Model-based Concept Development and Safety Driven Design

Cody H Fleming
with: Nancy Leveson

Stuttgart, Germany

23 September 2014

MIT
AEROASTRO

Table of Contents

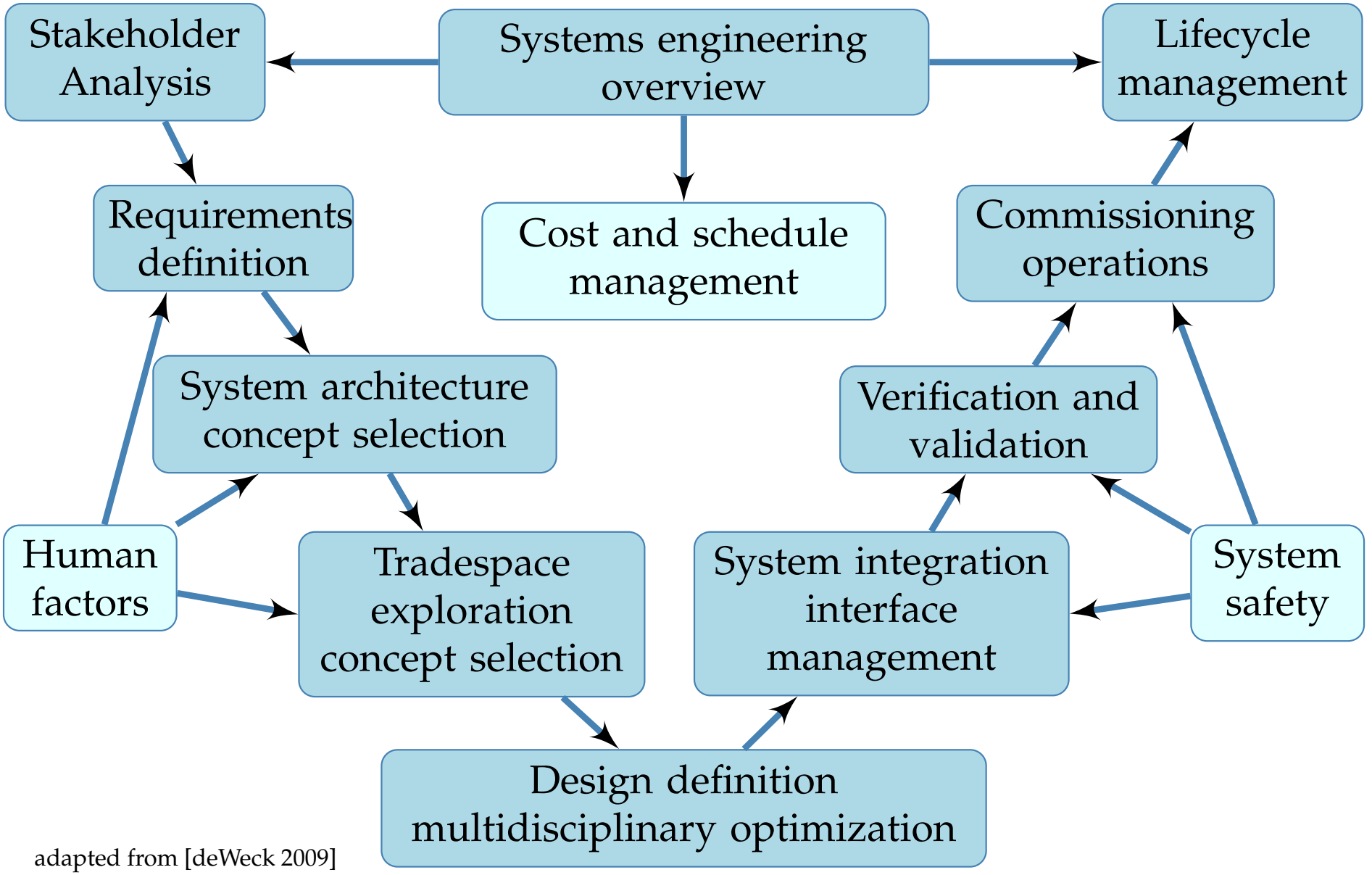
Table of Contents

Motivation

Safety must be designed and built into airplanes, just as are performance, stability, and structural integrity. [Stieglitz, 1948]

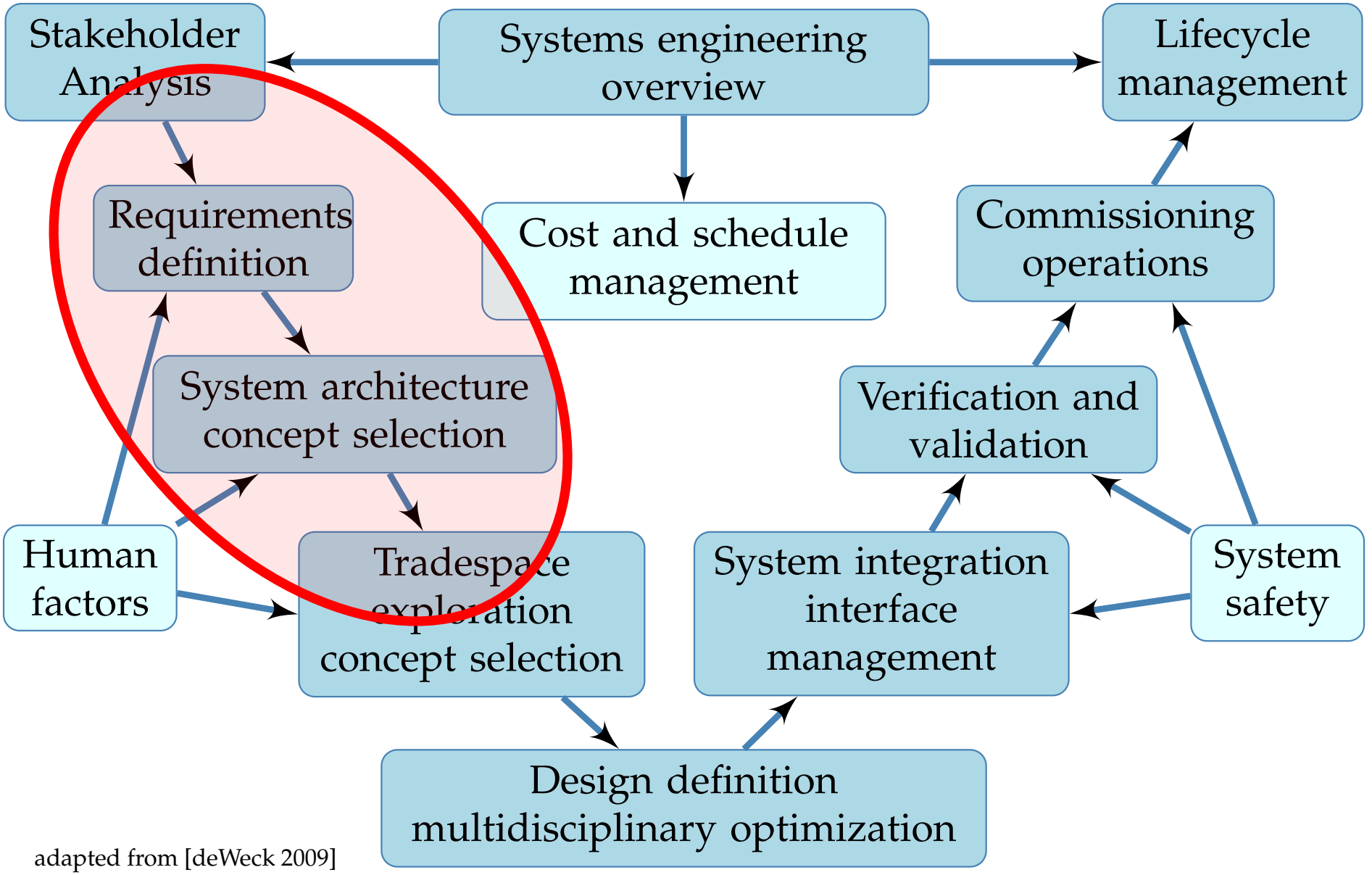
$\Rightarrow$ What is true for airplanes is true for any system

Systems Engineering Vee



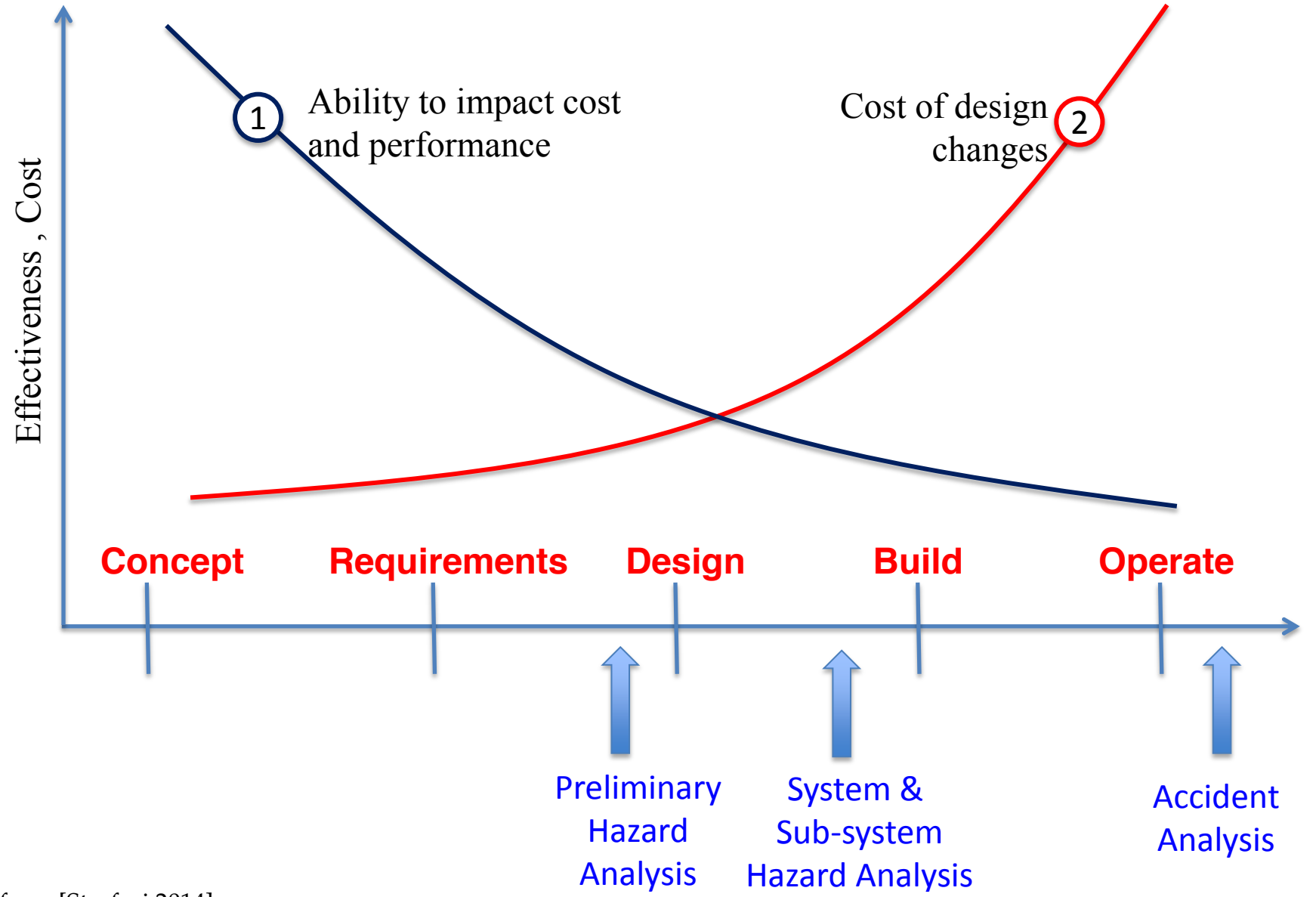
adapted from [deWeck 2009]

Systems Engineering Vee



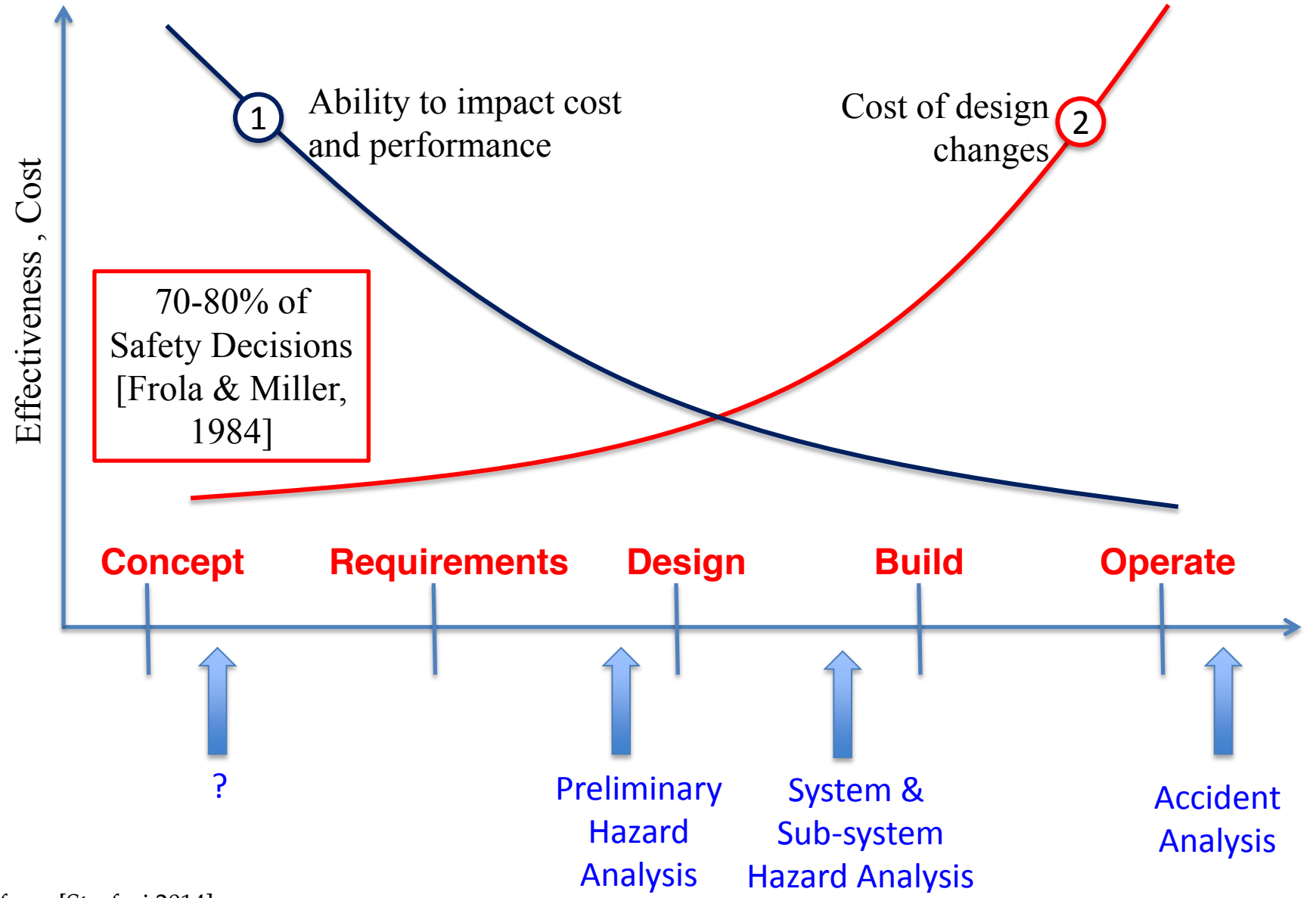
adapted from [deWeck 2009]

Motivation



adapted from [Strafaci 2014]

Motivation



adapted from [Strafaci 2014]

Framing Questions & Goals

1. Can we develop tools to assess safety-related properties of a concept?

2. Can we develop tools that help analysts, stakeholders, and designers to develop the concept in a safety-driven fashion?

Framing Questions & Goals

1. Can we develop tools to assess safety-related properties of a concept?
   - Improve hazard analysis of an existing Concept of Operations

2. Can we develop tools that help analysts, stakeholders, and designers to develop the concept in a safety-driven fashion?
   - Establish safety-driven design theory & methodology to develop a Concept of Operations
   - "safety-driven development", "safety-driven architecting"

In order to improve on the existing state of practice, the method should help analysts and stakeholders to identify:

1. missing information that will be required for safe operation of the system,

2. inconsistent or conflicting information that may lead to hazardous behavior,

3. where more specific operational concepts are required to understand safety- and functionally-related behavior of the system

Table of Contents

Systems Engineers

[China Daily Show, 2014]

Concept of Operations [CONOPS]

Describes the way the system works from the operator's perspective. The ConOps includes the user description and summarizes the needs, goals, and characteristics of the system's user community. This includes operation, maintenance, and support personnel. [INCOSE, 2011]

View of "how the system works"

Concept of Operations [CONOPS]

Describes the way the system works from the operator's perspective. The ConOps includes the user description and summarizes the needs, goals, and characteristics of the system's user community. This includes operation, maintenance, and support personnel. [INCOSE, 2011]

Characteristics of this phase:

- Little design detail is available
- Often occurs before engineering requirements exist
- Natural language text
- Developed by committee, disparate views of system

Problem:

Informal, natural language description of system makes it difficult to identify and "track" interactions, emergent behavior, etc.

Analysis of a ConOps

Problem:

Informal, natural language description of system makes it difficult to identify and "track" interactions, emergent behavior, etc.

Solution:

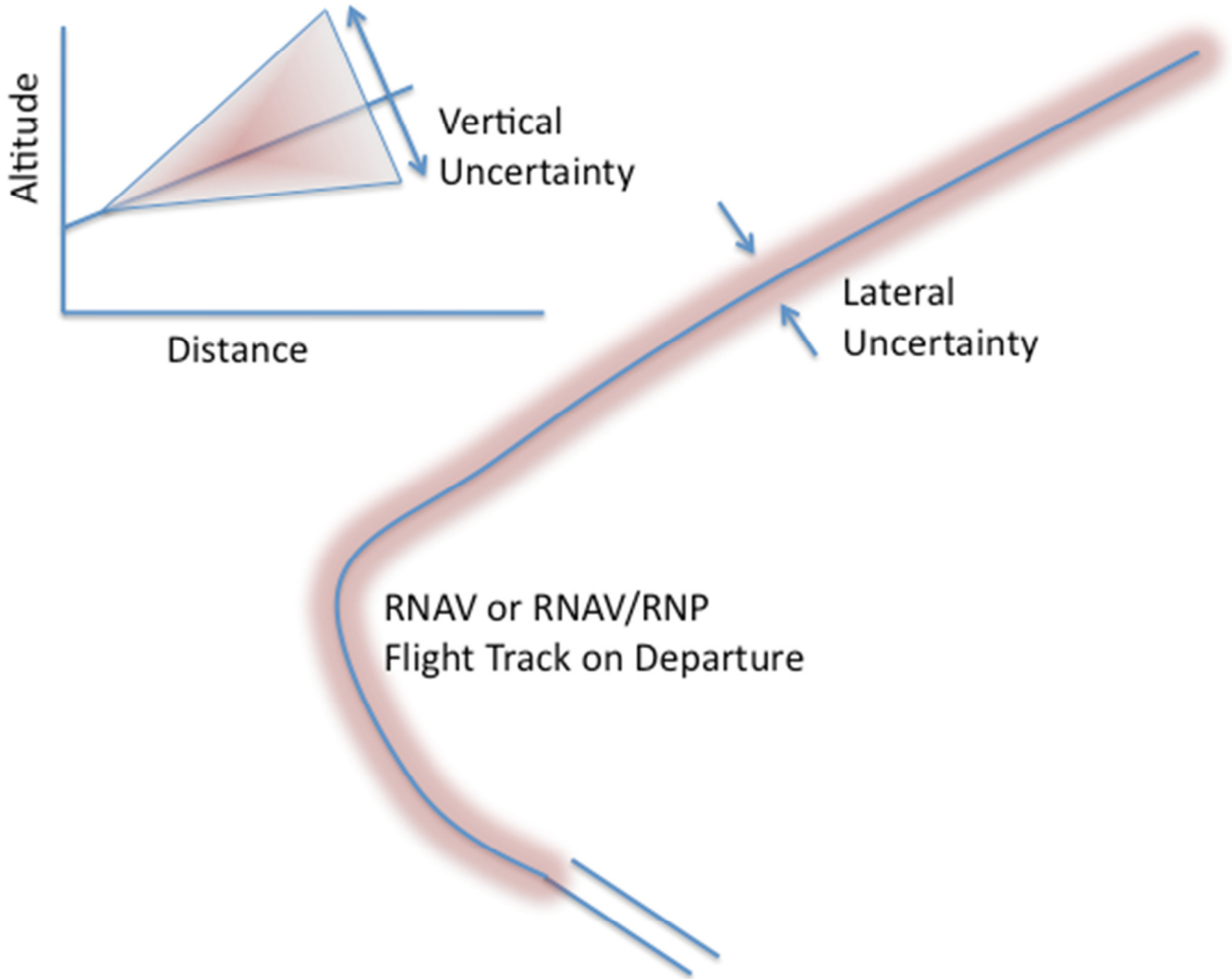
Using a model-based approach based on the STAMP accident causality will help overcome these problems and meet goals 1-3 above

Trajectory-Based Operations

- GENERAL ATM — 2 VERY generic functions required to operate the airspace
  - Strategic and tactical generation and management of trajectories within an air volume
    - ≈ATC today
  - Navigating of individual aircraft along those prescribed trajectories
    - ≈Pilots today

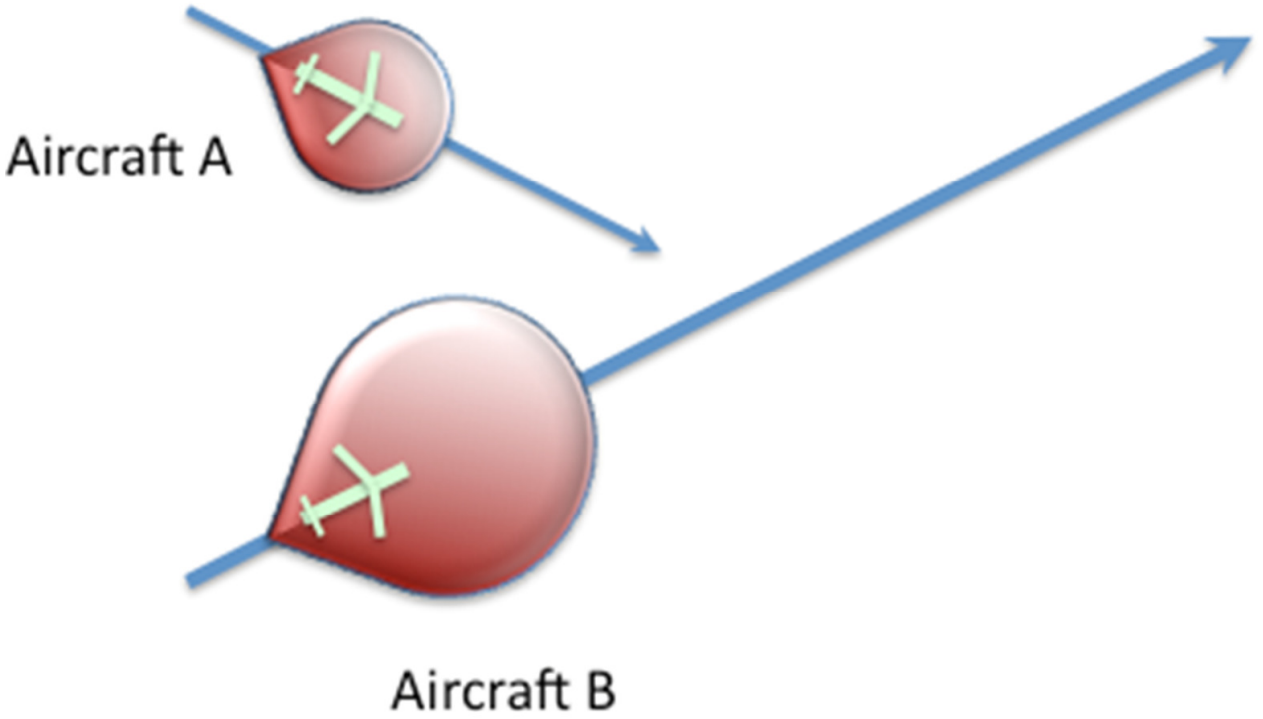
- TBO in particular (Trajectory-based Operations)
  - Same general functions, but specific mechanism for managing trajectories: 4DT
  - Roles within/across the two functions will also change

Trajectory-Based Operations



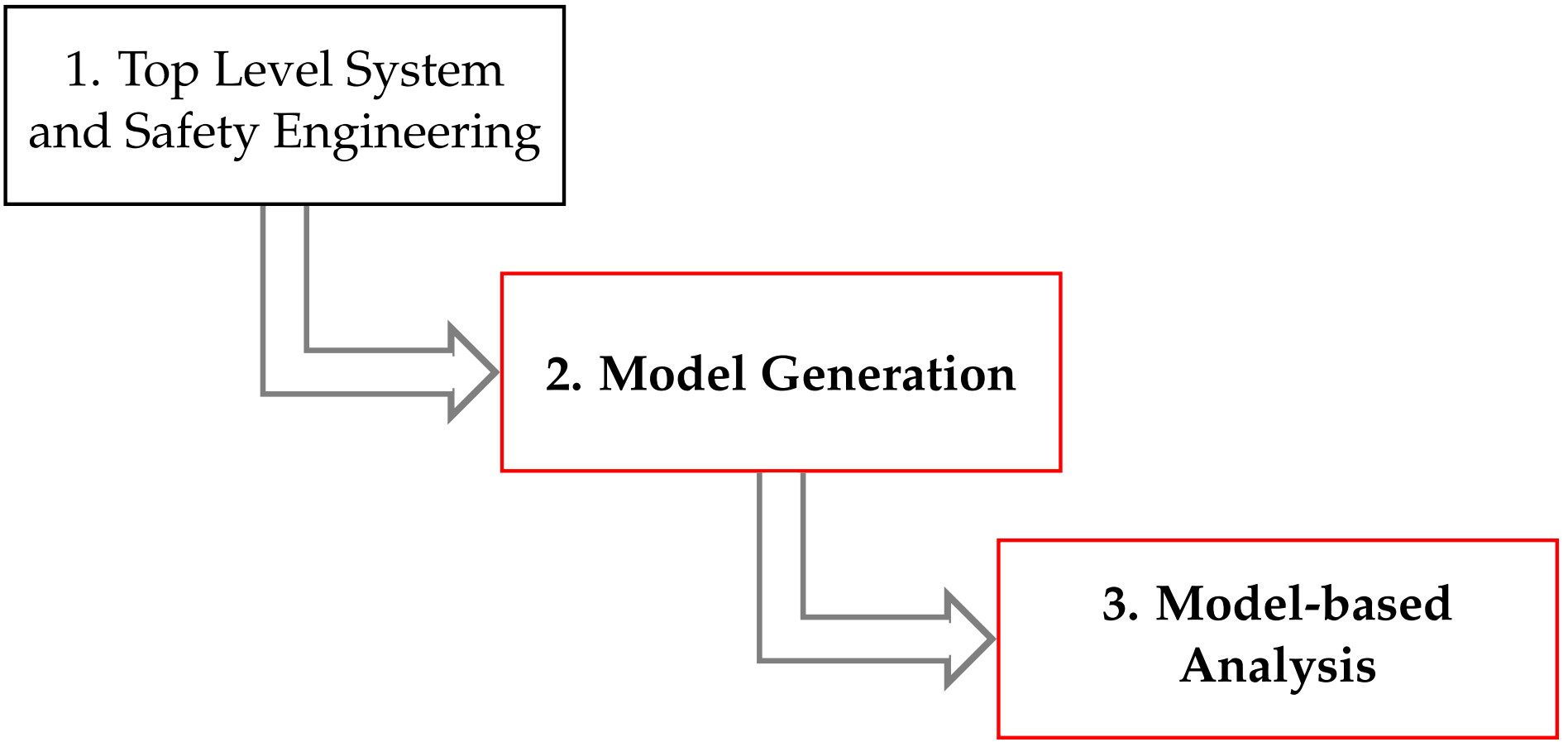
[JPDO, 2011]

Trajectory-Based Operations

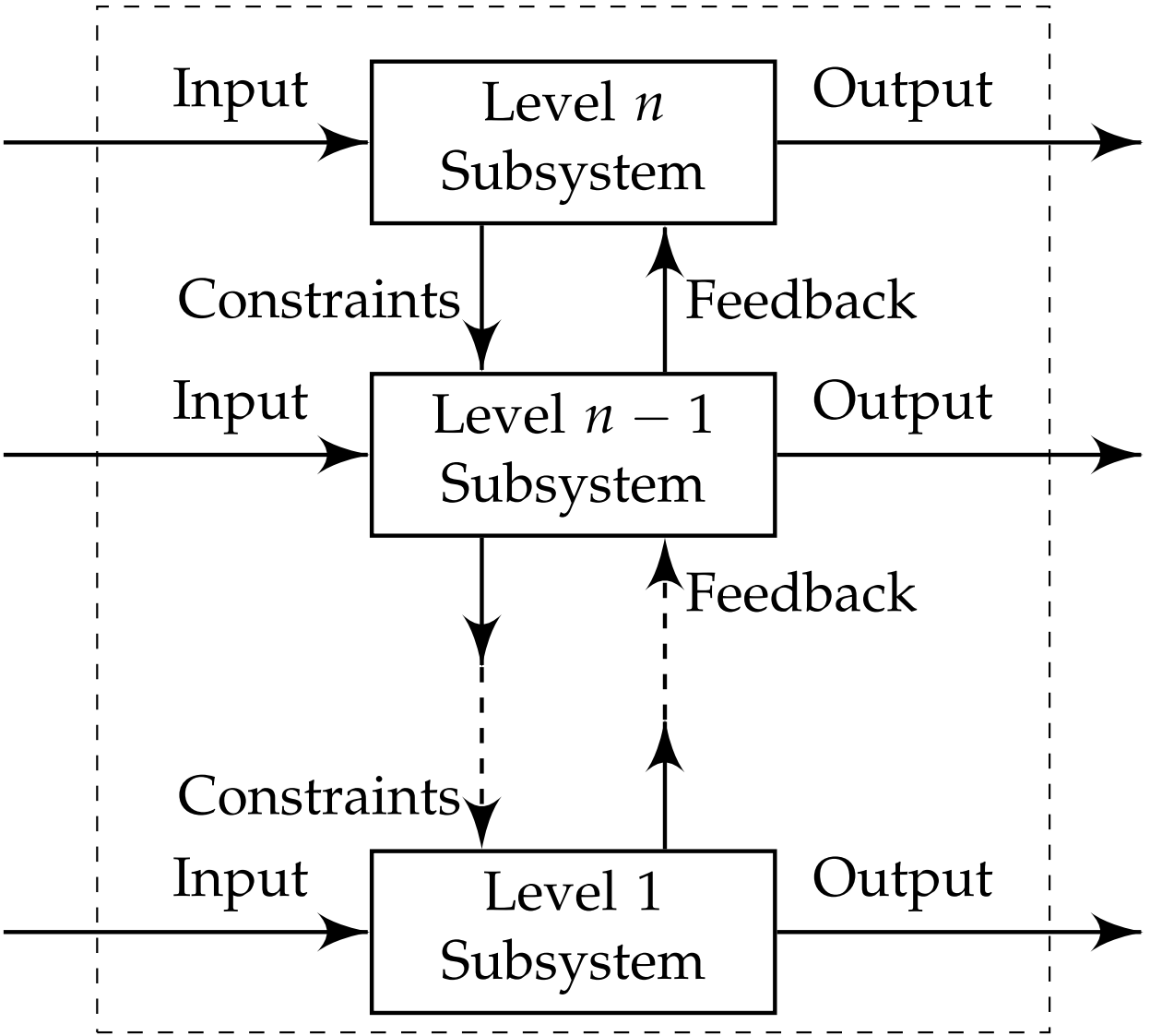


[JPDO, 2011]

Table of Contents


1. Top Level System and Safety Engineering
2. Model Generation
3. Model-based Analysis

The systems approach...recognizes that needs or problems originating at one level invariably have contributing factors at higher levels [Miles Jr, 1973]



[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

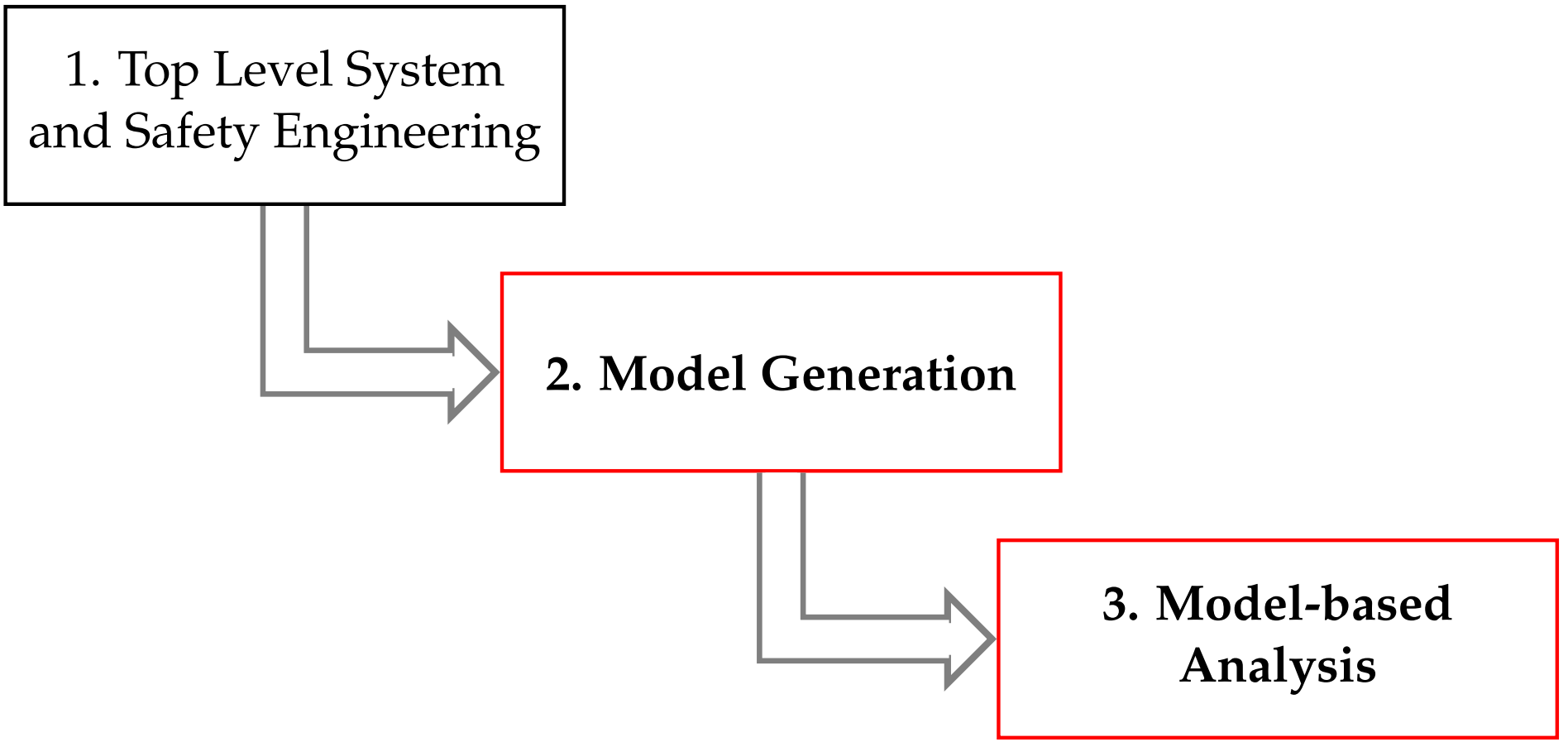
4. Observability condition: the controller must be able to ascertain the state of the system, typically by feedback from a sensor

[Ashby, 1957; Leveson, 2012]

Remember Goals and Problems

Identify:

1. missing information
2. inconsistent or conflicting information
3. more specific operational concepts


1. Top Level System and Safety Engineering
2. Model Generation
3. Model-based Analysis

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

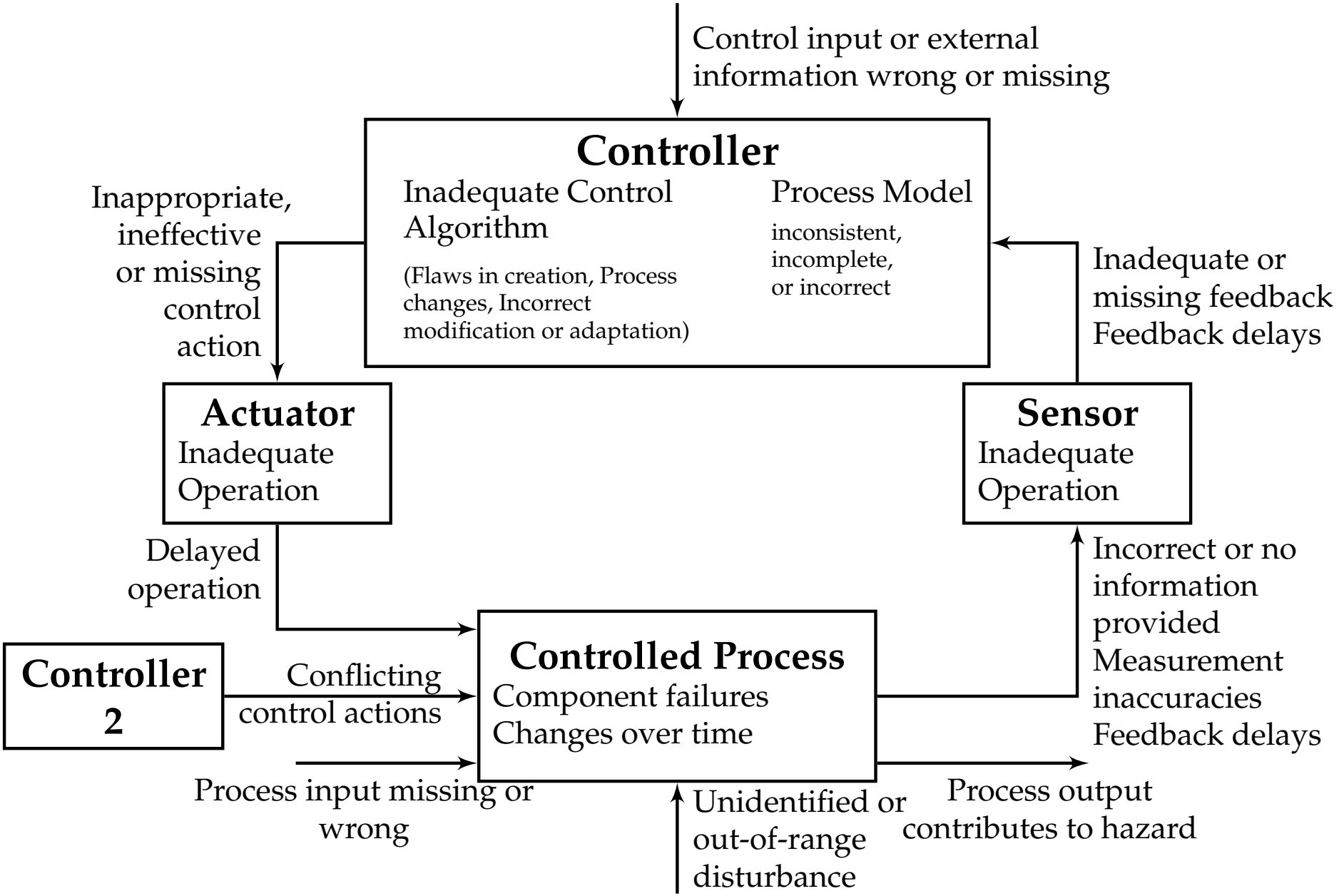
Roles in Control Loop

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

Control Elements



Control Elements

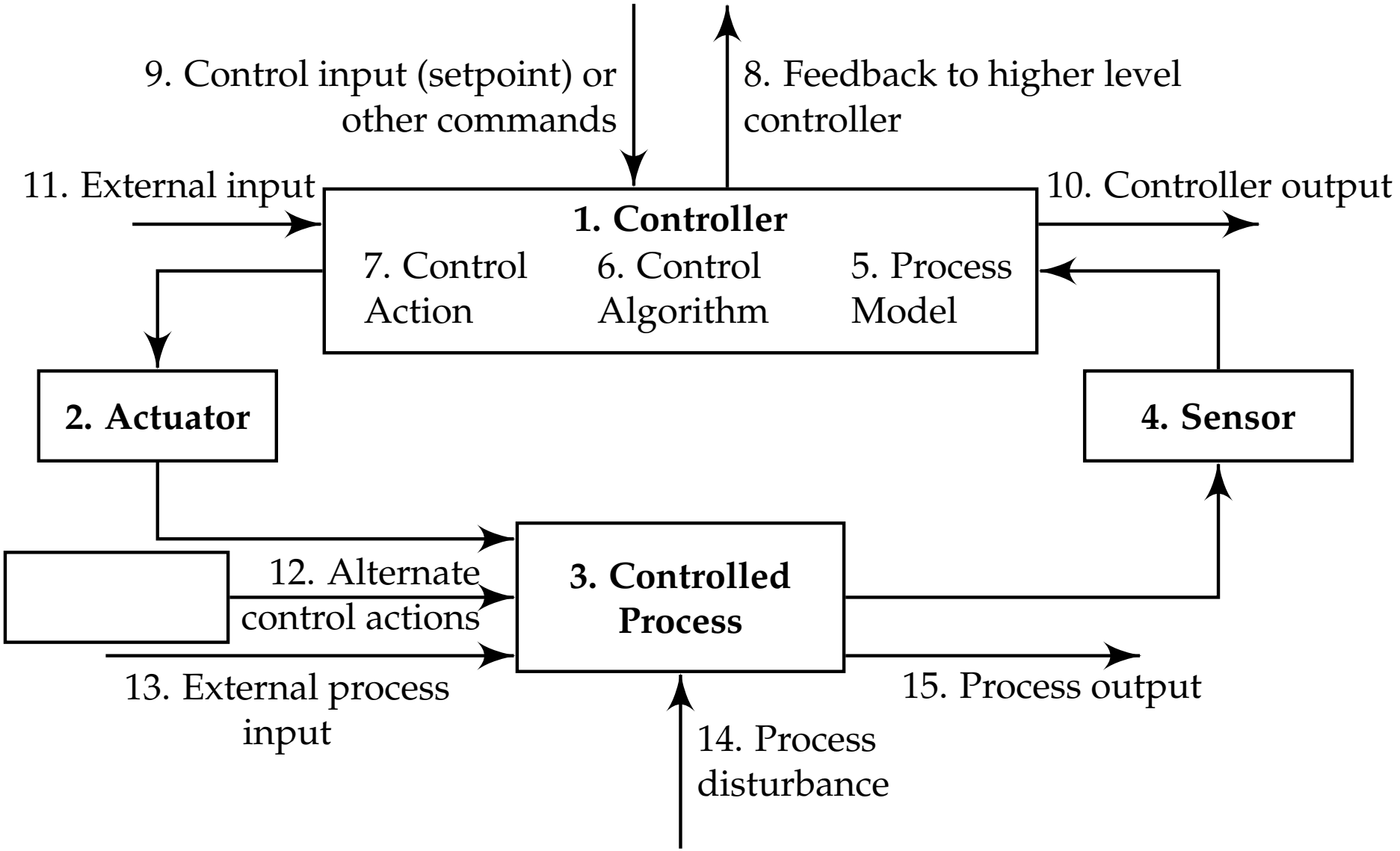
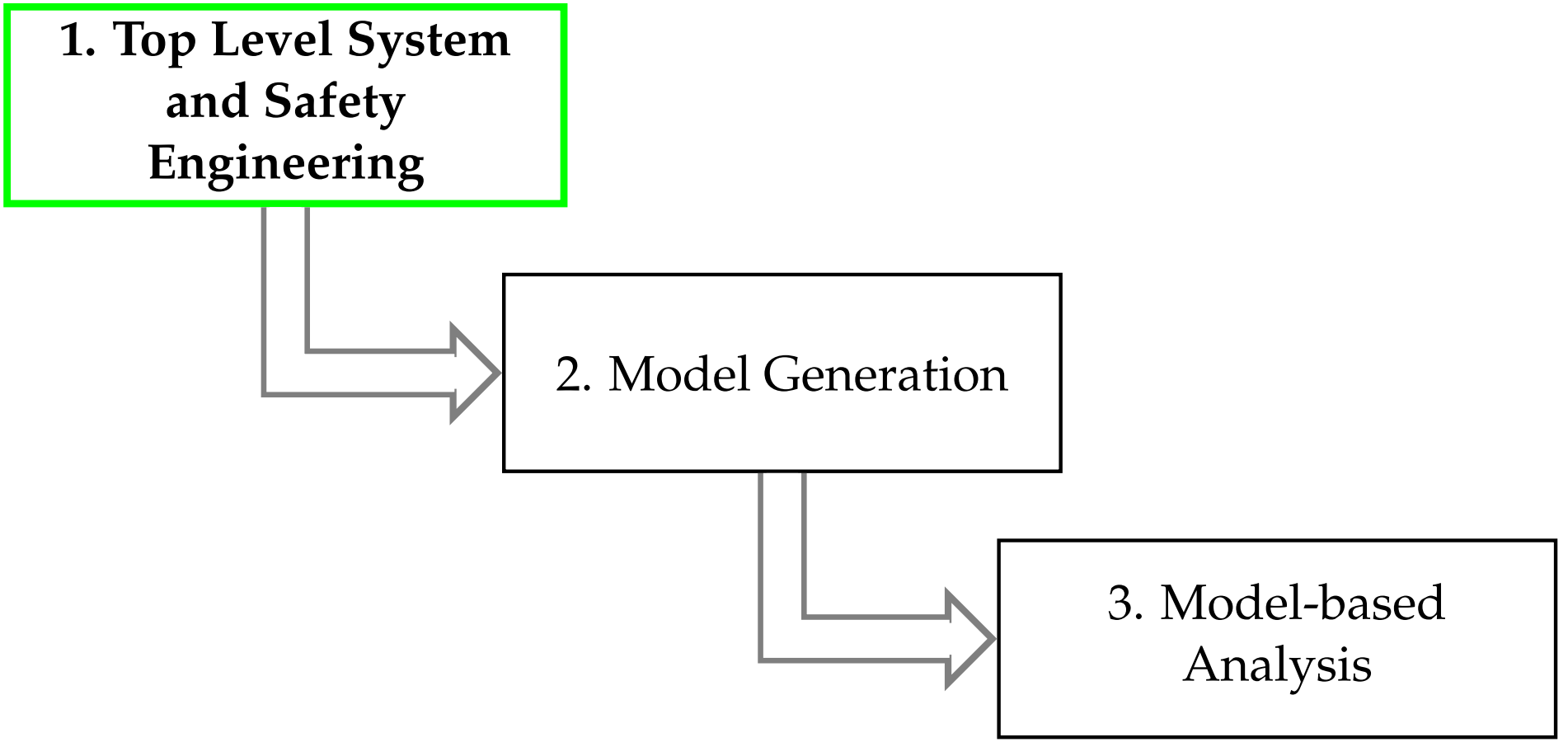
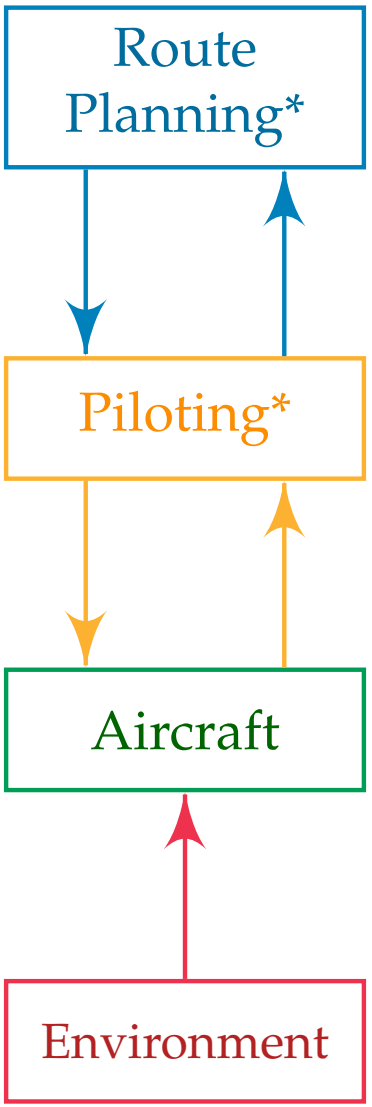


Table of Contents

High Level Control Structure



High Level Control Structure



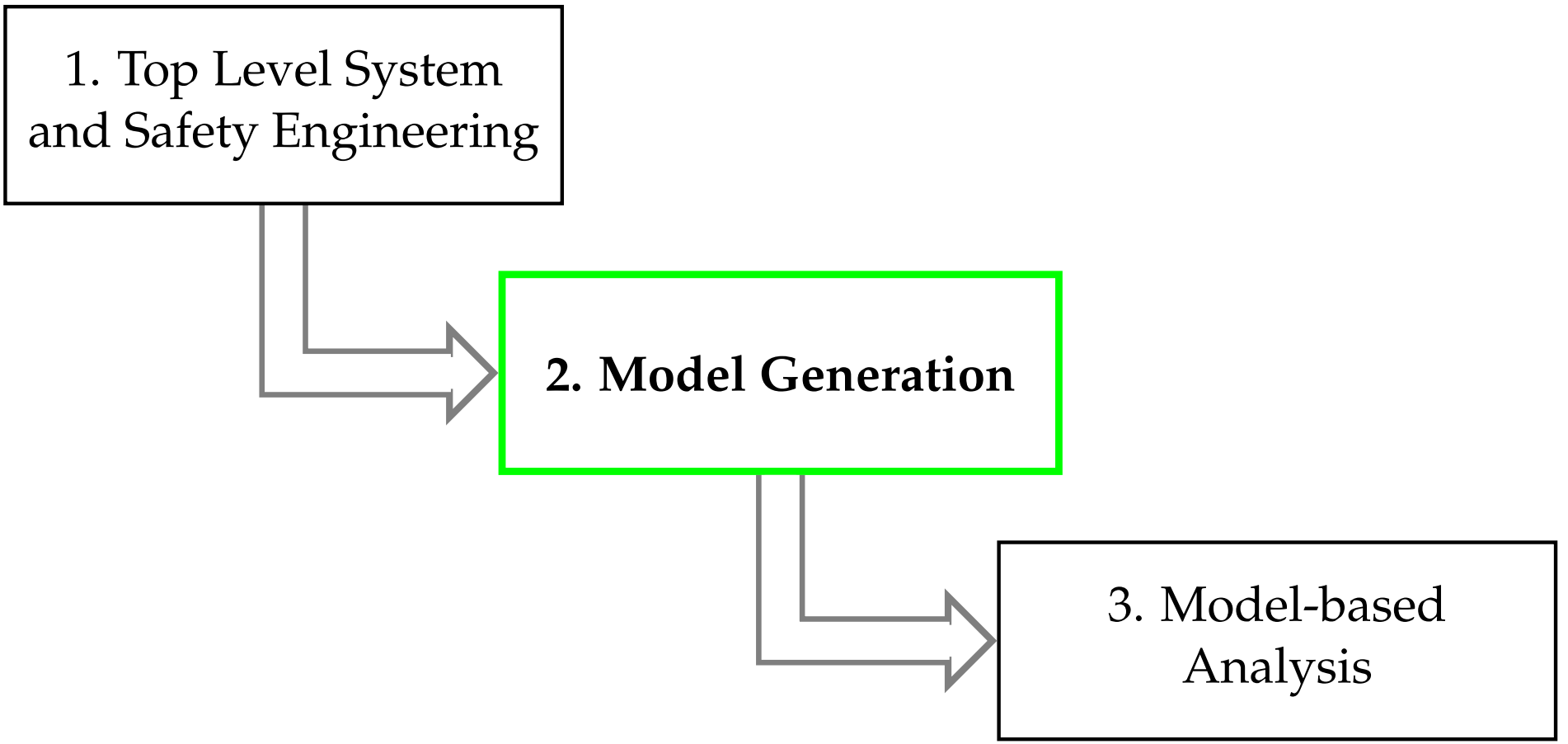
Safety-Related Responsibilities

- Provide conflict-free clearances & trajectories
- Sequence 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

Example - Conformance



Example - Conformance

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]

Example - Conformance

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]

Source	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 an intelligent sensor. That is, its role is a sensor but it has its own algorithms

Example - Conformance

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]

Source	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 an intelligent sensor. That is, its role is a sensor but it has its own algorithms

Controller
Control Action
Actuator
Cntl'd Process
Sensor
Process Model
Cntl Algorithm
...

Example - Conformance

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]

Controller	Piloting function
Control Action	
Actuator	
Cntl'd Process	Aircraft
Sensor	Altimeter, FMS, Aircraft conformance monitor
Process Model	Intended lat, long, alt, time; Actual lat, long, alt, time
Cntl Algorithm	
External Input	
Process Input	
Alt Controller	
Proc Disturbance	

Example - Conformance

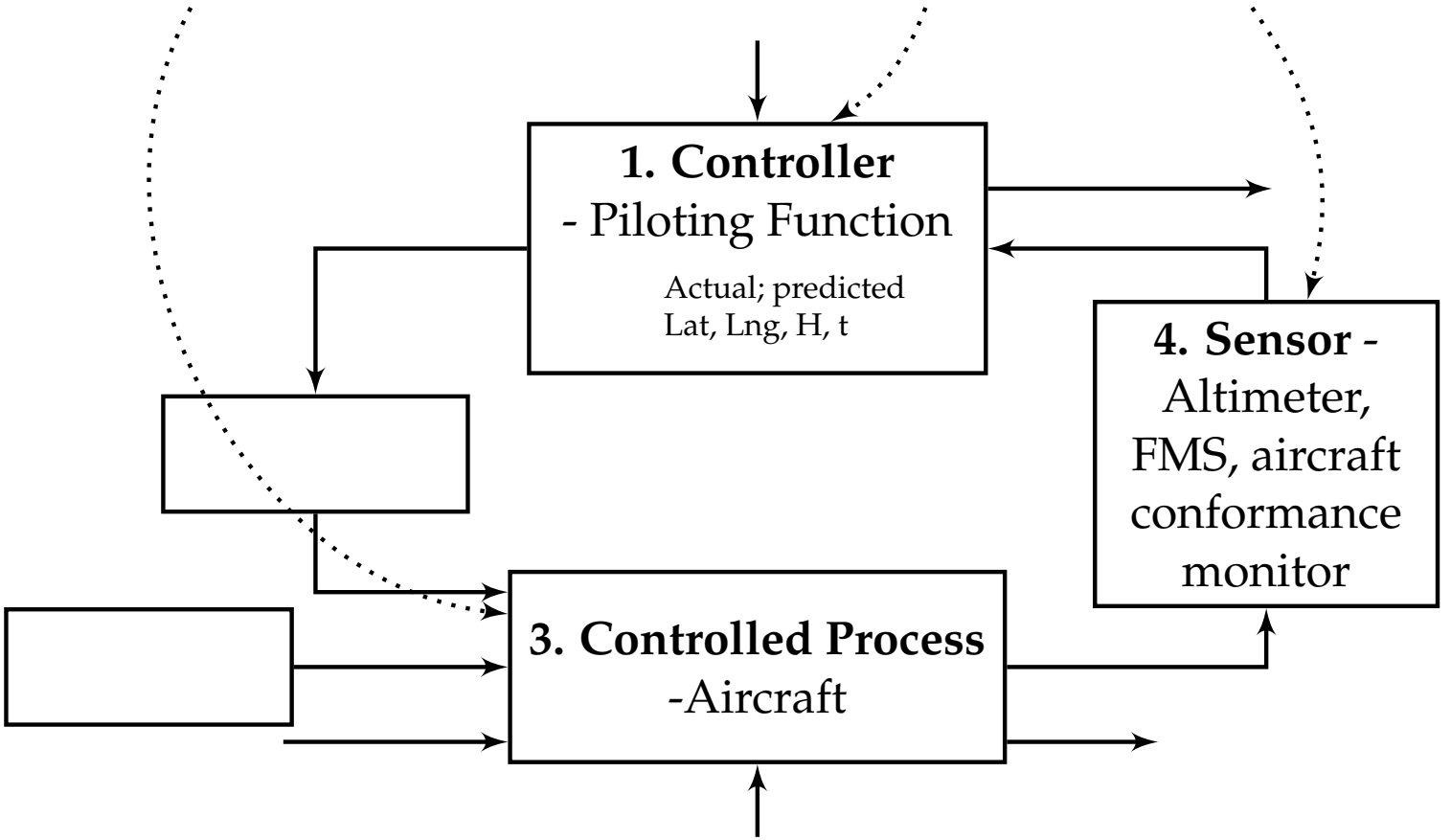
TBO conformance is monitored both in the aircraft and on the ground against the agreed-upon 4DT. In the air, this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other "time to go" aids. [JPDO, 2011]

Controller	Piloting function
Control Action	
Actuator	
Cntl'd Process	Aircraft
Sensor	Altimeter, FMS, Aircraft conformance monitor
Process Model	Intended lat, long, alt, time; Actual lat, long, alt, time
Cntl Algorithm	
External Input	
Process Input	
Alt Controller	
Proc Disturbance	

Control Model

Example - Conformance

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]



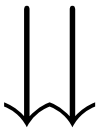
Example - Conformance

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]

Example - Conformance

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]

Source	Ground automation
Role	
Behavior Type	
Context	This is an intelligent sensor. That is, its role is a sensor but it has its own algorithms
Related UCAs	



Controller	
Control Action	
Actuator	
Cntl'd Process	Piloting function and aircraft
Sensor	
Process Model	
Cntl Algorithm	
External Input	
Process Input	
Alt Controller	
Proc Disturbance	

Example - Conformance

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]

Example - Conformance

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]

Source	Ground automation
Role	
Behavior Type	
Context	This is an intelligent sensor. That is, its role is a sensor but it has its own algorithms

Controller	
Control Action	
Actuator	
Cntl'd Process	Piloting function and aircraft
Sensor	
Process Model	
Cntl Algorithm	
External Input	
Process Input	
Alt Controller	
Proc Disturbance	

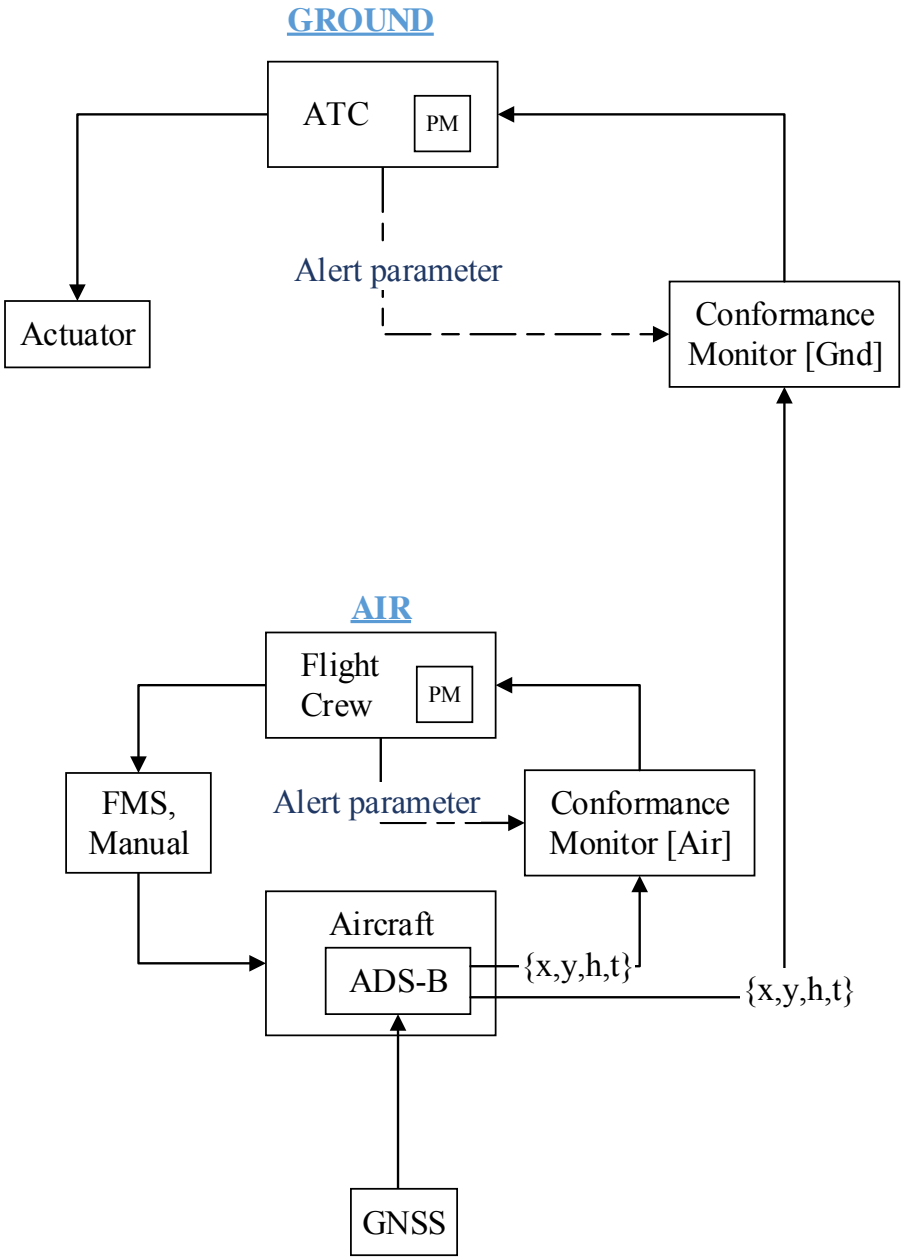
Example - Conformance

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]

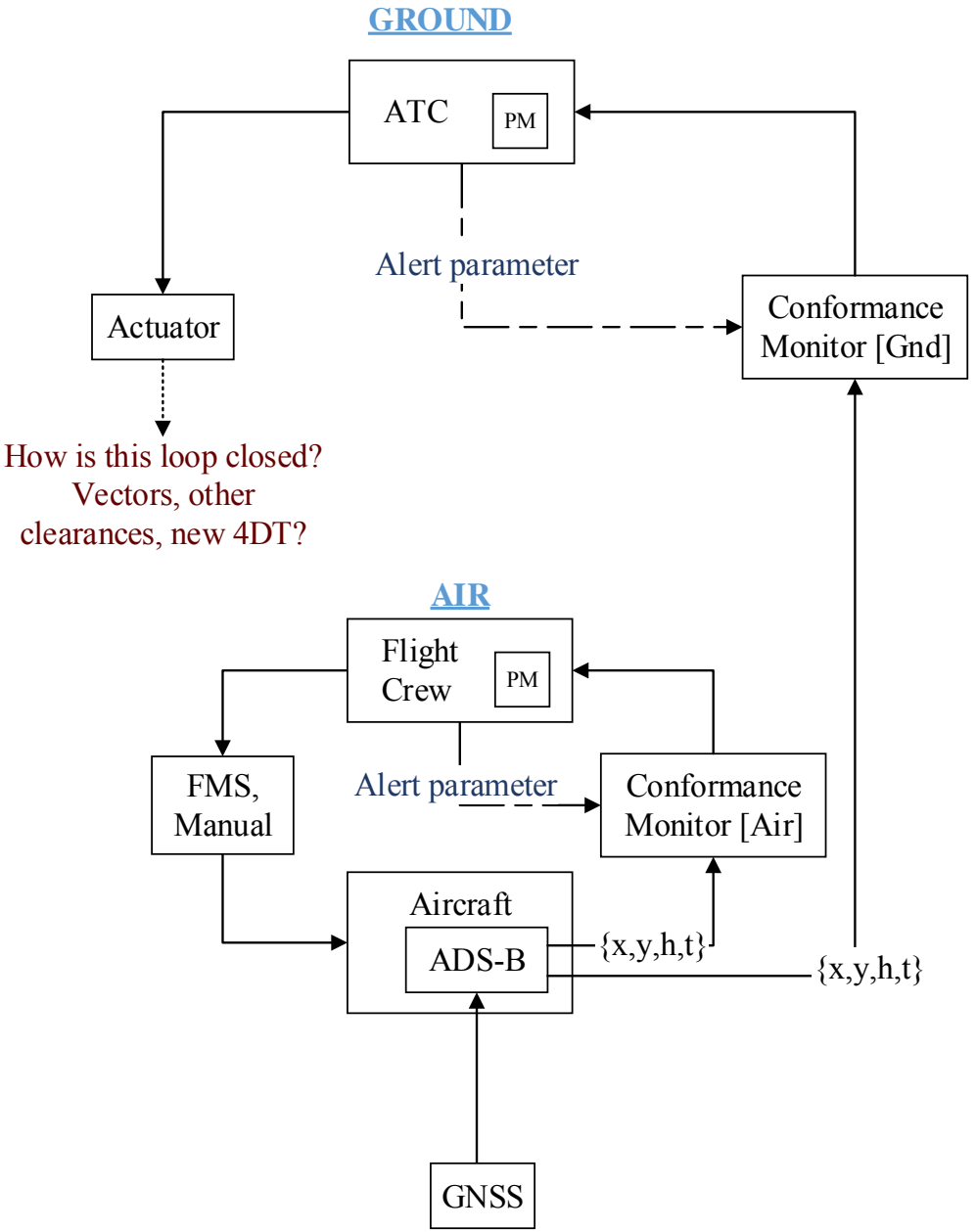
Source	Ground automation
Role	Sensor
Behavior Type	Sythesizes and integrates measurement data
Context	This is an intelligent sensor. That is, its role is a sensor but it has its own algorithms

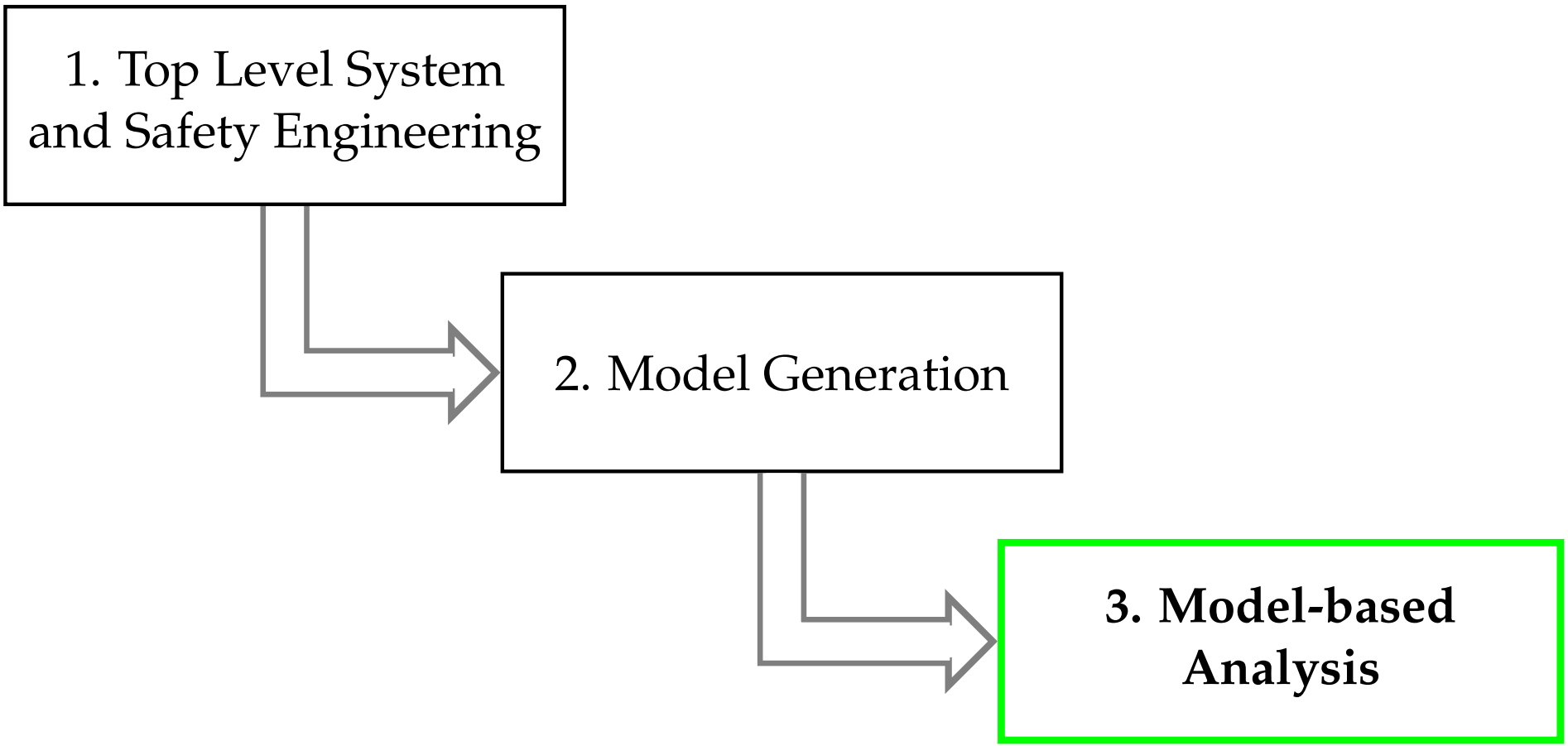
Controller	
Control Action	
Actuator	
Cntl'd Process	Piloting function and aircraft
Sensor	ADS-B, altitude reporting, "tools"
Process Model	All Intended lat, long, alt, time; All Actual lat, long, alt, time; traffic density; operation type; performance requirement
Cntl Algorithm	
External Input	Datalink - trajectory intent information
Process Input	
Alt Controller	
Proc Disturbance	

Resulting Model



Resulting Model




1. Top Level System and Safety Engineering
2. Model Generation
3. Model-based Analysis

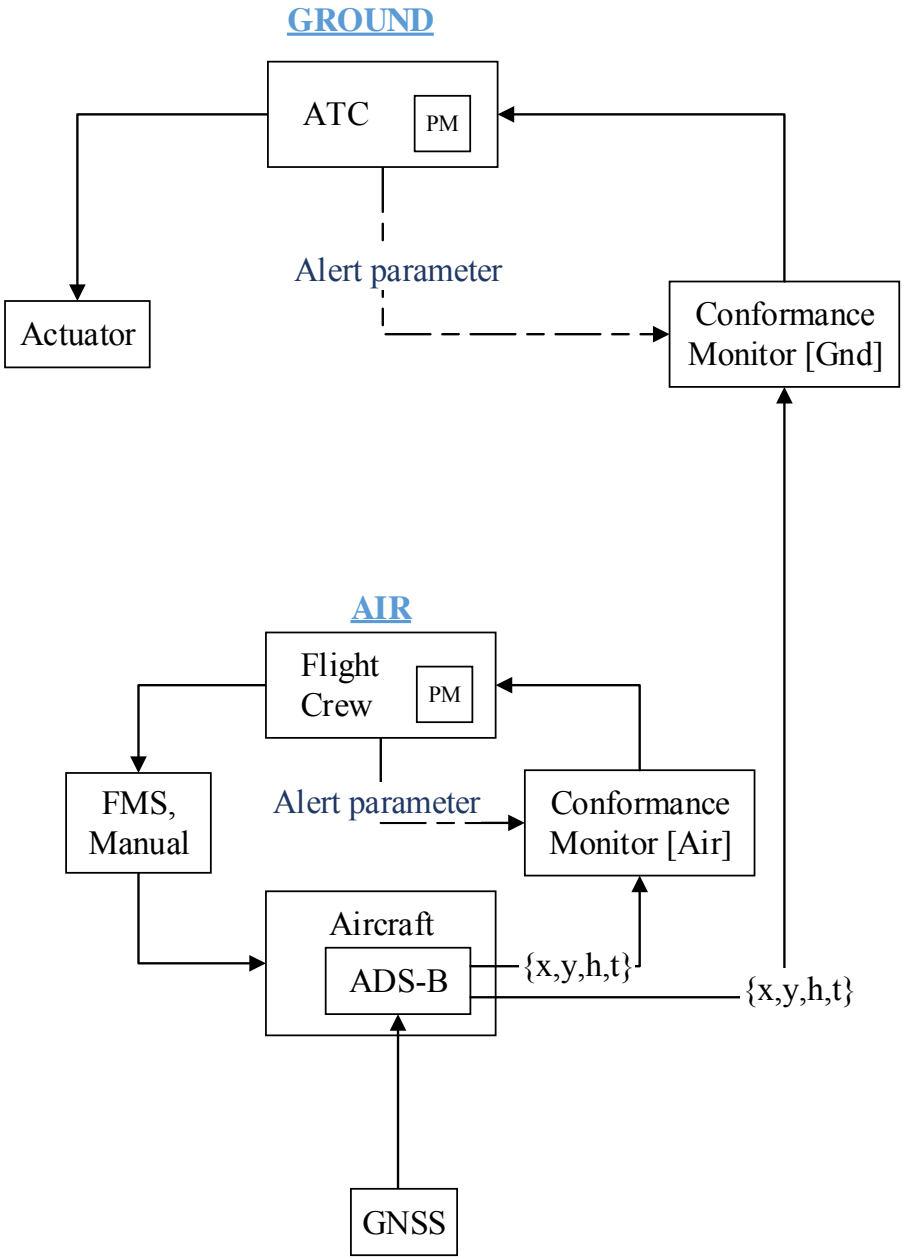
1. Are the control loops complete? That is, does each control loop satisfy:
   1.a. Goal Condition
   1.b. Action Condition
   1.c. Model Condition
   1.d. Observability Condition

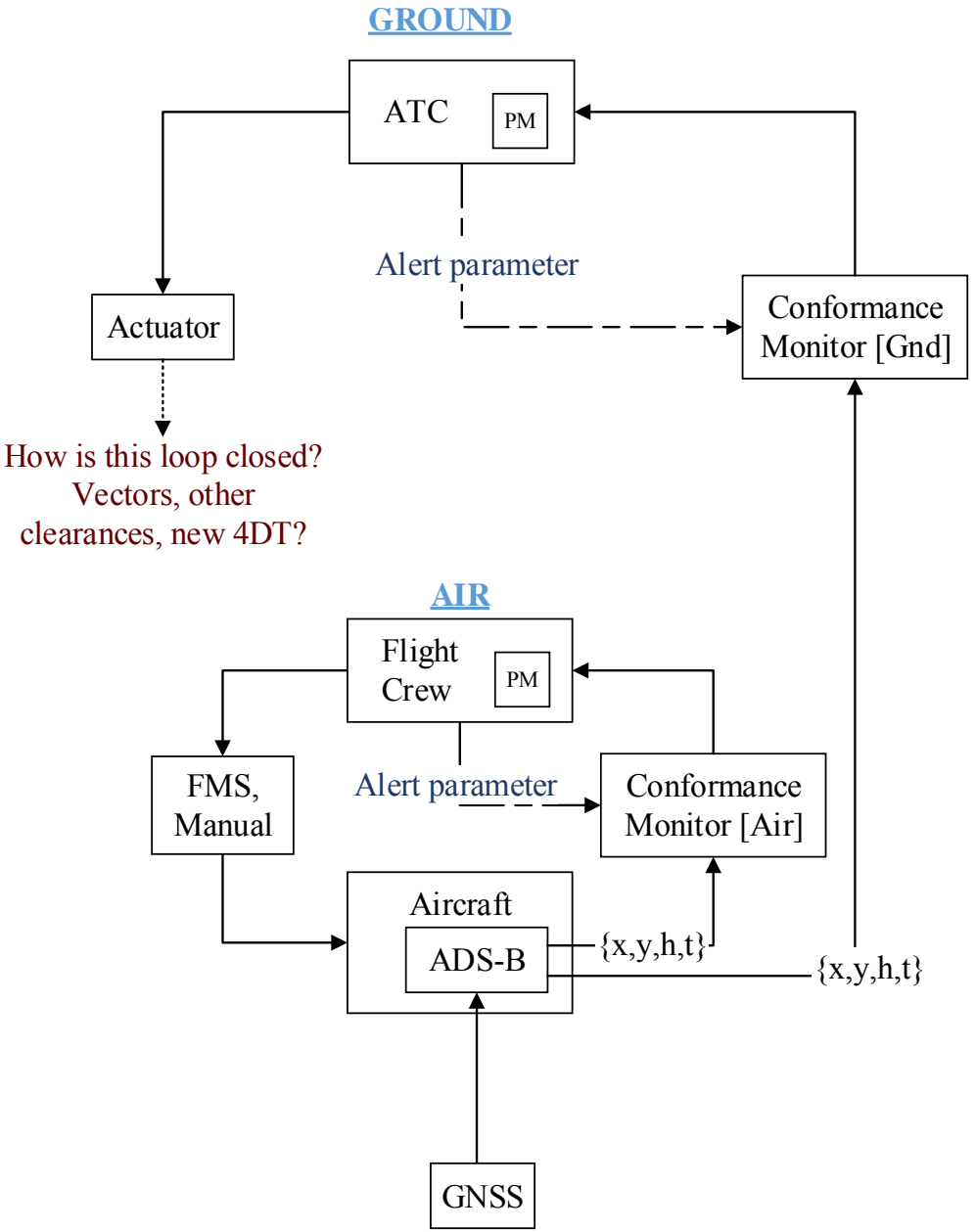
2. Safety-related responsiblities
   2.a. Are the system-level safety responsibilities accounted for?
   2.b. Do control agent responsibilities conflict with safety responsibilities?

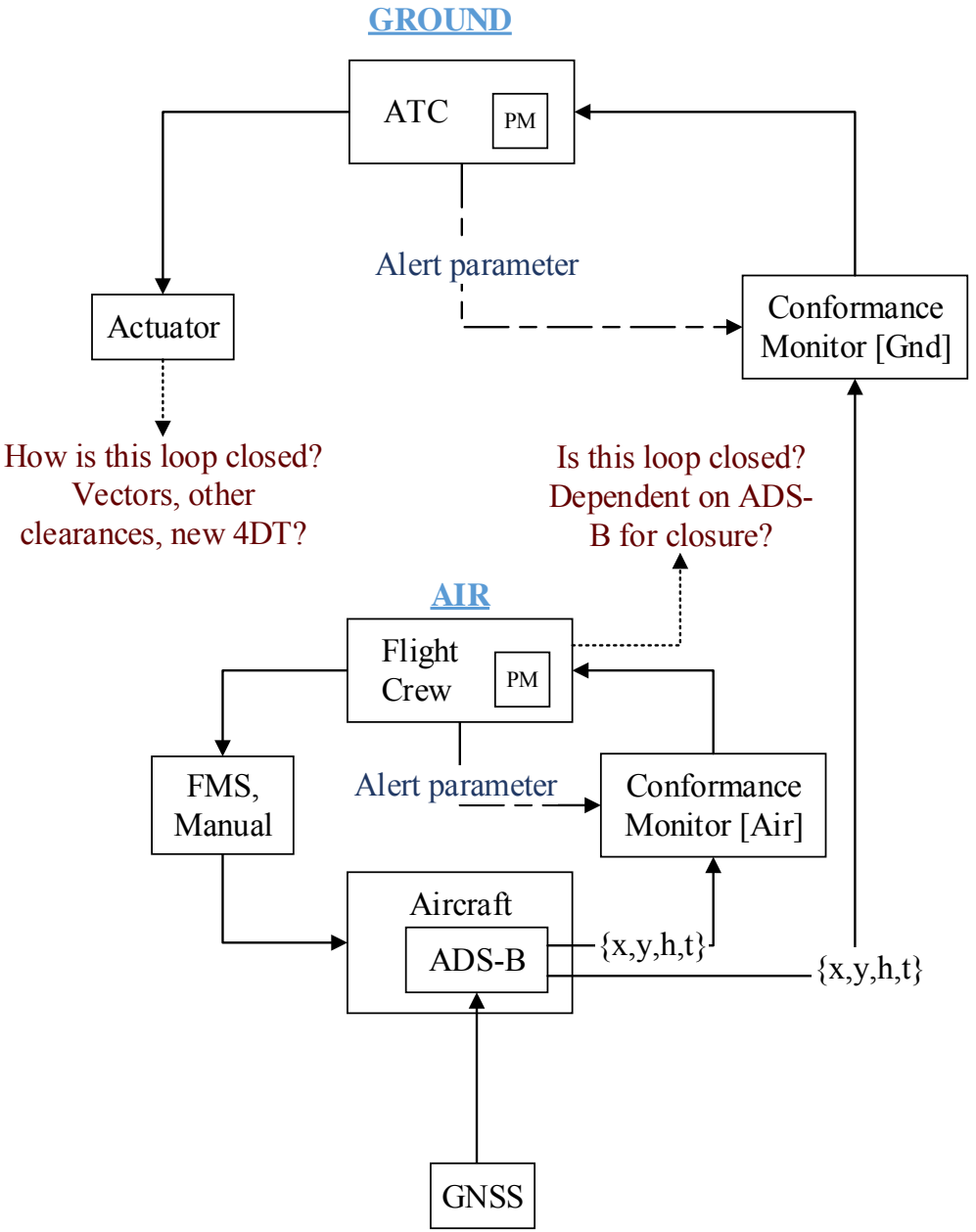
Analysis (2)

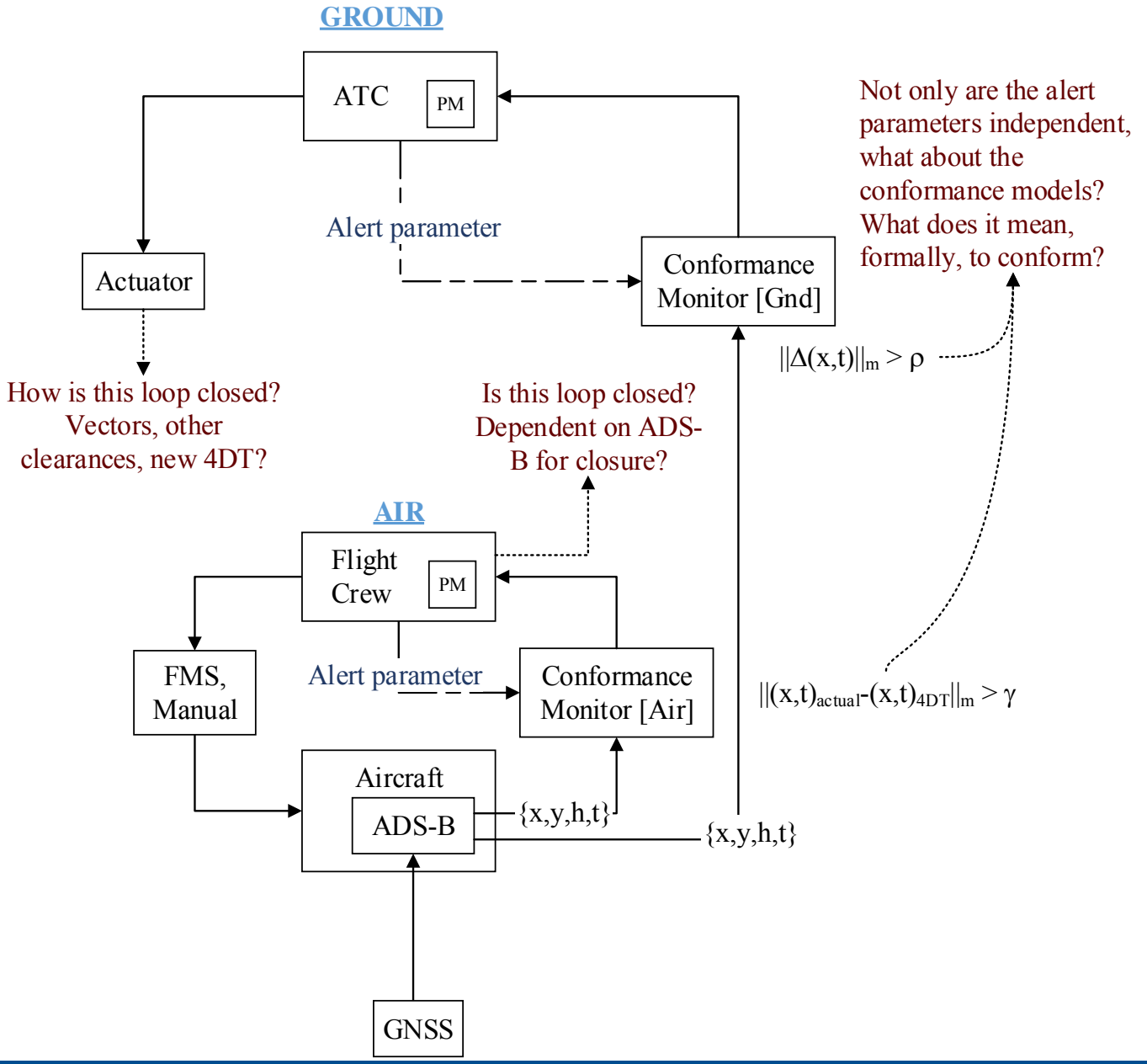
3. Multiple control agents
   - 3.a. Do multiple control agents have the same safety responsibility(ies)?
   - 3.b. Do multiple control agents have or require process model(s) of the same process(es)?

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


GROUND
ATC
PM
Alert parameter
Actuator
Conformance Monitor [Gnd]
AIR
Flight Crew
PM
FMS, Manual
Alert parameter
Conformance Monitor [Air]
Aircraft
ADS-B
{x,y,h,t}
{x,y,h,t}
GNSS


GROUND
ATC
PM
Alert parameter
Actuator
Conformance Monitor [Gnd]
How is this loop closed? Vectors, other clearances, new 4DT?
AIR
Flight Crew
PM
FMS, Manual
Alert parameter
Conformance Monitor [Air]
Aircraft
ADS-B
{x,y,h,t}
{x,y,h,t}
GNSS


GROUND
ATC
PM
Alert parameter
Actuator
Conformance Monitor [Gnd]
How is this loop closed? Vectors, other clearances, new 4DT?
Is this loop closed? Dependent on ADS-B for closure?
AIR
Flight Crew
PM
FMS, Manual
Alert parameter
Conformance Monitor [Air]
Aircraft
ADS-B
{x,y,h,t}
{x,y,h,t}
GNSS


GROUND
ATC
PM
Alert parameter
Actuator
Conformance Monitor [Gnd]
How is this loop closed? Vectors, other clearances, new 4DT?
Is this loop closed? Dependent on ADS-B for closure?
Not only are the alert parameters independent, what about the conformance models? What does it mean, formally, to conform?
$||\Delta(x,t)||_m > \rho$
AIR
Flight Crew
PM
FMS, Manual
Alert parameter
Conformance Monitor [Air]
$||(x,t)_{actual}-(x,t)_{4DT}||_m > \gamma$
Aircraft
ADS-B
{x,y,h,t}
{x,y,h,t}
GNSS

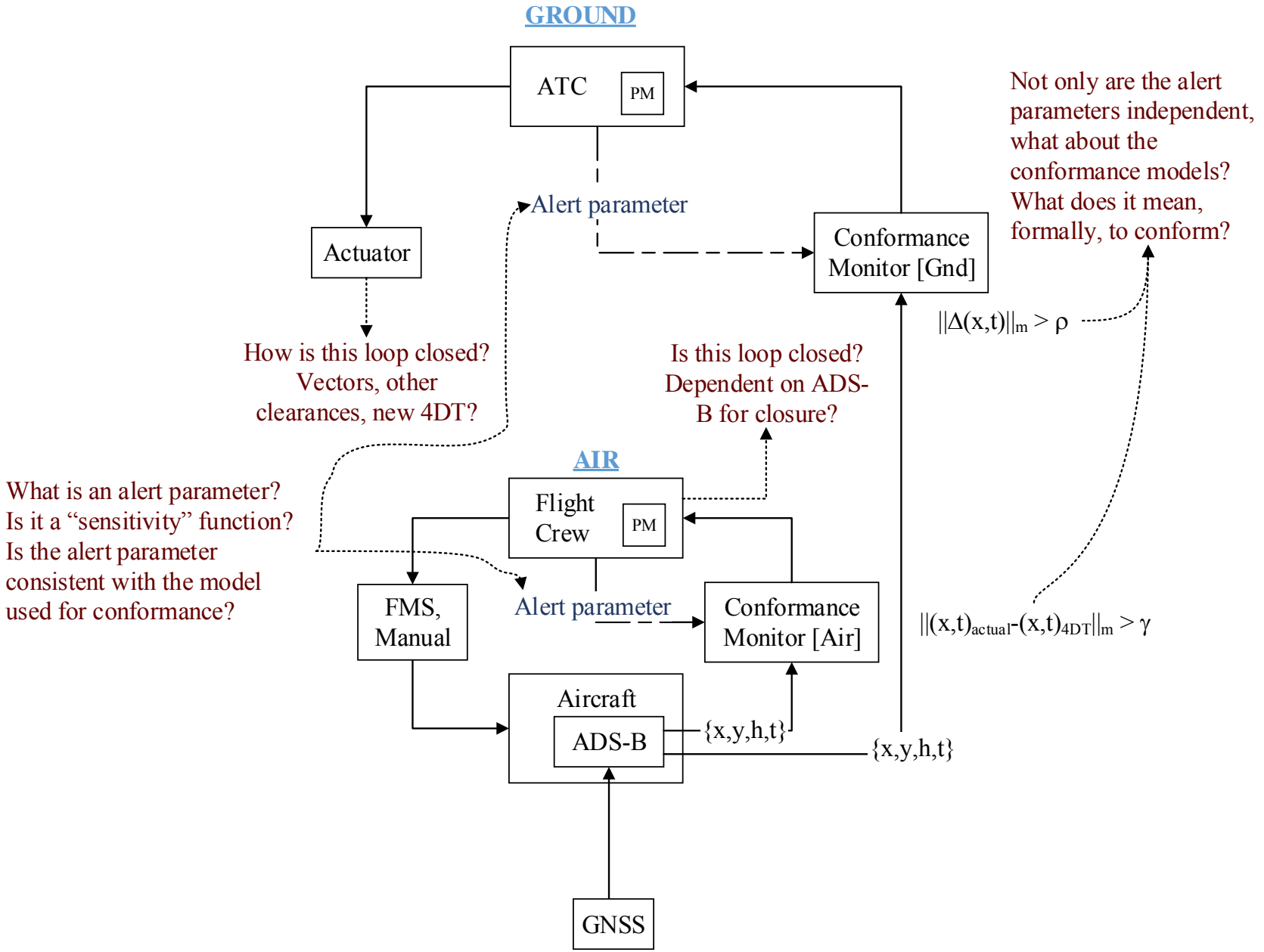
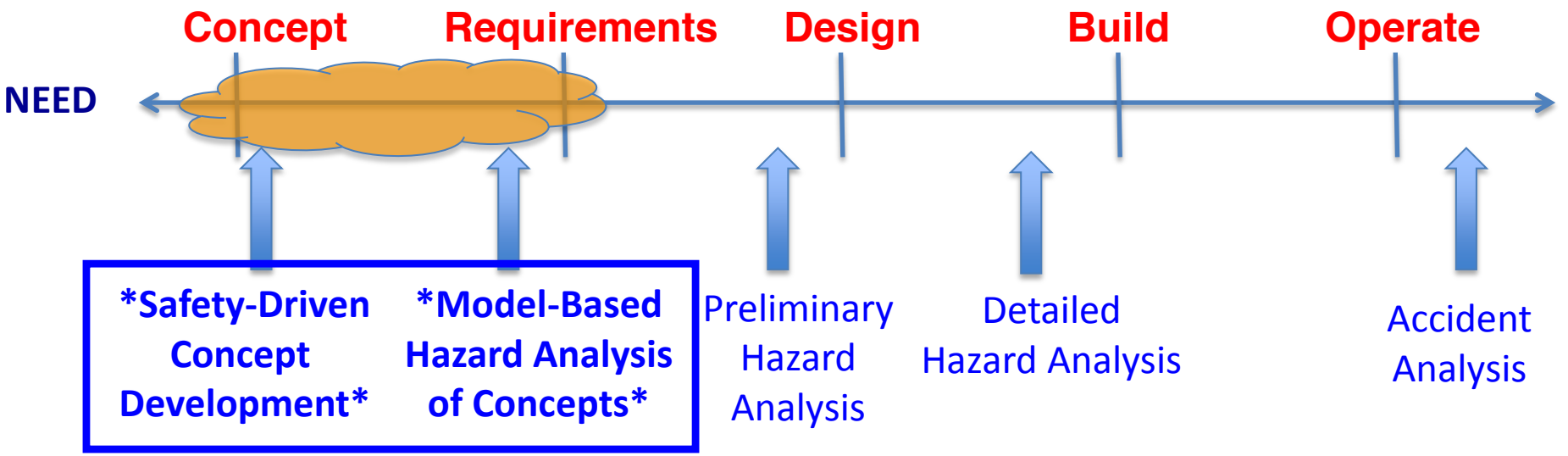

GROUND
ATC
PM
Alert parameter
Actuator
Conformance Monitor [Gnd]
Not only are the alert parameters independent, what about the conformance models? What does it mean, formally, to conform?
$||\Delta(x,t)||_m > \rho$
How is this loop closed? Vectors, other clearances, new 4DT?
Is this loop closed? Dependent on ADS-B for closure?
AIR
What is an alert parameter? Is it a "sensitivity" function? Is the alert parameter consistent with the model used for conformance?
Flight Crew
PM
FMS, Manual
Alert parameter
Conformance Monitor [Air]
$||(x,t)_{actual}-(x,t)_{4DT}||_m > \gamma$
Aircraft
ADS-B
{x,y,h,t}
{x,y,h,t}
GNSS

Table of Contents

System Engineering Phases



Safety Approaches

Applications

1. Identify potential design or architectural solutions for 1-3 (slide 5);
2. Identify the vulnerabilities, risks, and tradeoffs of 1-3 and architectures;
3. From Model $\rightarrow$ ConOps (or other type of document);
4. Accident investigation (or, analyzing accident investigations)

Conclusions

- Created systematic method for "building" a control structure from natural language text
- Identified missing, conflicting, and inconsistent issues in real-world ConOps
- Found hazards and causal factors that a professional working group did not
  [Or, identified their undocumented, implicit assumptions]
- Rigorous formulation/method to generate control structures and concepts

References

W Ross Ashby. An Introduction to Cybernetics. Chapman & Hall Ltd., 1957.

SE INCOSE. Incose systems engineering handbook v. 3.2. 2. Technical report, INCOSE-TP-2003-002-03.2. 2. October, 2011.

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

Nancy G. Leveson. Engineering a Safer World. MIT Press, 2012.

Mihajlo D Mesarovic. Multilevel systems and concepts in process control. Proceedings of the IEEE, 58(1):111–125, 1970. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1449475.

Ralph F Miles Jr. Systems concepts: Lectures on contemporary approaches to systems. 1973.

William I Stieglitz. Engineering for safety. Aeronautical Engineering Review, 7(2):18–23, 1948.