_{G}

CA_{A}, PM_{A}

Conformance Monitor [Air]

CDTI

Aircraft

ADS-B

Altitude Report

{x,y,h,t}

{x,y,h,t}

GNSS

{x,y,h,t}

{h}

FMS; Manual

PM; Manual

CA_{G}, PM_{G}

CA_{A}, PM_{A}

{x,y,h,t}

{x,y,h,t}

GNSS

{x,y,h,t}

{x,y,h,t}
Coordination & Consistency

Route, Trajectory Management Function

GROUND (ANSP / ATC)

Alert parameter (G)

4DT; Clearance

Data Link

Conformance Monitor [Gnd]

Altitude Report

AIR (Flight Crew)

Alert parameter (A)

Conformance Monitor [Air]

CDTI

Data Link

FMS; Manual

Altitude Report

Aircraft

ADS-B

Alert parameter (A)

{x,y,h,t}

{h}

CDTI

Data Link

FMS; Manual

Altitude Report

Aircraft

ADS-B

Alert parameter (A)

{x,y,h,t}

{h}

CDTI

Data Link

FMS; Manual

Altitude Report

Aircraft

ADS-B

Alert parameter (A)

{x,y,h,t}

{h}

Independent “alert parameter”

Theory

STECA

Application-TBO

Early Eng

©Fleming ‘15 32
Coordination & Consistency

Independent “alert parameter”

Route, Trajectory Management Function

4DT; Clearance

Piloting Function

FMS; Manual

Aircraft

ADS-B

GNSS

Alert parameter (G)

Alert parameter (A)

4DT; Clearance

Data Link

Conformance Monitor [Gnd]

Altitude Report

Independent conformance monitors

GROUND (ANSP / ATC)

CA_G, PM_G

AIR (Flight Crew)

CA_A, PM_A

Conformance Monitor [Air]

CDTI

FMS; Manual

{4DT} (Intent)

{x,y,h,t}

{x,y,h,t}

{x,y,h,t}

{h}

Theory

STECA

Application-TBO

Early Eng

©Fleming ‘15
Table of Contents

1. Theory

2. STECA

3. Application-TBO

4. Early Eng
What does an engineer need to develop the system??

Application of Results

Concept | Requirements | Design | Build | Operate
--- | --- | --- | --- | ---
Preliminary Hazard Analysis | System & Sub-system Hazard Analysis | Accident Analysis

Theory | STECA | Application-TBO | Early Eng
----- | ----- | ----- | ----

©Fleming ‘15
Architecture Studies

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

3 Examples of reqs identification included in backup slides on page 47
TBO relies on data link for the majority of the air-to-air, air-to-ground and ground-ground communications. There may be multiple data links involved in TBO, ranging from delivery of advisory information to the actual loading of a new 4DT that affects the flight path of the aircraft. This variation in message content drives different data link performance requirements. Much of the messaging is advisory in nature, but the actual clearance for the 4DT and confirmation of use of this information have higher performance requirements. An aircraft may be connected to network-centric operations over multiple data links, but there will be a specified, performance-driven path for the critical communication of 4DT information. Figure 4 is a depiction of notional communication flows.

Figure 4. TBO Information Flows

The numbers in Figure 4 identify the possible communications paths. Path 1 is the network-centric operations connectivity, a ground-ground communications used by the airline, military, or larger GA operation with dispatch services that connects the operator to the ANSP. For those operators lacking a dispatch service, this communications path may be supported by a third-party vendor and used by pilots to plan a flight and provide their desired 4DT to the ANSP. Path 1 is the principal path for flight-following activities by the airlines. Path 2 represents a user-specified performance for exchange of information between the flight crew and operations. For strategic changes to the 4DT under TBO, this communications path could be used to coordinate between the flight crew and operations, and then the Airline Operations Center/Flight Operations Center (AOC/FOC) could negotiate with the ANSP. Path [JPDO, 2011]
TBO Negotiation
Additional Requirement: \( \kappa^A_F \) and \( \kappa^O_F \) shall not occur simultaneously.
Additional Requirement: This becomes the active control structure within TBD minutes of gate departure.
Conclusion

Systems Engineering Phases

Concept
Requirements
Design
Build
Operate

“STECA”
“PHA”

Preliminary Hazard Analysis
System & Sub-system Hazard Analysis
Accident Analysis

Safety Activities

Theory
STECA
Application-TBO
Early Eng
©Fleming ‘15
References


Backup Slides
5. TBO Analysis

6. Early Eng

7. STAMP
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information is then compared to a performance requirement for the airspace and the operation. ...precision needed...will vary based on the density of traffic and the nature of the operation. [JPDO, 2011]
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information is then compared to a performance requirement for the airspace and the operation. ...precision needed...will vary based on the density of traffic and the nature of the operation. [JPDO, 2011]
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information is then compared to a performance requirement for the airspace and the operation. ...precision needed...will vary based on the density of traffic and the nature of the operation. [JPDO, 2011]

<table>
<thead>
<tr>
<th>Subject</th>
<th>Conformance monitoring, Ground automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Sensor</td>
</tr>
<tr>
<td>Behavior Type</td>
<td>Transmits binary or discretized state data to controller (i.e. measures behavior of process relative to thresholds; has algorithm built-in but no cntl authority)</td>
</tr>
<tr>
<td>Context</td>
<td>This is a decision support tool that contains algorithms to synthesize information and provide alerting based on some criteria.</td>
</tr>
</tbody>
</table>
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information is then compared to a performance requirement for the airspace and the operation. ...precision needed...will vary based on the density of traffic and the nature of the operation. [JPDO, 2011]
1. Are the control loops complete?
2. Are the system-level safety responsibilities accounted for?
3. Do control agent responsibilities conflict with safety responsibilities?
4. Do multiple control agents have the same safety responsibility(ies)?
5. Do multiple control agents have or require process model(s) of the same process(es)?
6. Is a control agent responsible for multiple processes? If so, how are the process dynamics (de)coupled?
Safety-Related Responsibilities

2. Are the system-level safety responsibilities accounted for?

3. Do control agent responsibilities conflict with safety responsibilities?
Safety-Related Responsibilities

• Gaps in Responsibility (2)
• Conflicts in Responsibility (3)

\[
\begin{align*}
(\forall \sigma_i \in \Sigma) \ (\exists c \in \mathcal{C}) \ [P(c, \sigma_i)], \\
(\forall H_i \in \mathcal{H}) \ (\neg \exists c \in \mathcal{C}) \ [P(c, H_i) \land P(c, G)]
\end{align*}
\]
Safety-Related Responsibilities

Potential conflict between goal condition, safety responsibilities???

[JPDO, 2011]

“The pilot must also work to close the trajectory. Pilots will need to update waypoints leading to a closed trajectory in the FMS, and work to follow the timing constraints by flying speed controls.”
Safety-Related Responsibilities
Safety-Related Responsibilities
Table of Contents

5. TBO Analysis

6. Early Eng

7. STAMP
Approach

ConOps

Model Generation

Model-based Analysis

- Unspecified assumptions
- Missing, inconsistent, incomplete information
- Vulnerabilities, risks, tradeoffs
- System, software, human requirements
- Architectural and design analysis
Scenario 2:

ANSP issues command that results in aircraft closing (or maintaining) a 4DT, but that 4DT has a conflict.

Causal Factors:

- This scenario arises because the ANSP has been assigned the responsibility to assure that aircraft conform to 4D trajectories as well as to prevent loss of separation.
  - A conflict in these responsibilities occurs when any 4D trajectory has a loss of separation (LOS could be with another aircraft that is conforming or is non-conforming). [Goal Condition]
**Scenario 2:**

ANSP issues command that results in aircraft closing (or maintaining) a 4DT, but that 4DT has a conflict.

**Causal Factors:**

- Additional hazards occur when the 4DT encounters inclement weather, exceeds aircraft flight envelope, or aircraft has emergency

- ANSP and crew have inconsistent perception of conformance due to independent monitor, different alert parameter setting

- ...

References

TBO Analysis  Early Eng

STAMP  ©Fleming ‘15
**Scenario 2:**
ANSP issues command that results in aircraft closing (or maintaining) a 4DT, but that 4DT has a conflict.

**Requirements:**

**S2.1** Loss of separation takes precedence over conformance in all TBO procedures, algorithms, and human interfaces [Goal Condition]

**S2.3** Loss of separation alert should be displayed more prominently when conformance alert and loss of separation alert occur simultaneously. [Observability Condition] This requirement could be implemented in the form of aural, visual, or other format(s).

**S2.4** Flight crew must inform air traffic controller of intent to deviate from 4DT and provide rationale [Model Condition] ...

**Human factors-related requirements**
Scenario 2:

ANSP issues command that results in aircraft closing (or maintaining) a 4DT, but that 4DT has a conflict.

Requirements:

S2.8 4D Trajectories must remain conflict-free, to the extent possible ...

S2.10 Conformance volume must be updated within TBD seconds of change in separation minima

S2.11 Conformance monitoring software must be provided with separation minima information

Software-related requirements
**Scenario 2:**

ANSP issues command that results in aircraft closing (or maintaining) a 4DT, but that 4DT has a conflict.

**Requirements:**

**S2.14** ANSP must be provided information to monitor the aircraft progress relative to its own “Close Conformance” change of clearance...

**S3.2** ANSP must be able to generate aircraft velocity changes that close the trajectory within TBD minutes (or TBD nmi).

*Rationale: TBO ConOps is unclear about how ANSP will help the aircraft work to close trajectory. Refined requirements will deal with providing the ANSP feedback about the extent to which the aircraft does not conform, the direction and time, which can be used to calculate necessary changes.*

**Component Interaction Constraints**
Table of Contents

5. TBO Analysis

6. Early Eng

7. STAMP
Controllers use a process model to determine control actions.

Accidents often occur when the process model is incorrect.

Four types of unsafe control actions:

1. **Not providing** the control action causes the hazard.
2. **Providing** the control action causes the hazard.
3. The **timing** or **sequencing** of control actions leads to the hazard.
4. The **duration** of a continuous control action, i.e., too short or too long, leads to the hazard.
Controllers use a **process model** to determine control actions.

Accidents often occur when the process model is incorrect.

Four types of unsafe control actions:

1. **Not providing** the control action causes the hazard.
2. **Providing** the control action causes the hazard.
3. The **timing** or **sequencing** of control actions leads to the hazard.
4. The **duration** of a continuous control action, i.e., too short or too long, leads to the hazard.

Better model of both software and human behavior
Explains software errors, human errors, interaction accidents,...
Controlled Process

Controller

Process Model

Control

Actions

Feedback

References

TBO Analysis

Early Eng

STAMP

©Fleming ‘15

51
Controller

Process Model

Control Actions

Feedback

Controlled Process

Operating Process

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

Physical Process

Operating Assumptions
Operating Procedures

Revised operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests

References
TBO Analysis
Early Eng

© Fleming '15
## Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing/Order Causes Hazard</th>
<th>Stopped Too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Execute ITP</strong></td>
<td></td>
<td>ITP executed when not approved</td>
<td>ITP executed too soon before approval</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ITP executed when ITP criteria are not satisfied</td>
<td>ITP executed too late</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ITP executed with incorrect climb rate, final altitude, etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Abnormal Termination</strong></td>
<td><strong>of ITP</strong></td>
<td>FC continues with maneuver in dangerous situation</td>
<td>FC aborts unnecessarily</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FC does not follow regional procedures while aborting</td>
<td></td>
</tr>
</tbody>
</table>

Four inadequate control actions of the ITP flight crew are identified as potentially unsafe in B.3. Again, these are self-explanatory: when the flight crew incorrectly executes the ITP or does so out of sequence (which we define as prior to receiving approval or not immediately after receiving approval) or does not initiated an abnormal termination or does so incorrectly, this action may very clearly put the ITP aircraft in proximity of a nearby aircraft. The other inadequate control actions are not highlighted as unsafe for one of three reasons. They are either not unsafe, as is the case of the flight crew not executing IT, they are logically identical to other inadequate control actions (e.g., ITP executed beyond final altitude), or they are illogical (ITP cannot be abnormally terminated if it has not begun or has already completed).

The 14 identified unsafe control actions (hazards) can be translated into high-level safety constraints on the air traffic controller and the flight crew:

**[SC-ATC.1]** Approval of an ITP request must be given only when the ITP criteria are met. (STPA-ATC.1, [1.14])

References

TBO Analysis

Early Eng

STAMP

©Fleming ‘15 52
Control Flaws

Controller

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

- Process Model inconsistent, incomplete, or incorrect

- Inadequate or missing feedback
  Feedback delays

Actuator

- Inadequate Operation

- Delayed operation

Sensor

- Inadequate Operation

- Incorrect or no information provided
  Measurement inaccuracies
  Feedback delays

Controlled Process

- Component failures
  Changes over time

- Conflicting control actions

- Process input missing or wrong

- Unidentified or out-of-range disturbance

- Process output contributes to hazard

- [Leveson, 2012]

References

©Fleming ‘15