Integrating Systems Safety into Systems Engineering during Concept Development

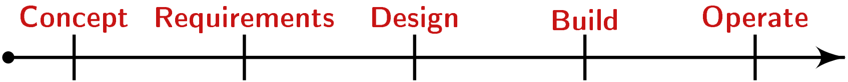
Cody H. Fleming & Nancy G. Leveson

15 July 2015
25th INCOSE International Symposium

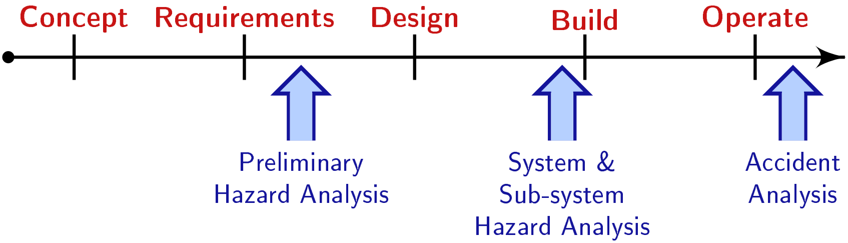
MIT AEROASTRO

UNIVERSITY of VIRGINIA ENGINEERING

Motivation

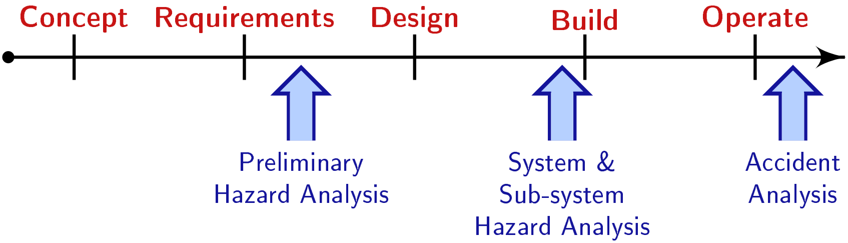


Motivation


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

Motivation

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



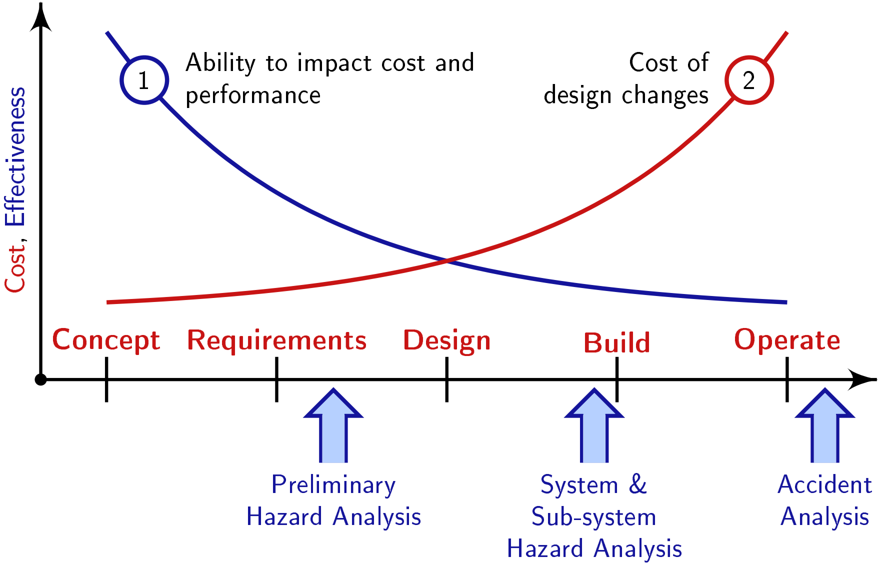
Concept
Requirements
Design
Build
Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

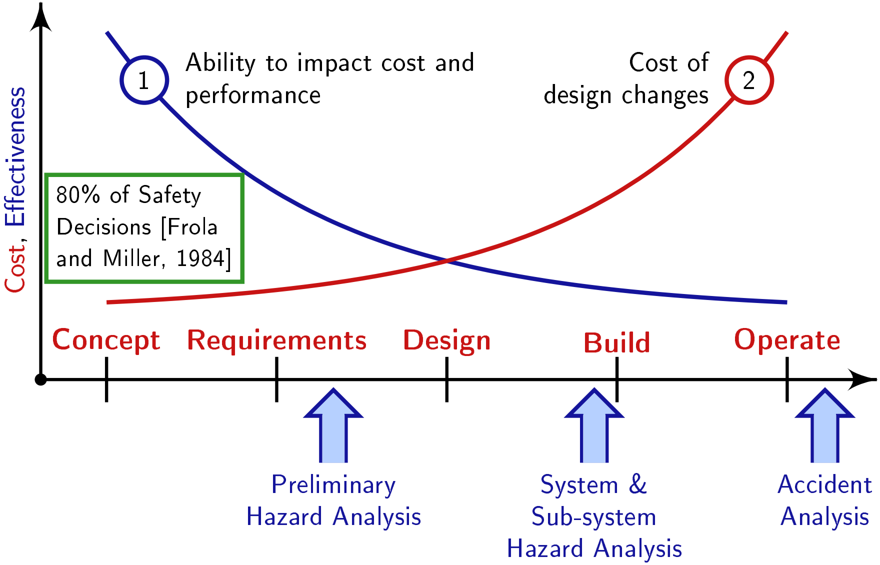
Accident Analysis

Motivation


Cost, Effectiveness
1
Ability to impact cost and performance
Cost of design changes
2
Concept
Requirements
Design
Build
Operate
Preliminary Hazard Analysis
System & Sub-system Hazard Analysis
Accident Analysis

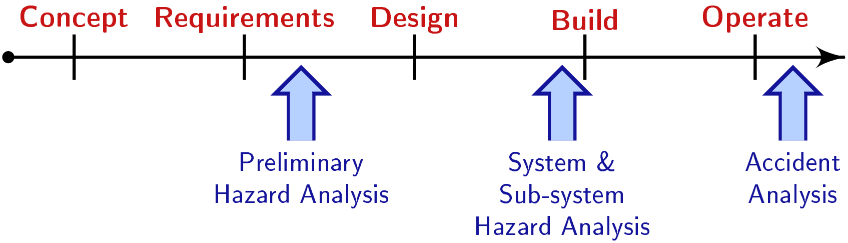
Adapted from [Strafaci, 2008]

Motivation



Cost, Effectiveness
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

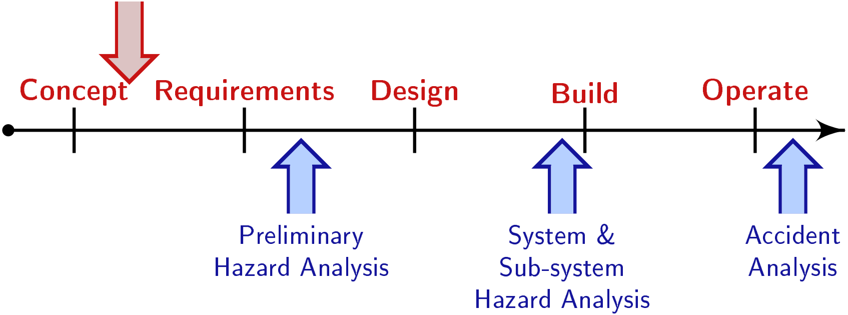
General Challenges



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

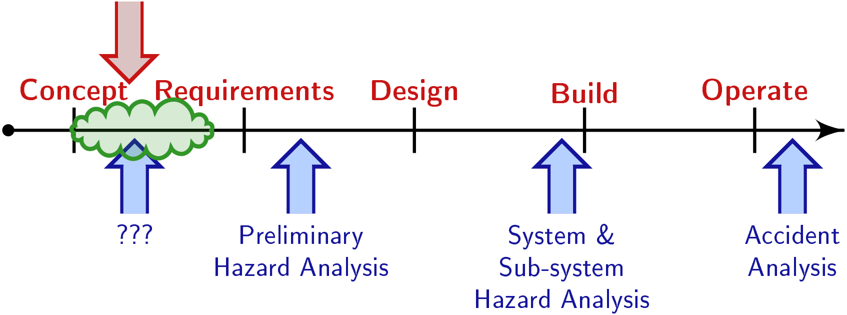
General Challenges

- 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

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

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

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
4. Early Eng

Table of Contents

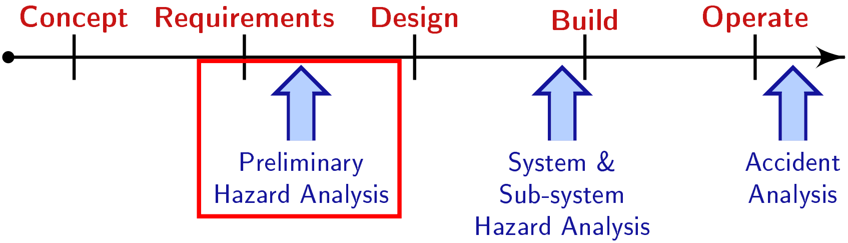
1. Theory

2. STECA

3. Application

4. Early Eng

Current State of the Art


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

Current State of the Art

Preliminary Hazard Analysis

PROGRAM: ____________________ DATE: __________

ENGINEER: ____________________ PAGE: __________

ITEM	HAZARD COND	CAUSE	EFFECTS	RAC	ASSESS-MENTS	RECOMM-ENDATIONS
Assigned number	List the nature of the condition	Describe what is causing the stated condition to exist	If allowed to go uncorrected, what will be the effect or effects of the hazardous condition	Hazard Level assign-ment	Probability, possibility of occurrence: -Likelihood -Exposure -Magnitude	Recommended actions to eliminate or control the hazard

[Vincoli, 2005]

Limitations of PHA

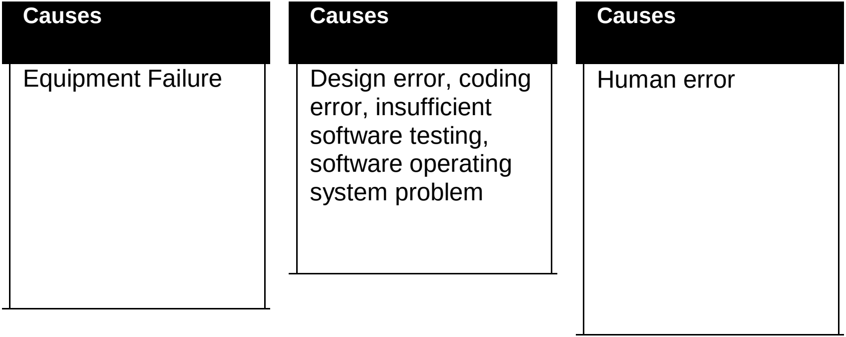
PHA tends to identify the following hazard causes:

Causes	Causes	Causes
Equipment Failure	Design error, coding error, insufficient software testing, software operating system problem	Human error

[JPDO, 2012]

Limitations of PHA

PHA tends to identify the following hazard causes:



Causes	Causes	Causes
Equipment Failure	Design error, coding error, insufficient software testing, software operating system problem	Human error

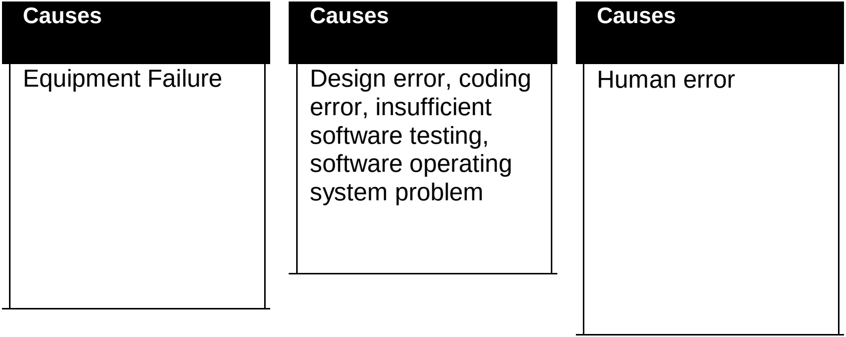
[JPDO, 2012]

This is true:

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

Limitations of PHA

PHA tends to identify the following hazard causes:



Causes	Causes	Causes
Equipment Failure	Design error, coding error, insufficient software testing, software operating system problem	Human error

[JPDO, 2012]

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?

Safety ⇒ Control Problem

Systems-Theoretic Accident Model and Process (STAMP)

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

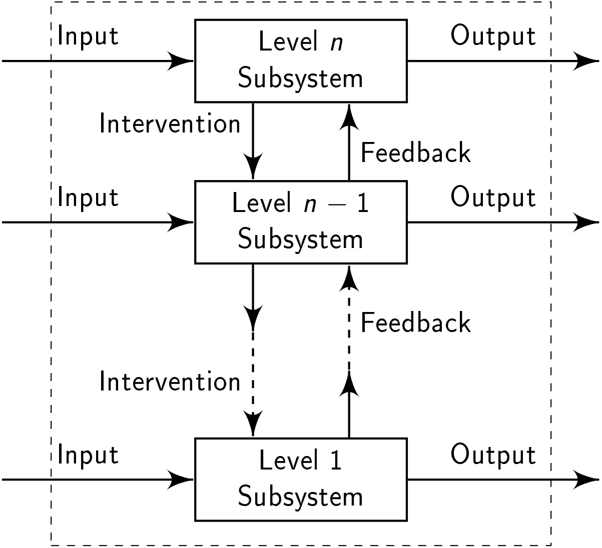
Organized complexity as a hierarchy of levels, “each more complex than the one below, a level being characterized by emergent properties which do not exist at the lower level” [Checkland, 1999]

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]

[Business Korea, 2014]

Hierarchy



[Mesarovic, 1970]

Process Control

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

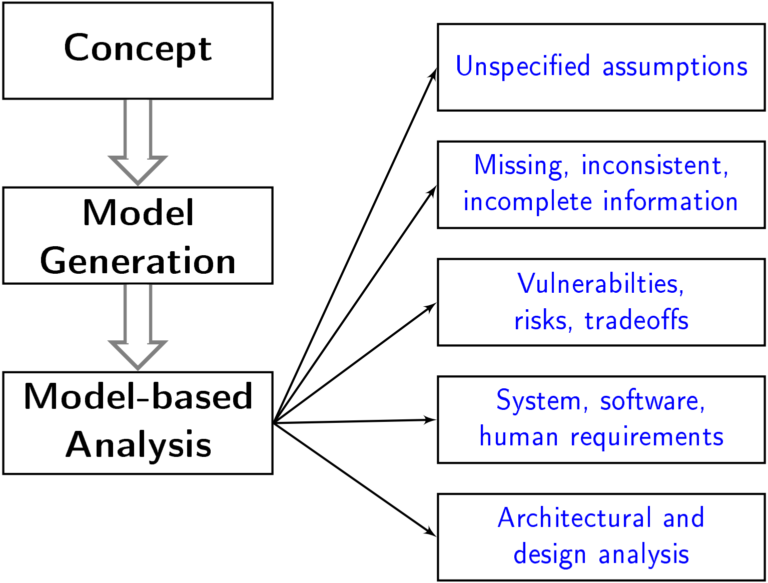
3. Application

4. Early Eng

Approach

Systems-theoretic Early Concept Analysis—STECA

Approach



Concept

Model Generation

Model-based Analysis

Unspecified assumptions

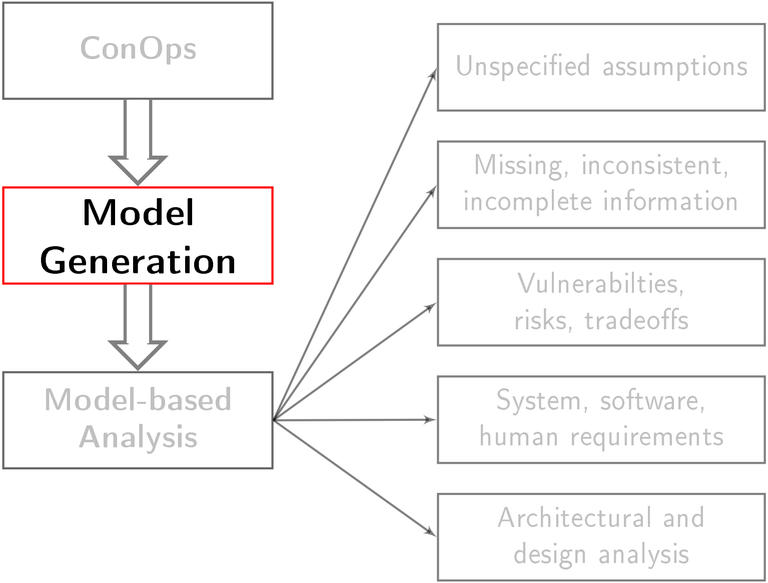
Missing, inconsistent, incomplete information

Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

Control Elements



ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

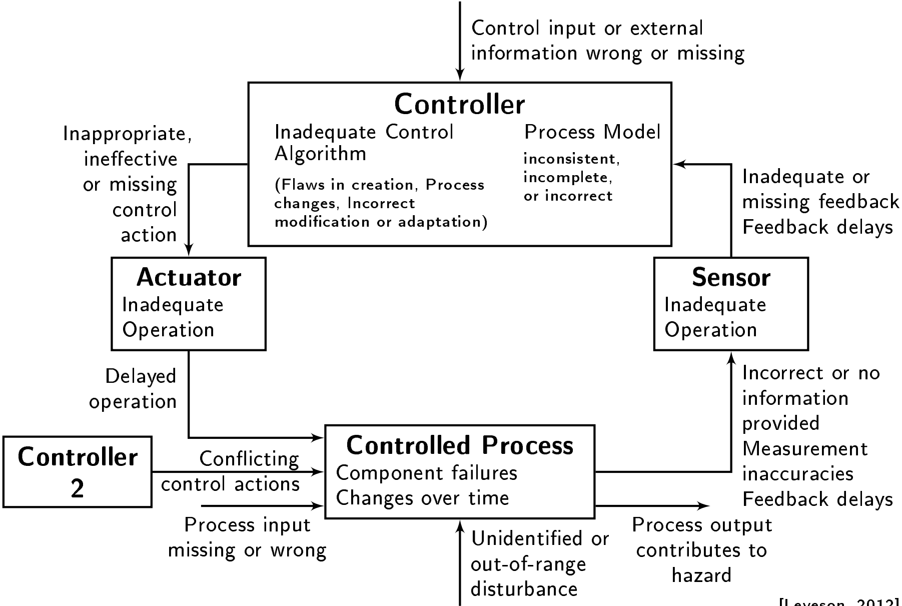
Missing, inconsistent, incomplete information

Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

Control Elements



Control input or external information wrong or missing

Controller

Inadequate Control Algorithm

(Flaws in creation, Process changes, Incorrect modification or adaptation)

Process Model

inconsistent, incomplete, or incorrect

Inappropriate, ineffective or missing control action

Inadequate or missing feedback

Feedback delays

Actuator

Inadequate Operation

Sensor

Inadequate Operation

Delayed operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller 2

Conflicting control actions

Controlled Process

Component failures

Changes over time

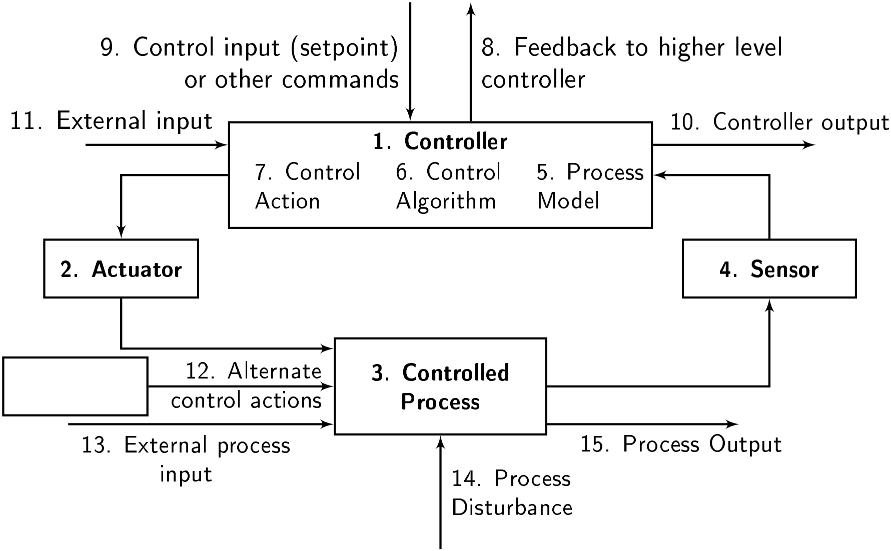
Process input missing or wrong

Unidentified or out-of-range disturbance

Process output contributes to hazard

[Leveson, 2012]

Control Elements



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

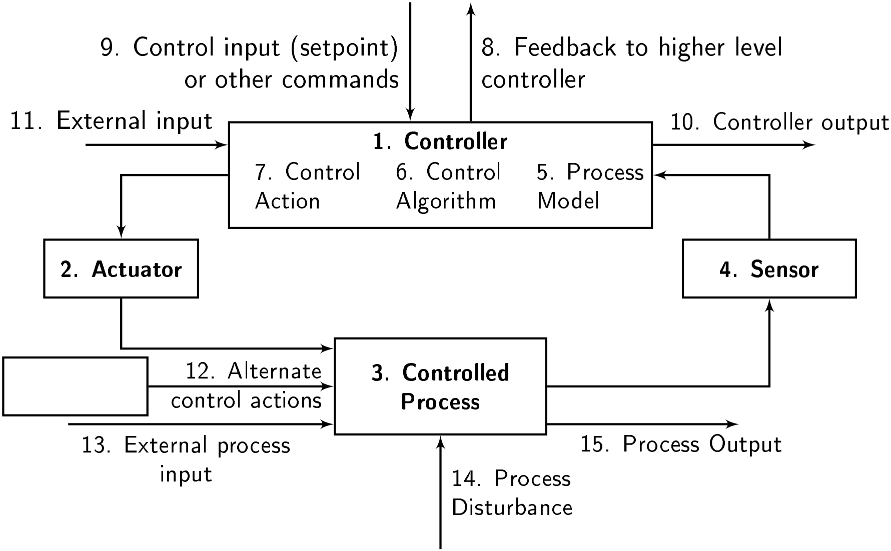
Roles in Control Loop

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

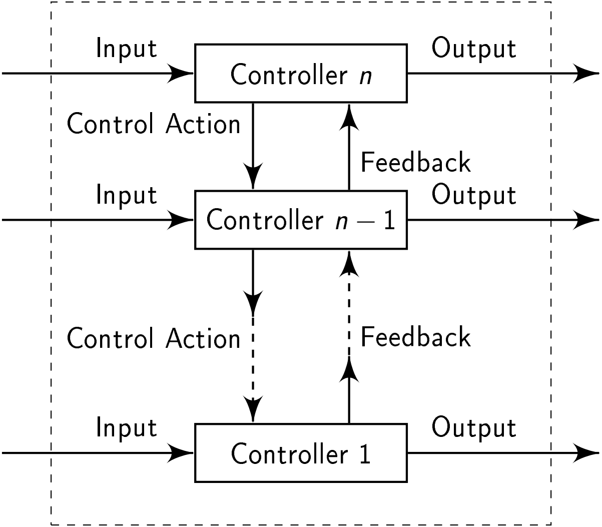
Sensor

- 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)
- Sythesizes and integrates measurement data

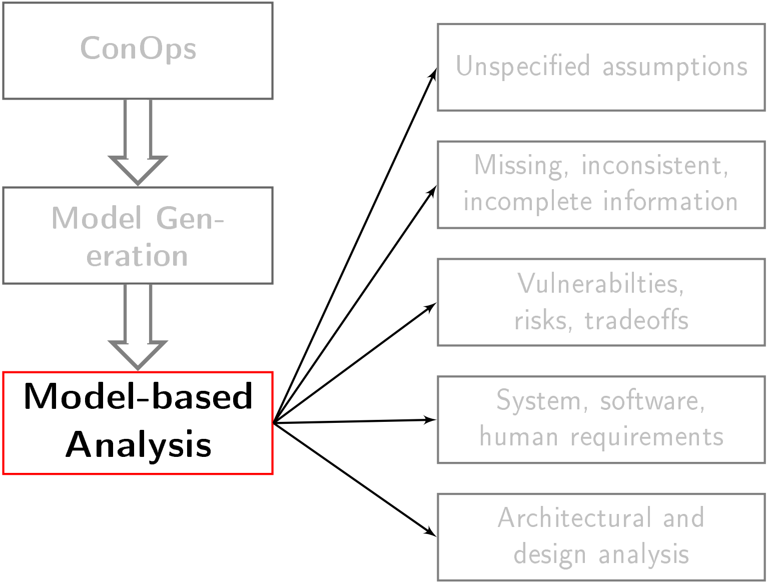
Individual Control Loop



Control Structure



Analysis



ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

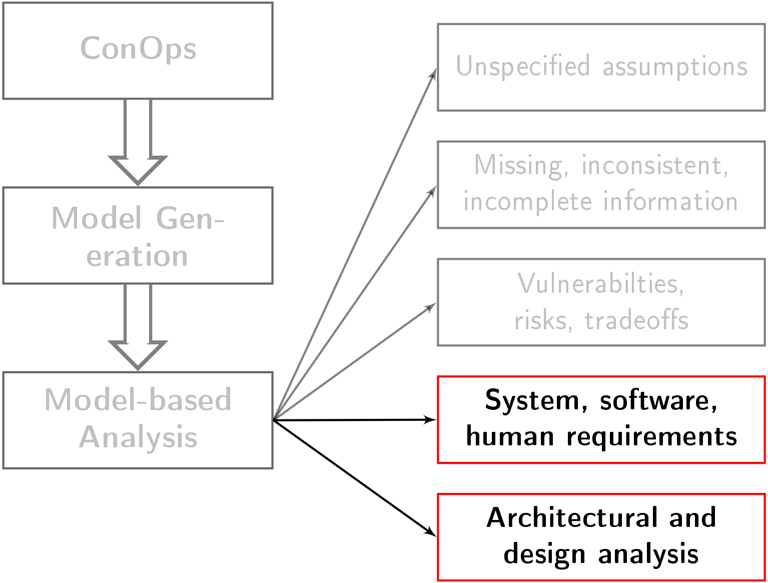
Analysis

"Completeness"

"Analyzing Safety-related Responsibilities"

"Coordination & Consistency"

Early Systems Engineering



ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

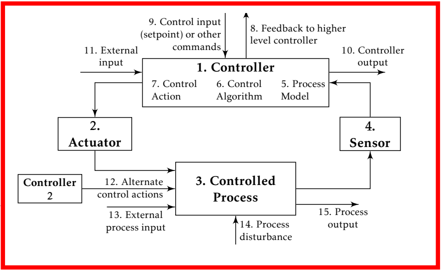
Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

Early Systems Engineering

Constraints on control loop behavior



Model-Based Analysis

Change the control structure

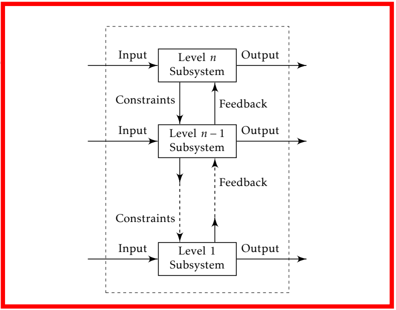


Table of Contents

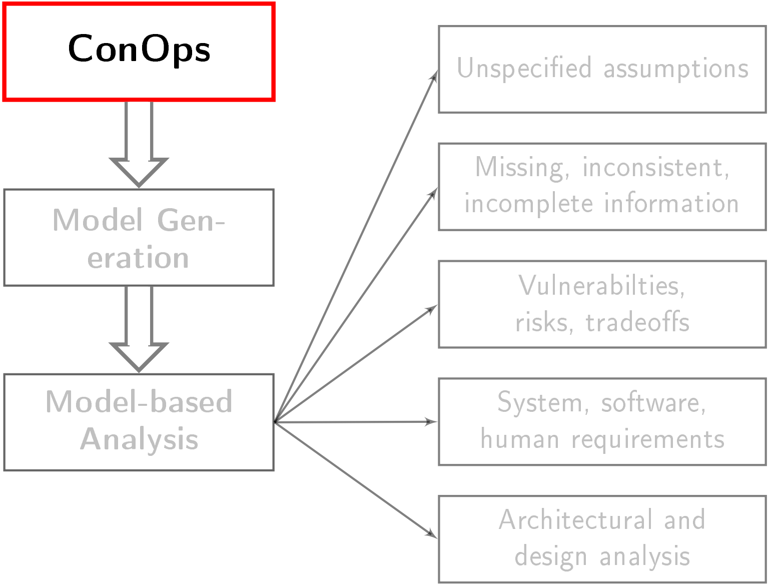
1. Theory

2. STECA

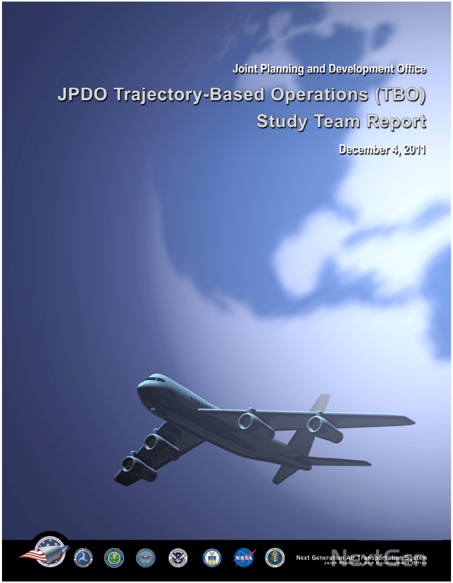
3. Application

4. Early Eng

Application—TBO


ConOps
Model Generation
Model-based Analysis
Unspecified assumptions
Missing, inconsistent, incomplete information
Vulnerabilties, risks, tradeoffs
System, software, human requirements
Architectural and design analysis

Application—TBO



Joint Planning and Development Office

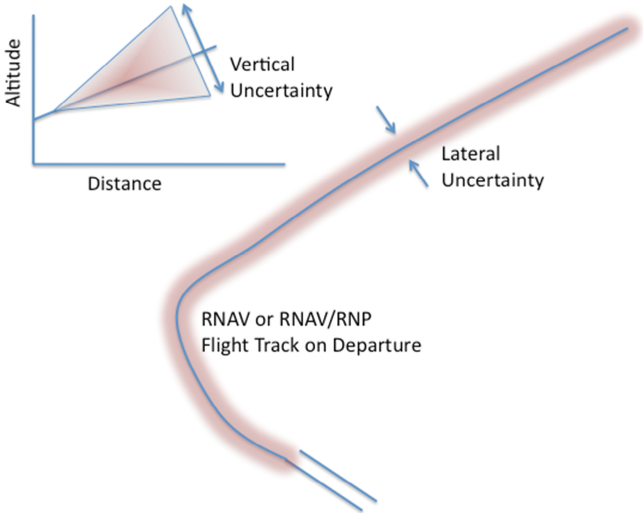
JPDO Trajectory-Based Operations (TBO)
Study Team Report

December 4, 2011

Next Generation Air Transportation System
Joint Planning and Development Office

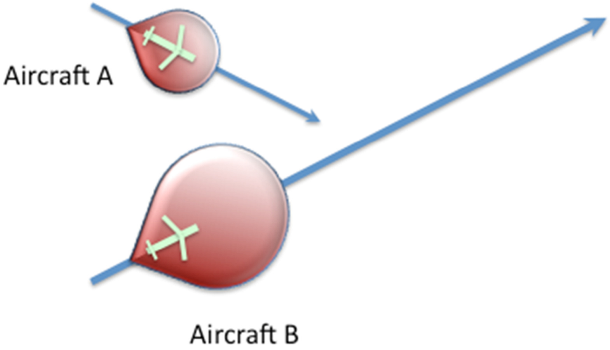
NextGen

Application—TBO



[JPDO, 2011]

Application—TBO



[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

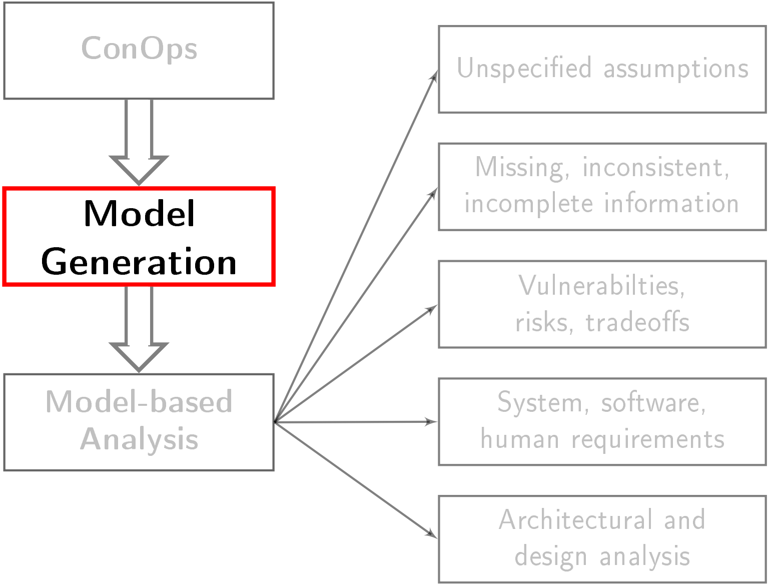
[H-3] Aircraft performs controlled maneuver into ground (CFIT, controlled flight into terrain)

[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

Vulnerabilties, 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]

Subject
Role
Behavior Type
Context

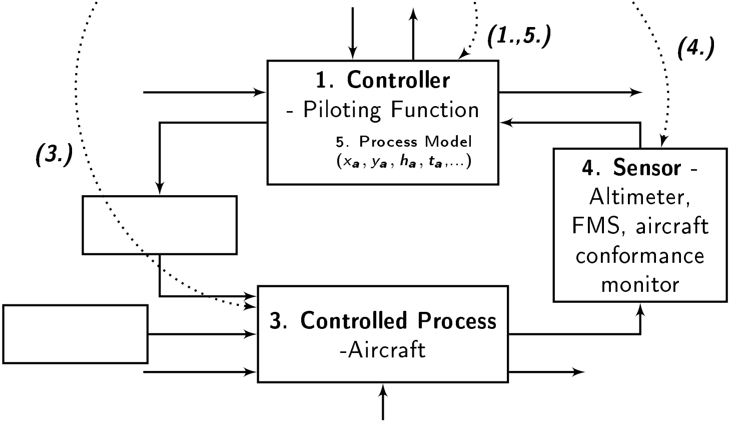
Identify Control Concepts

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]

Subject	Conformance monitoring, Air automation
Role	Sensor
Behavior Type	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)
	Sythesizes and integrates measurement data
Context	This is a decision support tool that contains algorithms to synthesize information and provide alerting based on some criteria.

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]



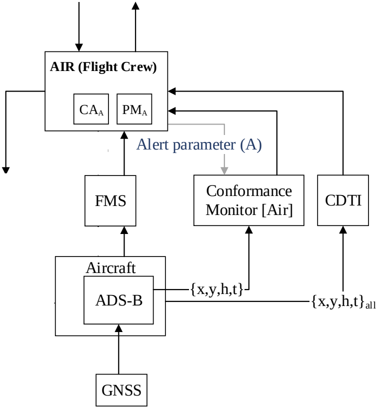
Identify Control Concepts

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]

1. Controller	Piloting function
2. Actuator	
3 Cntl'd Process	Aircraft
4. Sensor	Altimeter, FMS, Aircraft conformance monitor
5. Process Model	Intended latitude, longitude, altitude, time; Actual latitude, longitude, altitude, time
6. Cntl Algorithm	
7. Control Actions	
8. Controller Status	
9. Control Input	
10. Controller Output	
11. External Input	
12. Alt Controller	
13. Process Input	
14. Proc Disturbance	
15. Process Output	

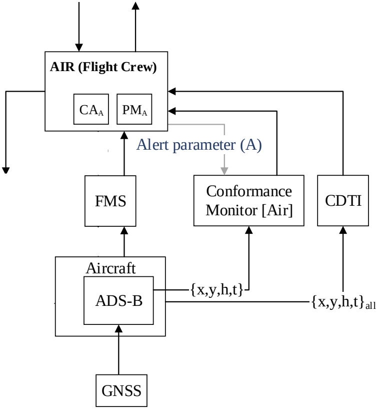
Conf Monitoring Control Loops

“Air”

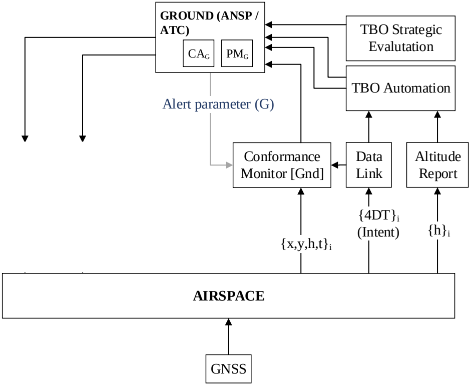


Conf Monitoring Control Loops

"Air"



"Ground"[1]

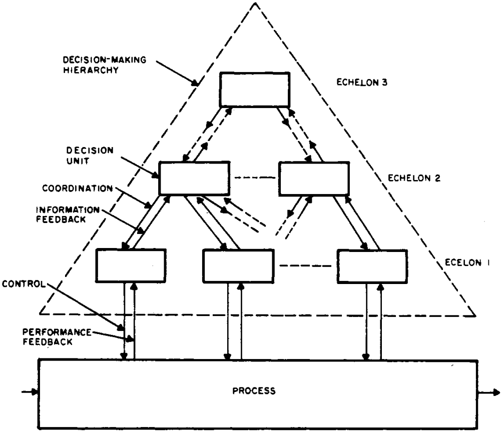


[1] Examples of model development for ground component included in backup slides

Hierarchical Control Structure

How to Establish Hierarchy?

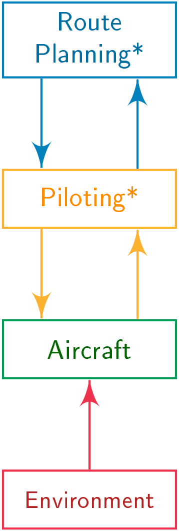
- Higher level of systems:
  - ▷ Decision Making Priority
  - ▷ Decision Complexity, ↑
  - ▷ Time Scale between decisions, ↑
  - ▷ Dynamics of controlled system, ↓



Hierarchical Control Structure

Function

Safety-Related Responsibilities

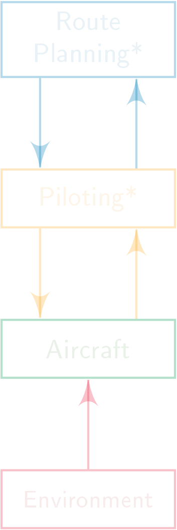


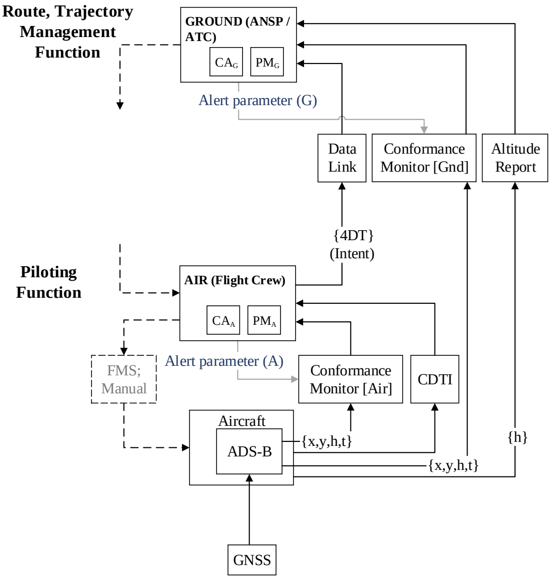
- Provide conflict-free clearances & trajectories
- Merge, sequence, space the flow of aircraft

- 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

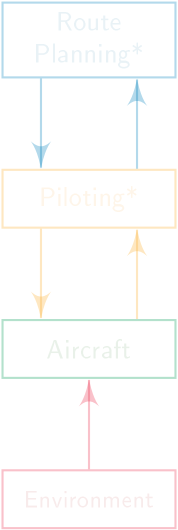
- Provide lift
- Provide propulsion (thrust)
- Orient and maintain control surfaces

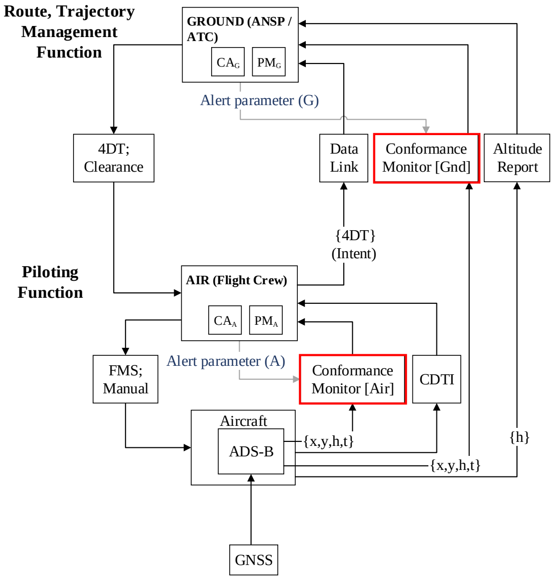
Hierarchical Control Structure

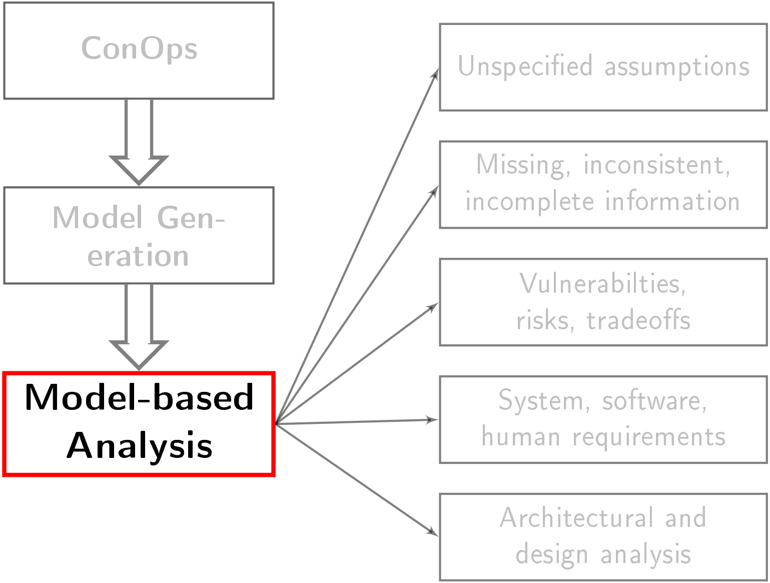




Hierarchical Control Structure







ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

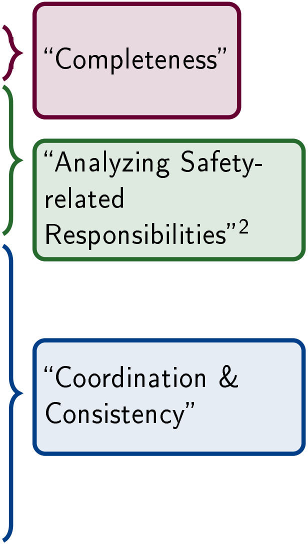
Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

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?



“Completeness”

“Analyzing Safety-related Responsibilities”[2]

“Coordination & Consistency”

Coordination & Consistency[2]

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] Example of "Analyzing Safety-related Responsibilities" included in Backup Slides on page 44

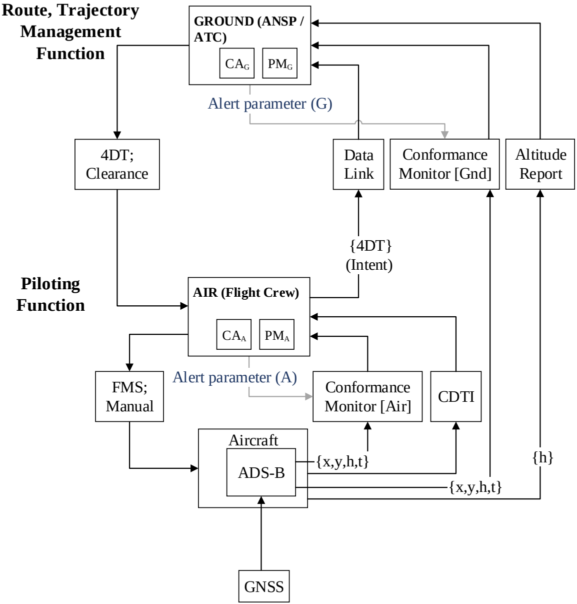
Coordination & Consistency

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

$$(\forall \mathtt{c} \in \mathscr{C}_i)\,(\forall \mathtt{d} \in \mathscr{C}_j)\,\exists\,(\mathscr{P}\,(\mathtt{c},\mathtt{d}) \vee \mathscr{P}\,(\mathtt{d},\mathtt{c}))\,[\mathtt{A}\,(\mathtt{c},\mathcal{V}_p)\ \wedge\ \mathtt{A}\,(\mathtt{d},\mathcal{V}_p)]\,, \tag{4}$$

$$\begin{multline}(\forall v \in \mathcal{V},\, \forall \mathtt{c} \in \mathscr{C}_i,\, \forall \mathtt{d} \in \mathscr{C}_j \mid \mathtt{A}\,(\mathtt{c},v) \wedge \mathtt{A}\,(\mathtt{d},v)) \\ [\rho_i(a,v) \equiv \rho_j(a,v)\ \wedge\ G_i \equiv G_j] \tag{5}\end{multline}$$

Coordination & Consistency



Coordination & Consistency

$$\mathcal{B}_{cm} := \mathcal{L}_{cm} \times D_{cm} \rightarrow \mathcal{I}_{cm}, \tag{6}$$

- $\mathcal{L}_{cm}$ is a model of the airspace state and
- D_{cm} is the decision criteria regarding conformance.

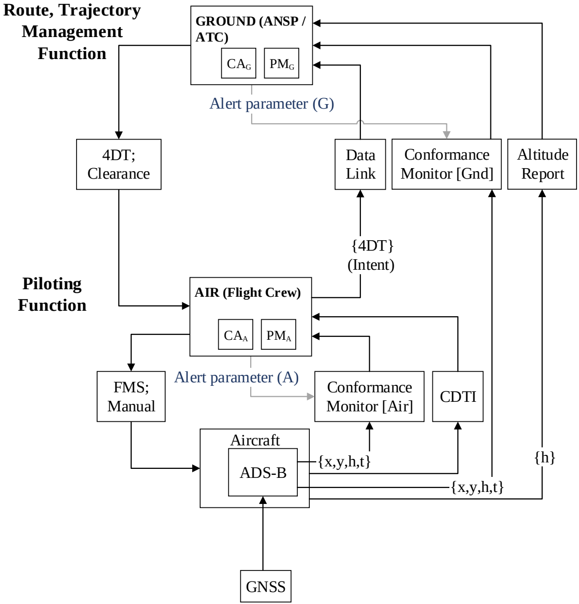
Coordination & Consistency

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

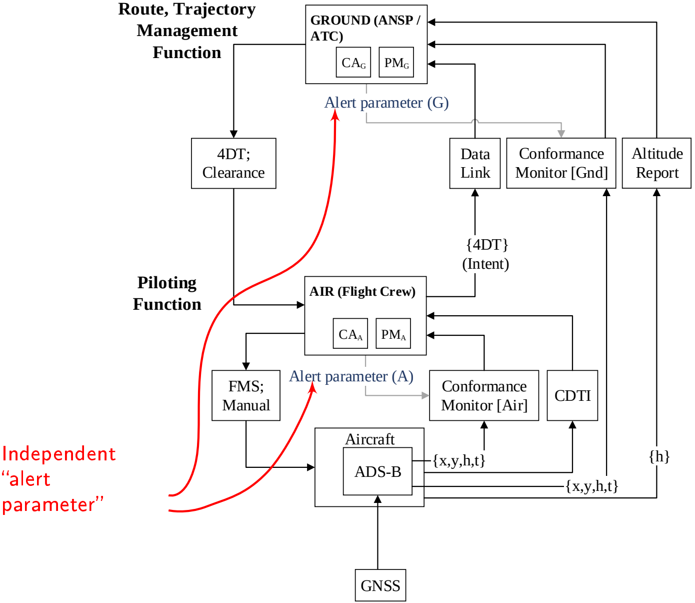
$$\begin{aligned}
z_{\text{int}} &:= \{G, C, t\}_{\text{int}} \\
z_{\text{act}} &:= \{G, C, t\}_{\text{act}} \\
\rho &:= \text{Traffic density} \\
\tau &:= \text{Operation type} \\
P_r &:= \{\text{RNP}, \text{RTP}\} \\
W &:= \text{Wake turbulence model} \\
E_{cm} &:= \text{Elliptical conformance model} \\
F_D &:= \{F, z_{\text{int}}\}
\end{aligned}$$

$$D_{cm} = \{z_{\text{act}} \,|\, z_{\text{act}} \notin \bar{z}\,(z_{\text{int}}, E_{cm}, a_{cm})\}\,, \tag{8}$$

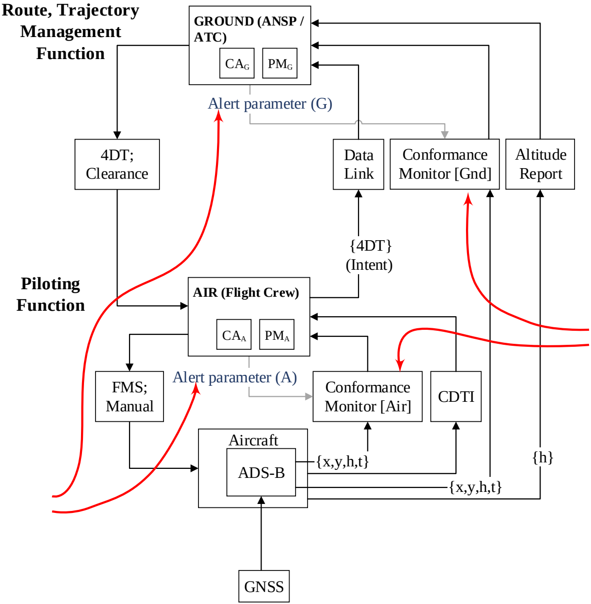
Coordination & Consistency



Coordination & Consistency



Coordination & Consistency



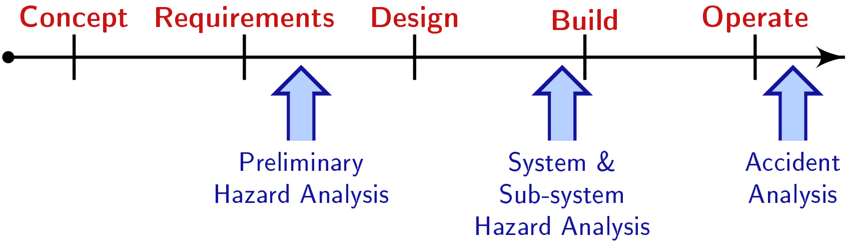
Independent "alert parameter"

Independent conformance monitors

Table of Contents

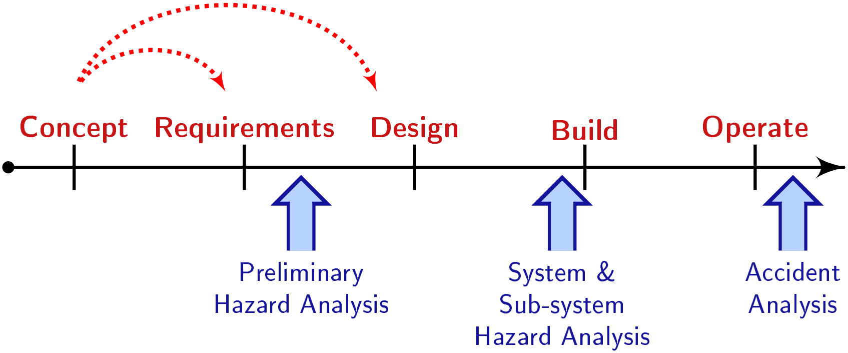
1. Theory
2. STECA
3. Application
4. Early Eng

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??



Concept

Requirements

Design

Build

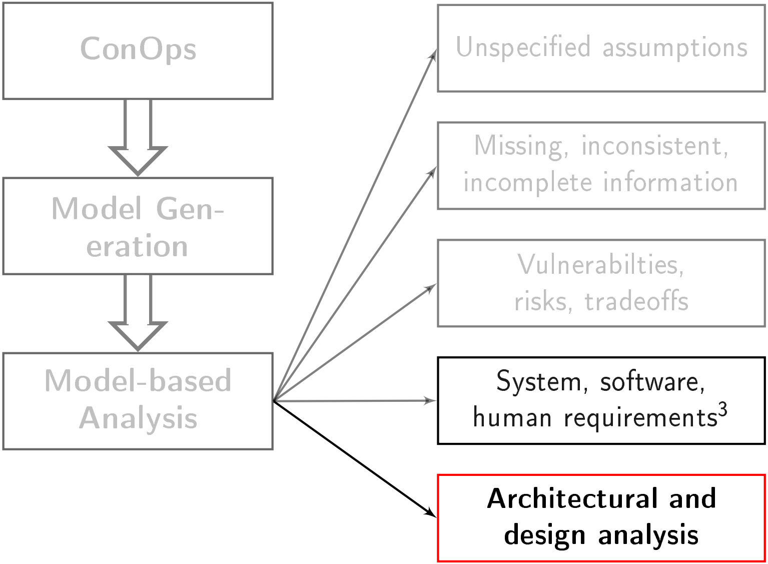
Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

Accident Analysis

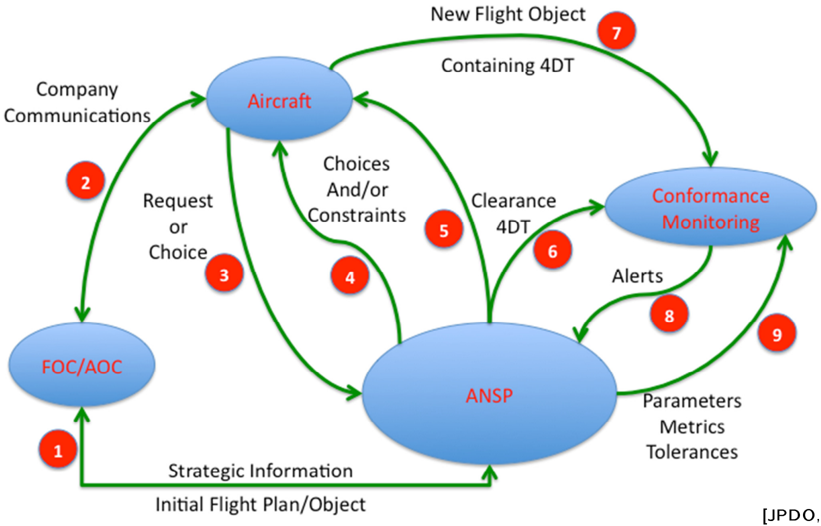
Architecture Studies


ConOps
Model Generation
Model-based Analysis
Unspecified assumptions
Missing, inconsistent, incomplete information
Vulnerabilties, risks, tradeoffs
System, software, human requirements[3]
Architectural and design analysis

[3] Examples of reqs identification included in backup slides on page 48

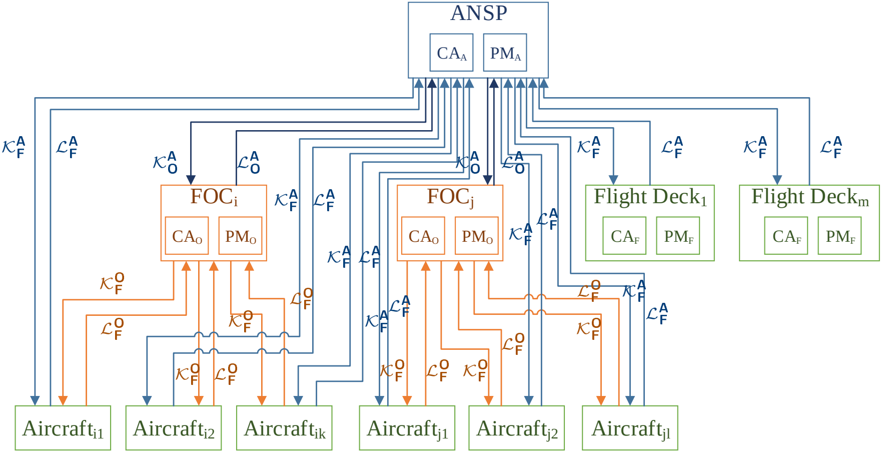
Architecture Studies

Negotiation

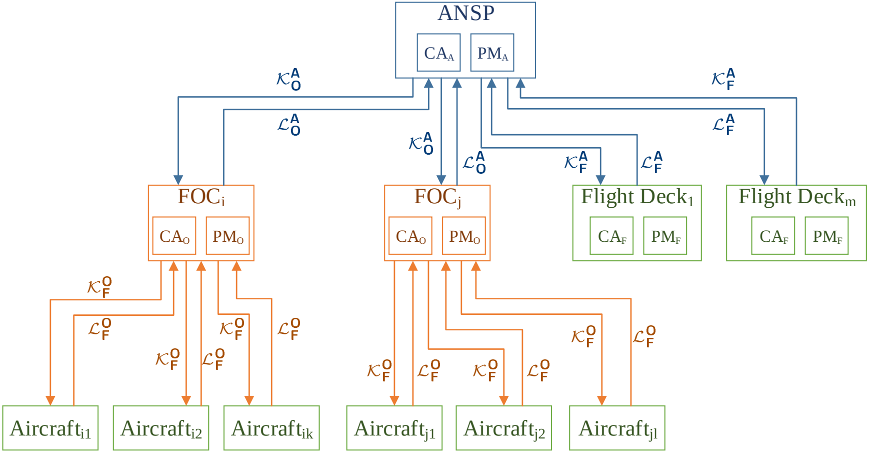


[JPDO, 2011]

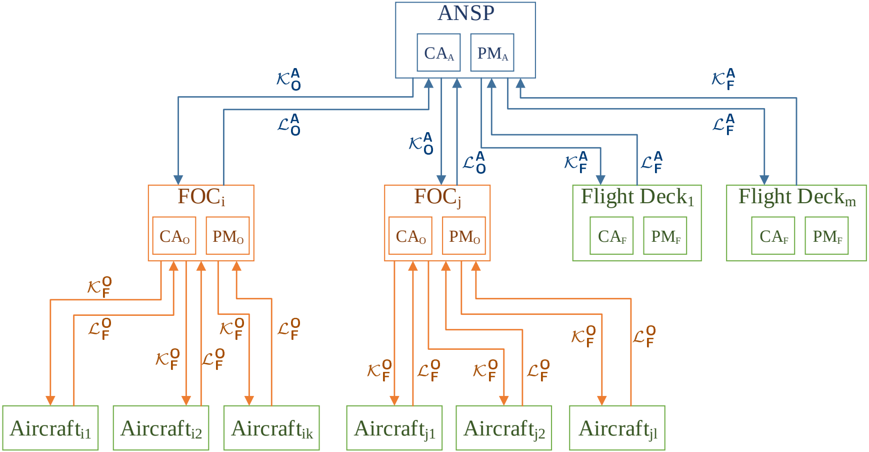
TBO Negotiation



Modified Structure

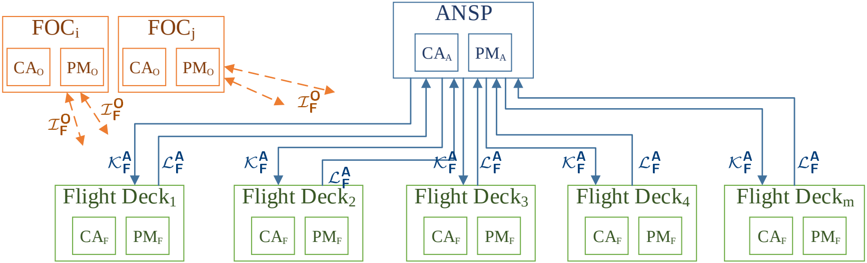


Modified Structure

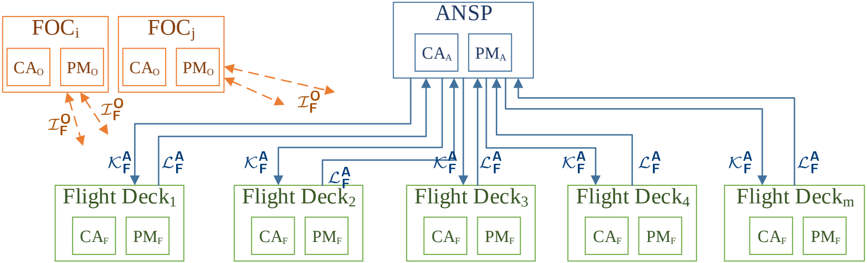


Additional Requirement: $\mathcal{K}_F^A$ and $\mathcal{K}_F^O$ shall *not* occur simultaneously.

Modified Structure



Modified Structure

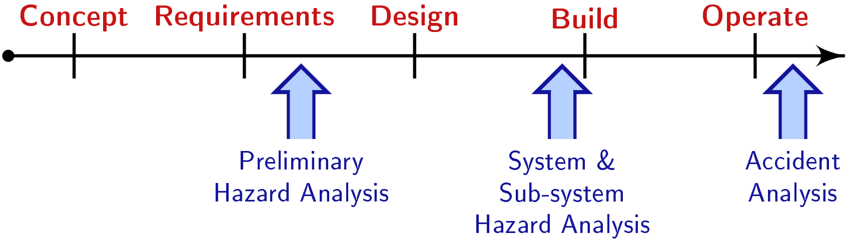


ANSP
$\mathrm{CA_A}$
$\mathrm{PM_A}$
$\mathrm{FOC_i}$
$\mathrm{CA_O}$
$\mathrm{PM_O}$
$\mathrm{FOC_j}$
$\mathrm{CA_O}$
$\mathrm{PM_O}$
$\mathcal{I}_\mathsf{F}^\mathsf{O}$
$\mathcal{I}_\mathsf{F}^\mathsf{O}$
$\mathcal{I}_\mathsf{F}^\mathsf{O}$
$\mathcal{K}_\mathsf{F}^\mathsf{A}$
$\mathcal{L}_\mathsf{F}^\mathsf{A}$
$\mathcal{K}_\mathsf{F}^\mathsf{A}$
$\mathcal{L}_\mathsf{F}^\mathsf{A}$
$\mathcal{K}_\mathsf{F}^\mathsf{A}$
$\mathcal{L}_\mathsf{F}^\mathsf{A}$
$\mathcal{K}_\mathsf{F}^\mathsf{A}$
$\mathcal{L}_\mathsf{F}^\mathsf{A}$
$\mathcal{K}_\mathsf{F}^\mathsf{A}$
$\mathcal{L}_\mathsf{F}^\mathsf{A}$
Flight $\mathrm{Deck_1}$
Flight $\mathrm{Deck_2}$
Flight $\mathrm{Deck_3}$
Flight $\mathrm{Deck_4}$
Flight $\mathrm{Deck_m}$
$\mathrm{CA_F}$
$\mathrm{PM_F}$

Additional Requirement: This becomes the active control structure within TBD minutes of gate departure.

Conclusion

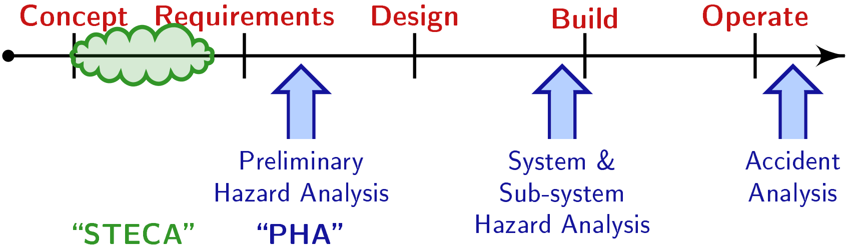
Systems Engineering Phases


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

Safety Activities

Conclusion

Systems Engineering Phases



Concept Requirements Design Build Operate

Preliminary Hazard Analysis

System & Sub-system Hazard Analysis

Accident Analysis

“STECA” “PHA”

Safety Activities

Thanks!

fleming@virginia.edu

References

Ashby, W. R. (1957). *An Introduction to Cybernetics*. Chapman & Hall Ltd.

Business Korea (2014). Auto parts manufacturers concerned over new ordinary wage standards.

Checkland, P. (1999). *Systems thinking, systems practice: includes a 30-year retrospective*. John Wiley & Sons, Inc.

Frola, F. and Miller, C. (1984). System safety in aircraft management. *Logistics Management Institute, Washington DC*.

JPDO (2011). JPDO Trajectory-Based Operations (TBO) study team report. Technical report, Joint Planning and Development Office.

JPDO (2012). Capability safety assessment of trajectory based operations v1.1. Technical report, Joint Planning and Development Office Capability Safety Assessment Team.

Leveson, N. G. (2012). *Engineering a Safer World*. MIT Press.

Mesarovic, M. D. (1970). Multilevel systems and concepts in process control. *Proceedings of the IEEE*, 58(1):111–125.

Strafaci, A. (2008). What does BIM mean for civil engineers? *CE News, Tranportation*.

Vincoli, J. W. (2005). *Basic Guide to System Safety, Second Edition*. John Wiley & Sons, Inc., Hoboken, NJ, USA.

Backup Slides

Table of Contents

5. TBO Analysis

6. Early Eng

7. STAMP

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]

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]

Subject
Role
Behavior Type
Context

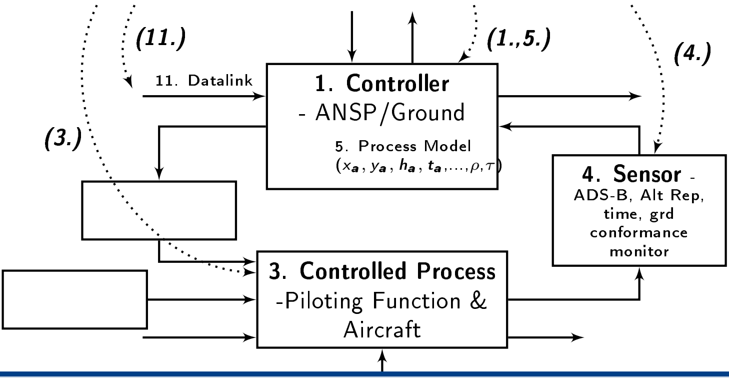
Ground

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]

Subject	Conformance monitoring, Ground automation
Role	Sensor
Behavior Type	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)
	Sythesizes and integrates measurement data
Context	This is a decision support tool that contains algorithms to synthesize information and provide alerting based on some criteria.

Ground

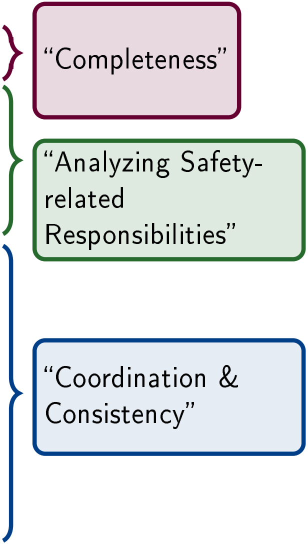
Independent of the aircraft, the ANSP uses ADS-B position reporting for lateral and longitudinal progress, altitude reporting for vertical, and tools that measure the time progression for the flight track. Data link provides aircraft intent information. Combined, this position and timing information 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]



(11.)
(1.,5.)
(4.)
(3.)
11. Datalink
1. Controller
- ANSP/Ground
5. Process Model
$(x_a, y_a, h_a, t_a, \ldots, \rho, \tau)$
4. Sensor -
ADS-B, Alt Rep, time, grd conformance monitor
3. Controlled Process
-Piloting Function & Aircraft

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?



"Completeness"

"Analyzing Safety-related Responsibilities"

"Coordination & Consistency"

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)

$$(\forall \sigma_i \in \Sigma)\,(\exists \mathtt{c} \in \mathscr{C})\,[\mathtt{P}\,(\mathtt{c}, \sigma_i)]\,, \tag{2}$$

$$(\forall H_i \in \mathcal{H})\,(\neg\exists \mathtt{c} \in \mathscr{C})\,[\mathtt{P}\,(\mathtt{c}, H_i)\;\wedge\;\mathtt{P}\,(\mathtt{c}, \mathcal{G})] \tag{3}$$

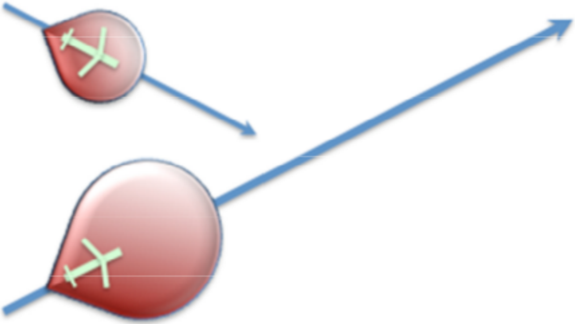
Safety-Related Responsibilities

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

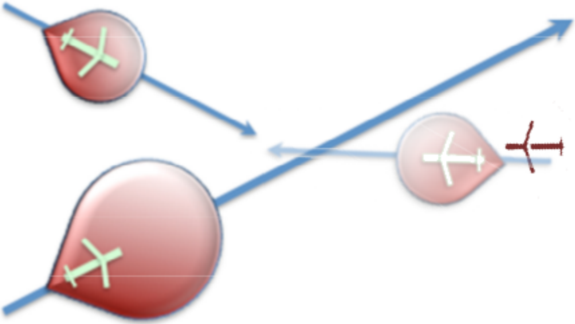


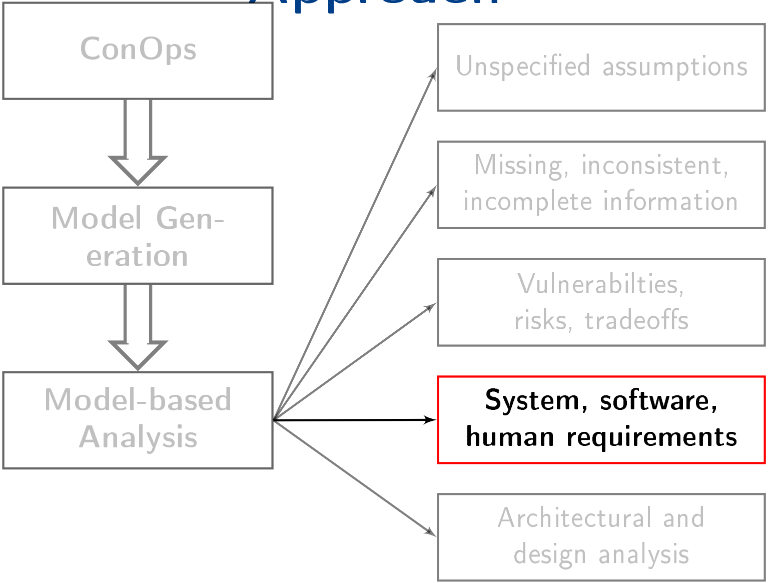
Table of Contents

5. TBO Analysis

6. Early Eng

7. STAMP

Approach



ConOps

Model Generation

Model-based Analysis

Unspecified assumptions

Missing, inconsistent, incomplete information

Vulnerabilties, risks, tradeoffs

System, software, human requirements

Architectural and design analysis

Deriving Requirements

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]

Deriving Requirements

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
- ...

Deriving Requirements

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

Deriving 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

Deriving 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

...

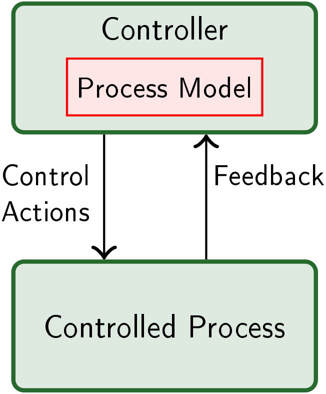
S3.2 ANSP must be able to generate aircraft velocity changes that close the trajectory within TBD minutes (or TBD nmi).
Rationale: *TBO ConOps is unclear about how ANSP will help the aircraft work to close trajectory. Refined requirements will deal with providing the ANSP feedback about the extent to which the aircraft does not conform, the direction and time, which can be used to calculate necessary changes.*

Component Interaction Constraints

Table of Contents

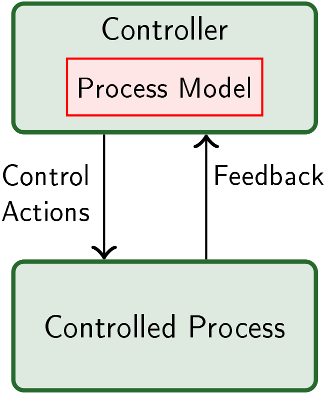
STAMP

- 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.



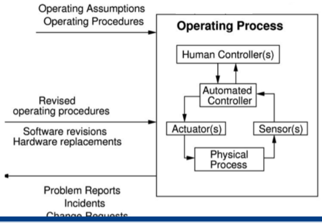
STAMP

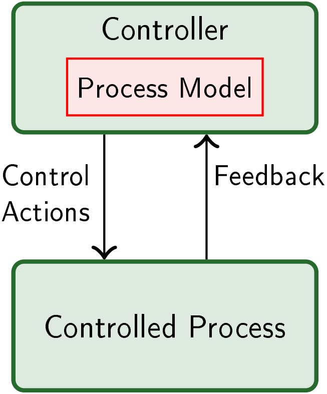
- Controllers use a **process model** to determine control actions
- Accidents often occur when the process model is incorrect
- Four types of unsafe control actions:
  1. **Not providing** the control action causes the hazard
  2. **Providing** the control action causes the hazard
  3. The **timing** 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.



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

STAMP




Controller

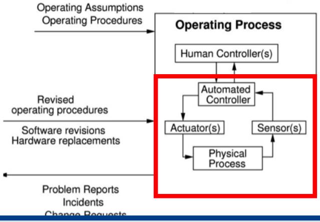
Process Model

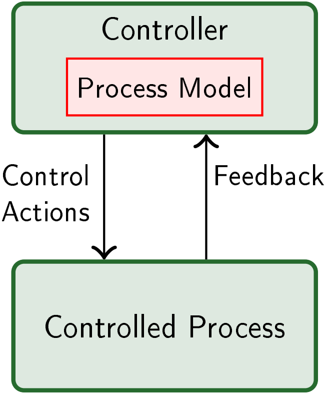
Control Actions

Feedback

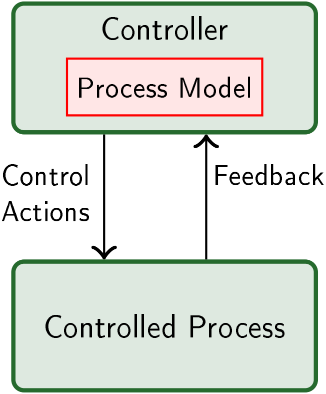
Controlled Process

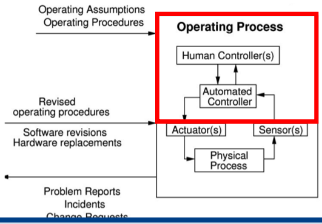
STAMP


Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated Controller
Actuator(s)
Sensor(s)
Physical Process
Revised operating procedures
Software revisions
Hardware replacements
Problem Reports
Incidents
Change Requests

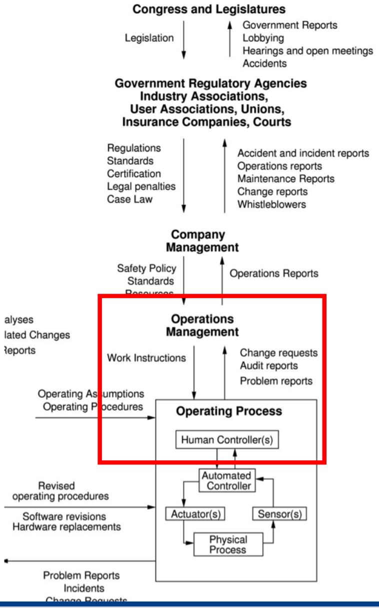

Controller
Process Model
Control Actions
Feedback
Controlled Process

STAMP


Controller
Process Model
Control Actions
Feedback
Controlled Process


Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated Controller
Revised operating procedures
Software revisions
Hardware replacements
Actuator(s)
Sensor(s)
Physical Process
Problem Reports
Incidents
Change Requests

STAMP



Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company
Management

Safety Policy
Standards
Resources

Operations Reports

alyses
lated Changes
Reports

Operations
Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated
Controller

Actuator(s)

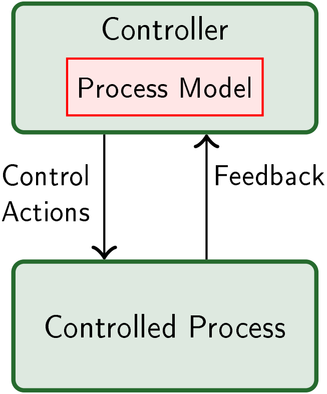
Sensor(s)

Physical
Process

Revised
operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests



Controller

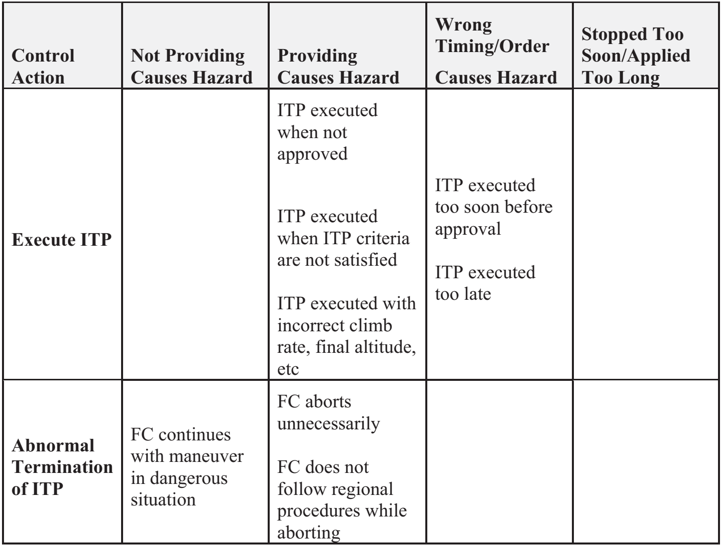
Process Model

Control
Actions

Feedback

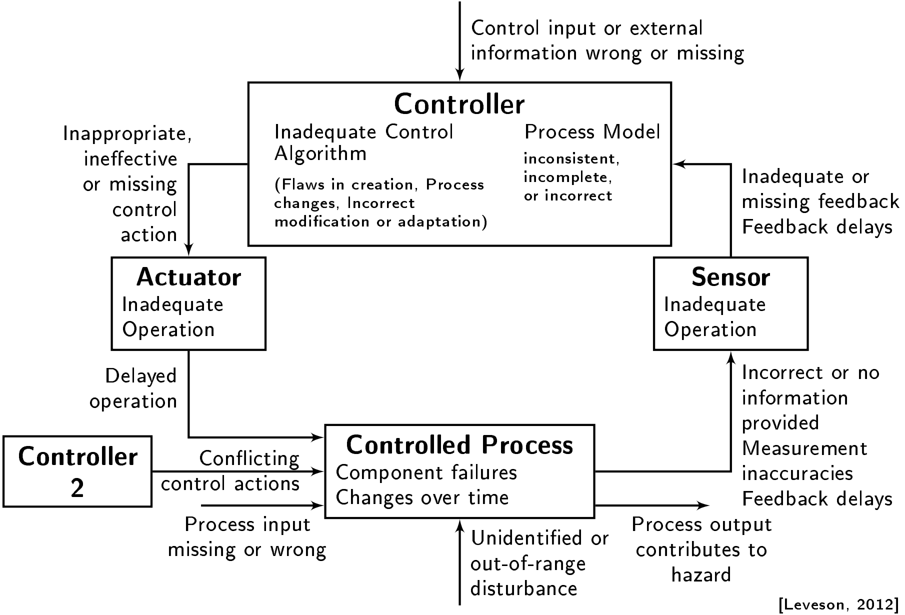
Controlled Process

Unsafe Control Actions



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

Control Flaws



Control input or external information wrong or missing

Controller

Inadequate Control Algorithm

(Flaws in creation, Process changes, Incorrect modification or adaptation)

Process Model

inconsistent, incomplete, or incorrect

Inappropriate, ineffective or missing control action

Inadequate or missing feedback
Feedback delays

Actuator
Inadequate Operation

Sensor
Inadequate Operation

Delayed operation

Incorrect or no information provided
Measurement inaccuracies
Feedback delays

Controller 2

Conflicting control actions

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]