Systems-Theoretic Early Concept Analysis (and Development)

Cody H. Fleming
Presented By: David Horney and Andrea Scarinci
21 March 2016
5th STAMP Workshop
Systems Engineering Research Lab
Motivation

1. Ability to impact cost and performance

2. Cost of design changes

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

Concept | Requirements | Design | Build | Operate

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

© Fleming '15
General Challenges

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

©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. STAMP

3. STECA

4. Case Study

© Fleming ‘15
Current State of the Art

Concept

Requirements

Design

Build

Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

Accident Analysis

Theory

STAMP

STECA

Case Study

© Fleming '15
## 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>Causes</th>
<th>Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment Failure</td>
<td>Design error, coding error, insufficient software testing,</td>
<td>Human error</td>
</tr>
<tr>
<td></td>
<td>software operating system problem</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?
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

Input → Level $n$ Subsystem → Output

Input → Level $n - 1$ Subsystem → Output

Input → Level 1 Subsystem → Output

Intervention → Feedback

Feedback

[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. STAMP

3. STECA

4. Case Study
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.
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, ...
Controller

Process Model

Control Actions

Feedback

Controlled Process

Operating Assumptions
Operating Procedures

Revised operating procedures
Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

Physical Process
Controller

Process Model

Control Actions

Feedback

Controller 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

Theory
STAMP
STECA
Case Study
©Fleming '15
Control Flaws

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

Actuator
- Inadequate Operation
- Delayed operation

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

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

[Leveson, 2012]
Table of Contents

1. Theory

2. STAMP

3. STECA

4. Case Study
Approach

Systems-theoretic Early Concept Analysis—STECA
Approach

Concept

Unspecified assumptions

Model Generation

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Model-based Analysis

Architectural and design analysis
Control Elements

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

- Model Generation
- Model-based Analysis
Control Elements

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

2. Actuator
3. Controlled Process

4. Sensor

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

© 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
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
Constraints on control loop behavior

Model-Based Analysis

Change the control structure

Figure 11: Control Loop with generic entities

The information in Figure 11 and the above lists (Controller, Actuator, Controlled Process, Sensor) can then be used to systematically parse and query the natural language description or graphical depiction in a concept of operations. The resulting model and subsequent database are easy to interrogate and visualize. These qualities help the analyst to check for internal inconsistencies and/or missing information that may result in unsatisfied control conditions, and also to check for inconsistencies across the system hierarchy.

Table 6 provides a series of prompts that an analyst can use when reading a text or graphic in a ConOps.

In order to obtain a “complete” model of the ConOps, this model development approach should be applied recursively over the entire ConOps document. The key-words, with associated questions and comments (Tables 6 and 7), can be applied to the model itself. The process is conducted according to Figure 9, where the main contributions from this extension are represented by the lower four boxes. The following sub-sections describe the theoretical development as well as provide a brief example for illustrative purposes.

Like a typical STPA hazard analysis, the systems-theoretic early concept analysis (STECA) begins with accidents and hazards, a high level decomposition of control functions, and then a set of high level safety responsibilities. These are basic system and safety engineering activities that should be done for any project (first box, Figure 9). Chapter 4 provides an example of how to identify a hierarchical list of safety responsibilities that is based on systems theory.

3.2 Systematic Control Model Development

Potential benefits of model-based systems engineering include the use of repeatable processes, promoting consistent views of the system, and formal application of modeling to support requirements generation, design, analysis, and verification [Friedenthal et al., 2007]. It is in this vein that this research seeks to develop ConOps in terms of models rather than informal documentation.
<table>
<thead>
<tr>
<th>Theory</th>
<th>STAMP</th>
<th>STECA</th>
<th>Case Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>©Fleming ‘15</td>
</tr>
</tbody>
</table>
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]
Figure 1. Position Uncertainty

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.

Figure 2. En Route Uncertainties Defining Conformance Boundaries

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]*
**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>
<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>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>
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>Role</th>
<th>Behavior</th>
<th>Type</th>
<th>Context</th>
</tr>
</thead>
</table>

© Fleming ‘15
**Ground**

*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><strong>Role</strong></td>
<td>Sensor</td>
</tr>
<tr>
<td><strong>Behavior Type</strong></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><strong>Context</strong></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]
“Ground”

**GROUND (ANSP / ATC)**

CA, PM

Alert parameter (G)

Conformance Monitor [Gnd]

Data Link

Altitude Report

{4DT}i (Intent)

{h}i

**TBO Strategic Evaluation**

**TBO Automation**

**AIRSPACE**

GNSS

{x,y,h,t}i

Theory

STAMP

STECA

©Fleming '15 31
Conf Monitoring Control Loops

“Ground”

GROUND (ANSP / ATC)

CAG, PMG

Alert parameter (G)

Conformance Monitor [Gnd]

{x, y, h, t}_i

{4DT}_i (Intent)

{h}_i

TBO Strategic Evaluation

TBO Automation

Data Link

Altitude Report

AIRSPACE

GNSS

“Air”

AIR (Flight Crew)

CA_A, PM_A

Alert parameter (A)

FMS

Conformance Monitor [Air]

CDTI

Aircraft

ADS-B

{x, y, h, t}_i

{x, y, h, t}_all

GNSS

©Fleming ‘15

Theory

STAMP

STECA

Case Study

©Fleming ‘15 31
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

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

3. Do control agent responsibilities conflict with safety 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
Coordination & Consistency

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?
Coordination & Consistency

Route, Trajectory Management Function

GROUND (ANSP / ATC)

CA_G, PM_G

Alert parameter (G)

4DT; Clearance

Data Link

Conformance Monitor [Gnd]

Altitude Report

AIR (Flight Crew)

CA_A, PM_A

Alert parameter (A)

FMS; Manual

Conformance Monitor [Air]

CDTI

Aircraft

ADS-B

{x,y,h,t}

{x,y,h,t}

{h}

Independent “alert parameter”

Theory
STAMP
STECA
Case Study
©Fleming ‘15
Coordination & Consistency

- Aircraft ADS-B Conformance Monitor
- Alert parameter (A): \( \{x,y,h,t\} \)
- Conformance Monitor [Gnd]
- Data Link
- Route, Trajectory Management Function
- 4DT; Clearance
- AIR (Flight Crew)
- Alert parameter (A): \( \{x,y,h,t\} \)
- Conformance Monitor [Air]
- Piloting Function
- FMS; Manual
- Aircraft ADS-B
- CDTI
- {h}
- Altitude Report
- GROUND (ANSP / ATC)
- CA_G, PM_G
- Alert parameter (G): \( \{4DT\} \) (Intent)
- Independent conformance monitors
- Independent “alert parameter”

Theory

STAMP

STECA

Case Study

©Fleming '15 42


Table of Contents

5. Early SE
Application of Results

- Concept
- Requirements
- Design
- Build
- Operate

- Preliminary Hazard Analysis
- System & Sub-system Hazard Analysis
- Accident Analysis
Application of Results

What does an engineer need to develop the system?

References

©Fleming ‘15
Application of Results

ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilities, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

References

©Fleming '15
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

©Fleming '15
## Deriving Requirements

### Scenario 2:

ANSO 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

References

©Fleming ‘15
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
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
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

References

Early SE

©Fleming '15 48
Additional Requirement: $\mathcal{K}_F^A$ and $\mathcal{K}_F^O$ shall not occur simultaneously.
Additional Requirement: This becomes the active control structure within TBD minutes of gate departure.
Systems Engineering Phases

Concept

Requirements

Design

Build

Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

Accident Analysis

Safety Activities
Systems Engineering Phases

Concept

Requirements

Design

Build

Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

Accident Analysis

“STECA”

“PHA”

Safety Activities

References

©Fleming ‘15