STAMP/STPA Seminar

Dong-Ah Lee

Konkuk University

2013-04-25

Contents

- Introduction to STAMP
- Introduction to STPA
- Simple STPA Exercise

INTRODUCTION TO STAMP

Background

- A new approach to building safer systems
  - The traditional approaches do not work well for current systems.

- Why?
  - Fast pace of technological change
  - Reduced ability to learn from experience
  - Changing Nature of Accidents
  - New types of hazards
  - Increasing complexity and coupling
  - Decreasing tolerance for single accidents
  - Difficulty in selecting priorities and making tradeoffs
  - More complex relationships between humans and automation
  - Changing regulatory and public views of safety

Systems Theory (1)

- Foundation of systems theory
  - Emergence and Hierarchy
  - Communication and Control

Systems Theory (2)

- Emergence
  - Irreducible properties at a given level
  - Emergent properties: meaningless at lower levels
- Hierarchy
  - Relationships between different levels
    - what generates levels, what separates them, and what links them
  - Emergent properties at one level
    - constraints upon the degree of freedom of components

Systems Theory (3)

- Control
  - Laws of behavior at a level
  - Control imposes (safety) constraints
  - Avoiding failures → Imposing constraints on system behavior
- Communication
  - Open systems: Interrelated components
  - Control in open system: communication between components
- Four conditions to control a process
  - Goal condition, Action condition, Model condition, and Observability condition

STAMP: Intro

- An accident
  - An unplanned and undesired loss event

- Causes of losses
  - Component failures
  - Disturbances external to the systems
  - Interactions among system components
  - Behavior of individual system components

- Example of hazards
  - The release of toxic chemicals from an oil refinery
  - A patient receiving a lethal does of medicine
  - Two aircraft violating minimum separation requirements

STAMP: Intro

- Emergent properties (safety)
  - Arising from the interactions among the system components
  - Being controlled by imposing constraints on the behavior of and interactions among the components
- Safety = A control problem
  - The goal of the control: Enforcing the safety constraints
- Accidents
  - Inadequate control or enforcement of safety-related constraints
  - On the development, design, and operation of the system

STAMP: Safety Constraints

- Not a event, but a constraint
  - Events leading to losses only occur because safety constraints were not successfully enforced (controlled).
- Passive controls
  - Maintaining safety by their presence
    - EX) Shields or barriers, hardhats, fences, etc.
- Active controls
  - Detection, Measurement, Diagnosis, and Response

Must be completed before a loss occur
by a control system with a computer

STAMP: Safety Constraints

- The failure modes

  The active control system > The passive design

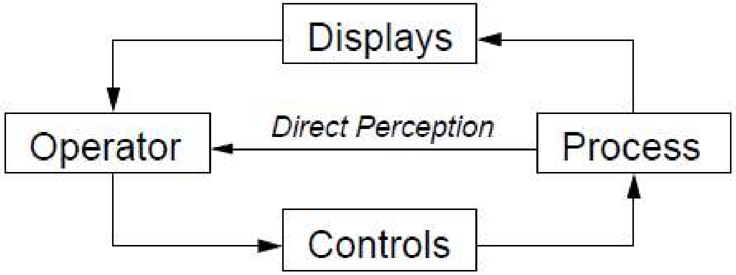
  - The complexity of the system component interactions

- The pros of using the active controls
  - Including increased functionality
  - More flexibility in design
  - Ability to operate over large distances
  - Weight reduction, and so on

- The cons of using the active controls
  - The difficulty of the engineering problems → Being increased and more potential for design errors

STAMP: Safety Constraints

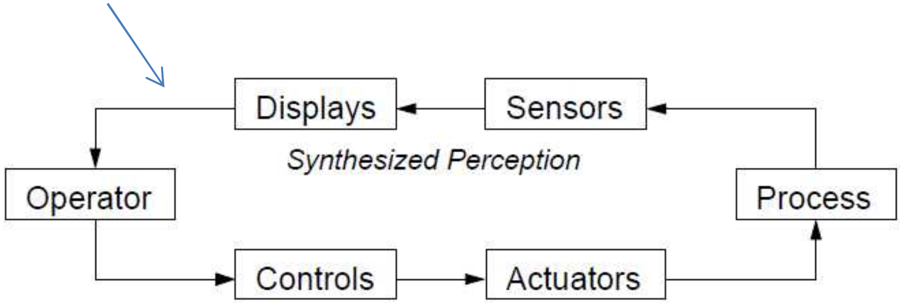
- Proximity allowed sensory perception of the status of the process via physical feedback
  - When controls were primarily mechanical
  - When controls were operated by people close to the operating process



STAMP: Safety Constraints

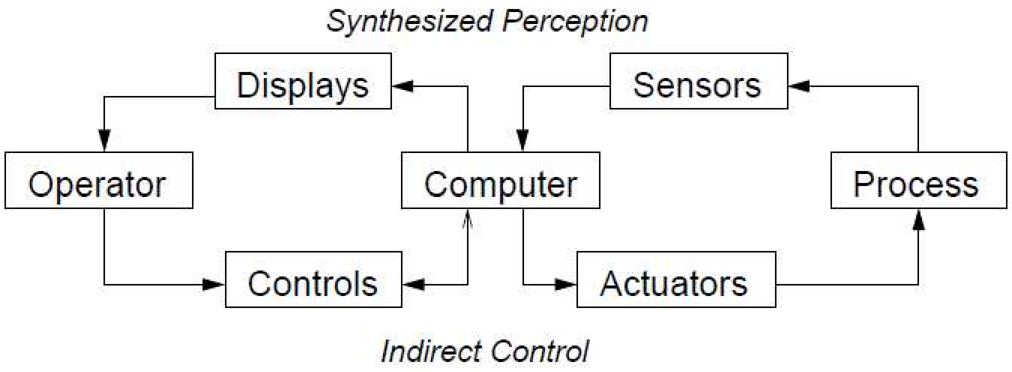
- Electromechanical controls
  - Allowing operators to control processes from a grater distance
  - Losing a lot of direct information

- The system designers
  - Synthesizing and providing an image of the process state to the operators
  - Providing feedback on the actions of the operators and any failures



STAMP: Safety Constraints

- Computer and digital controls
  - Affording additional advantages
  - Removing even more constraints
  - More possibility for error



STAMP: Safety Constraints

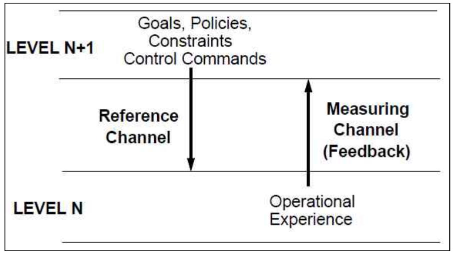
- The same argument
  - The increasing complexity in organizational and social controls
  - The increasing complexity in the interactions among the components of socio-technical systems

- A new holistic approach to safety
  - Controls and enforcing safety constraints in the entire socio-technical system
  - System-level constraints
  - Responsibility
  - Allocation

STAMP: The Hierarchical Safety Control Structure

- Hierarchical structures
  - Imposing constraints on the activity of the level beneath it
  - Control processes: Controlling the processes at lower levels in the hierarchy

- Inadequate control
  - Missing constraints
  - Inadequate safety control command
  - Commands that were not executed correctly at a lower level
  - Inadequately communicated or processed feedback about constraint enforcement



LEVEL N+1

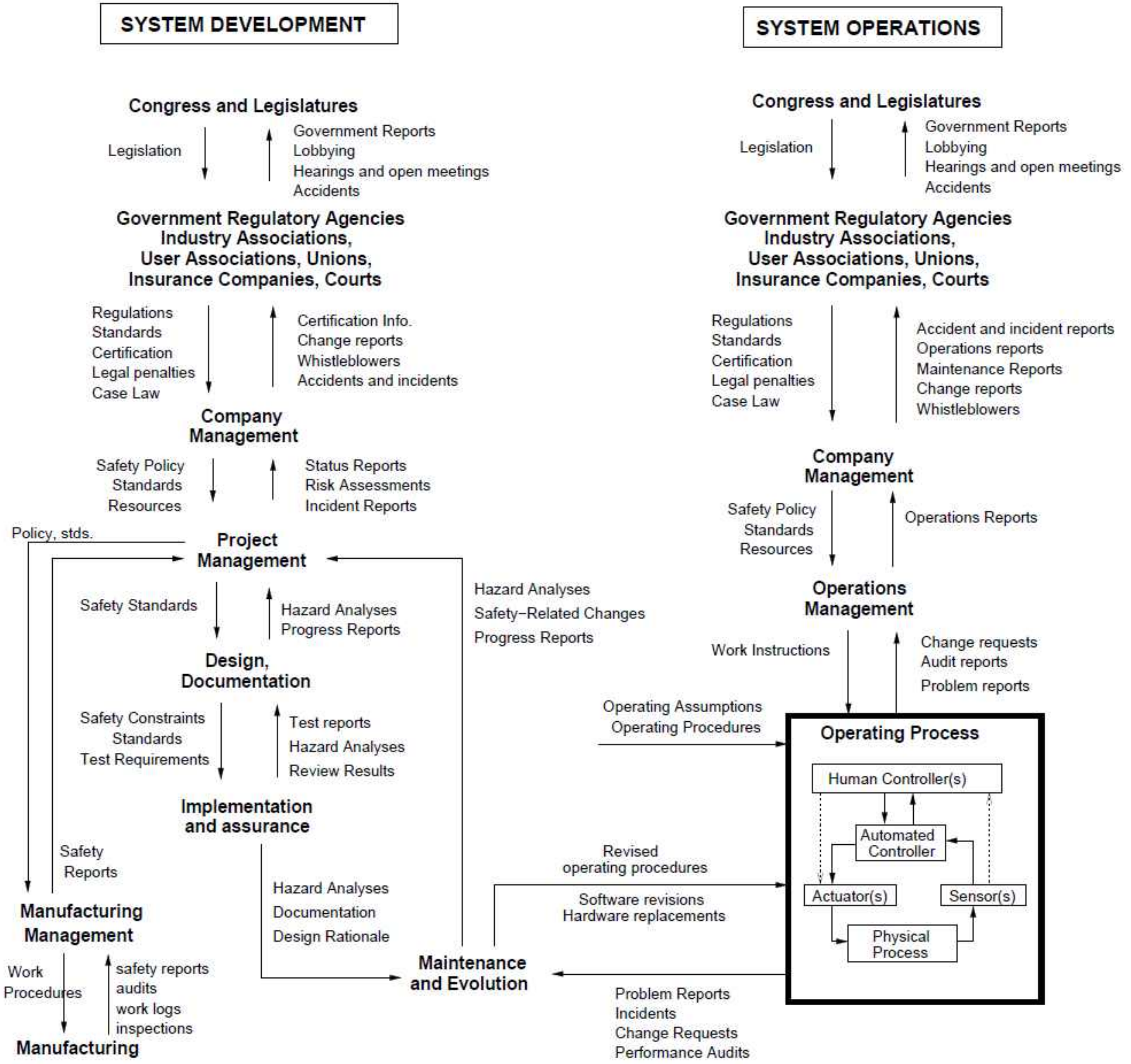
Goals, Policies,
Constraints
Control Commands

Reference
Channel

Measuring
Channel
(Feedback)

LEVEL N

Operational
Experience



SYSTEM DEVELOPMENT

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

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company
Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project
Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety-Related Changes
Progress Reports

Design,
Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation
and assurance

Safety
Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing
Management

Work
Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance
and Evolution

SYSTEM OPERATIONS

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

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

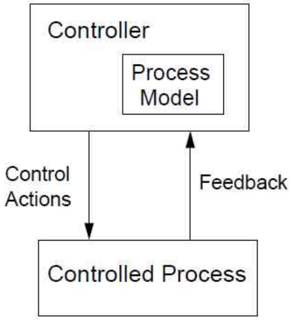
Revised
operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

STAMP: Process Models

- The four conditions to control a process
  - A goal: Safety constraints enforced by controllers
  - Action condition: The (downward) control channels
  - Observability condition: The (upward) feedback or measuring channels
  - Model condition: A model of the process begin controlled to control it effectively



STAMP: Process Models

- Three essential information of process model
  - The required relationship among the system variables
  - The current state
  - The ways the process can change state

- Component interaction accidents: incorrect process models
  - Incorrect or unsafe control commands are given.
  - Required control action (for safety) are not provided.
  - Potentially correct control commands are provided at the wrong time (too early or too late).
  - Control is stopped too soon.

STAMP

- Systems-Theoretic Accident Model and Process model of accident causation
  - Safety constraints
  - A hierarchical safety control structure
  - Process models

STAMP is now simply a matter of putting them together

STAMP

- System
  - Interrelated components kept in a state of dynamic equilibrium by feedback control loops
  - Dynamic processes that are continually adapting to achieve their ends and to react to change in themselves and their environment

- Safety
  - An emergent property of the system that is achieved when appropriate constraints on the behavior of the system and its components are satisfied

- Accidents
  - The result of flawed processes
    - Interactions among people, societal and organizational structures, engineering activities, and physical system components that lead to violating the system safety constraints

STAMP

- Consideration of more accident causes than simple component failures
- More sophisticated analysis of failures and component failure accidents

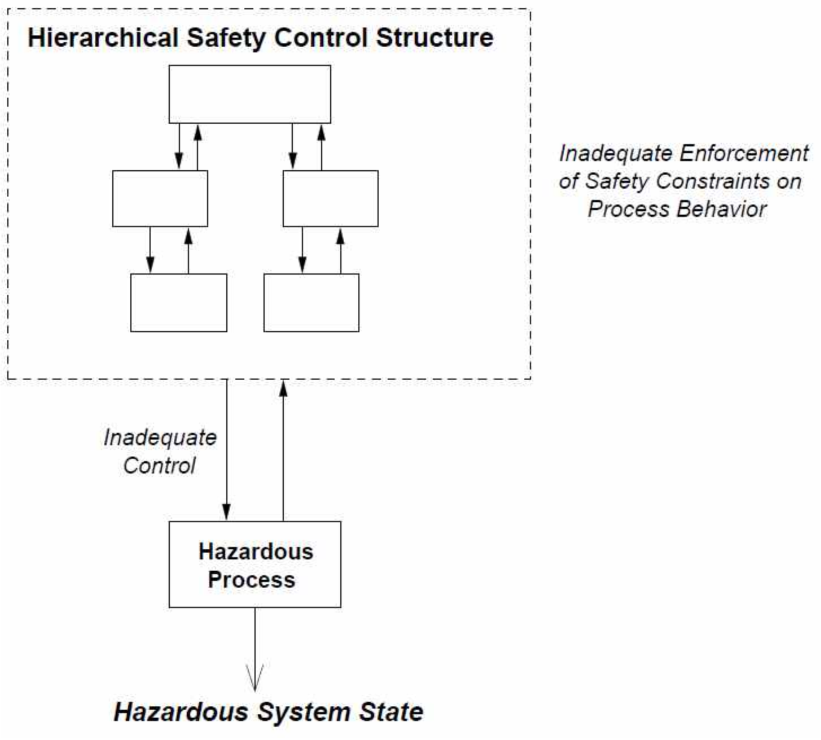
- Component failures
  - Inadequate engineering design such as missing or incorrectly implemented fault tolerance
  - Lack of correspondence between individual component capacity (including human capacity) and task requirements
  - Unhandled environmental disturbances
  - Inadequate maintenance
  - Physical degradation

STAMP

- Identification of the reasons
  - Why those failures occurred and led to and accident
  - Why the controls instituted for preventing such failures or for minimizing their impact on safety
- Other types of accident causes
  - Component interaction accident

STAMP

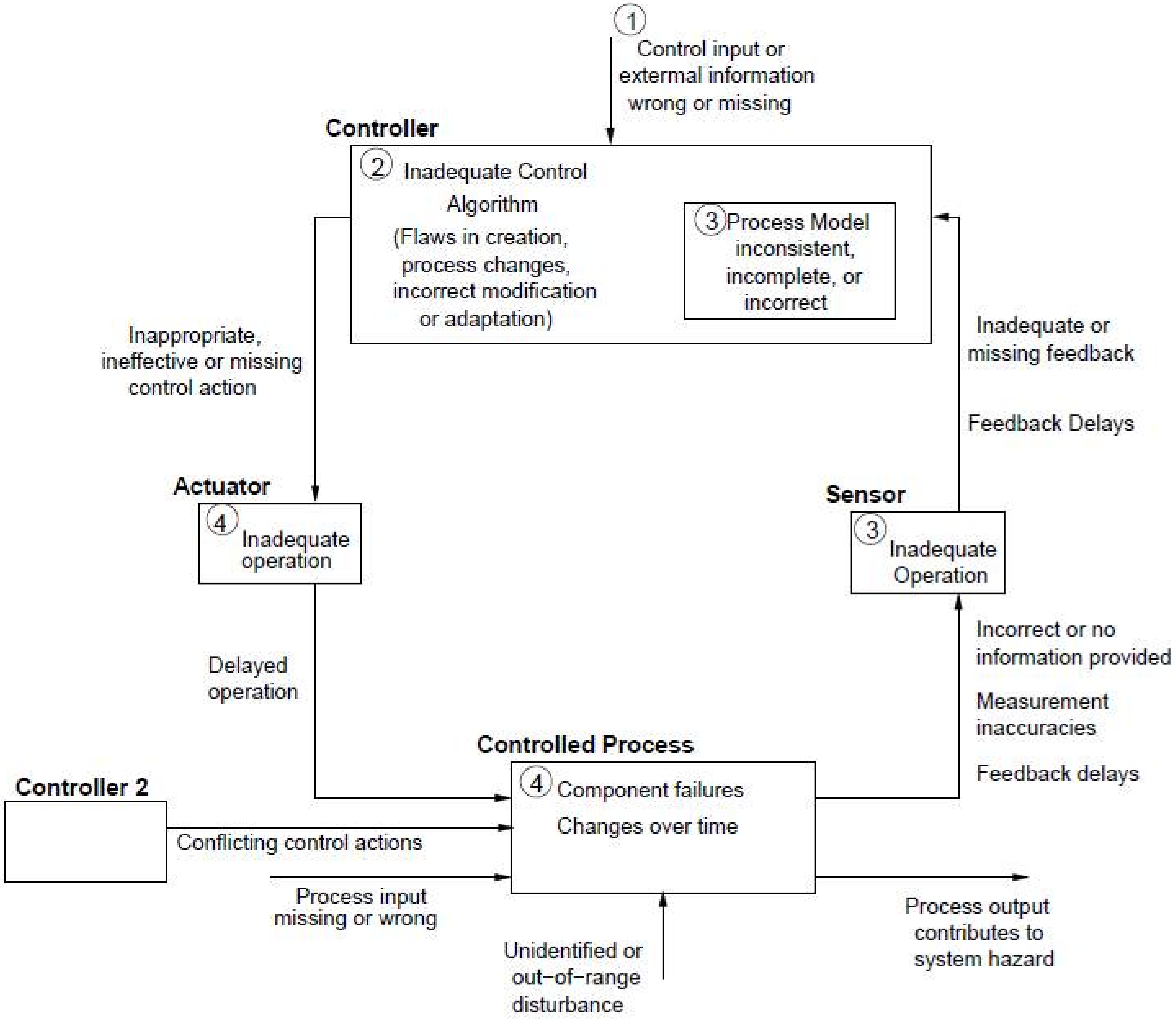
- Not a simple graphic representation of accident causality


Hierarchical Safety Control Structure
Inadequate Enforcement of Safety Constraints on Process Behavior
Inadequate Control
Hazardous Process
Hazardous System State

STAMP: A General Classification of Accident Causes

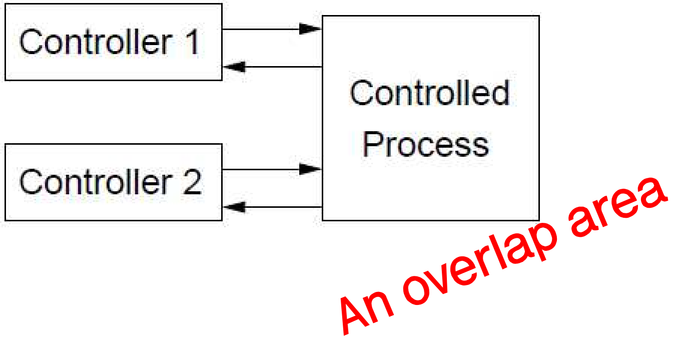
- An accident
  - The safety constraints were not enforced by the controller.
    - The control actions necessary to enforce the associated safety constraint at each level of the socio-technical control structure for the system were not provided.
    - The necessary control actions were provided but at the wrong time (too early or too late) or stopped too soon.
    - Unsafe control actions were provided that caused a violation of the safety constraints.
  - Appropriate control actions were provided but not followed

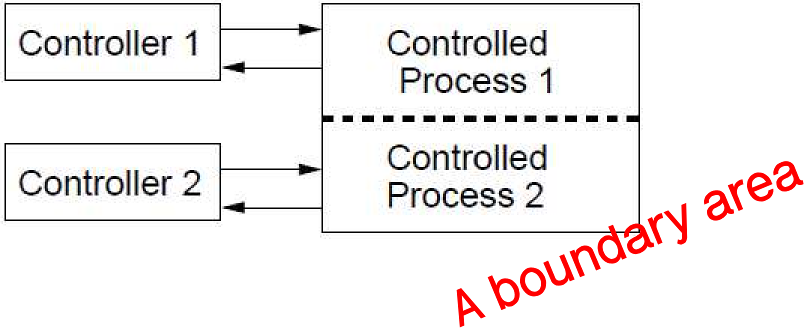
- The causal factors in accidents
  - The controller operation
  - The behavior of actuators and controlled processes
  - Communication and coordination among controllers and decision makers


1
Control input or external information wrong or missing
Controller
2
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
3
Process Model inconsistent, incomplete, or incorrect
Inappropriate, ineffective or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
4
Inadequate operation
Sensor
3
Inadequate Operation
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controlled Process
4
Component failures
Changes over time
Controller 2
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

STAMP: A General Classification of Accident Causes

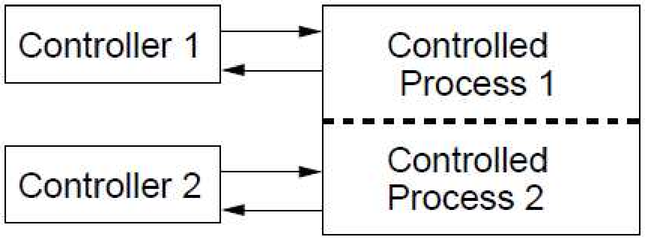
- Coordination and Communication Among Controllers and Decision Makers
  - Inadequately coordinated Multiple controllers (human and/or automated)
    - Unexpected side effects of decisions or action
    - Conflicting control action





STAMP: A General Classification of Accident Causes

- Coordination and Communication Among Controllers and Decision Makers

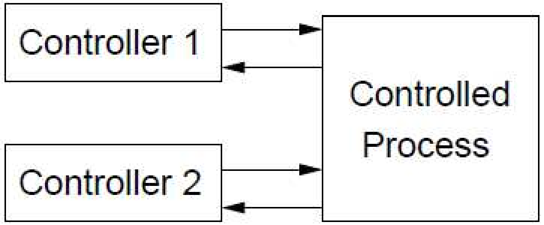


A boundary area

- Poorly defined boundary areas
- Coordination problems

STAMP: A General Classification of Accident Causes

- Coordination and Communication Among Controllers and Decision Makers



An overlap area

- A function by two controllers
- The same object influenced by two controllers

STAMP: A General Classification of Accident Causes

- Context and Environment
  - Human behavior by the context and environment in which the human is working
  - Behavior shaping mechanisms

STAMP: Applying the New Model

- Summary
  - STAMP: constraints in safety management.
  - Accident causal analysis: identifying the safety constraints.
  - The accident “cause”: an inadequate safety control structure
  - Accidents: dynamic processes

- STAMP
  - Helping us to separate factual data
  - Begin more complete than other models
  - Providing more help in understanding accidents
  - Begin useful in analyzing accidents and in developing new and potentially more effective system engineering methodologies to prevent accidents
  - Providing a direction to new hazard analysis and prevention techniques
  - Improving performance analysis
  - Pointing the way to very different approaches to risk assessment

INTRODUCTION TO STPA

STPA?

Older techniques

FTA, ETA, HAZOP, FMEA

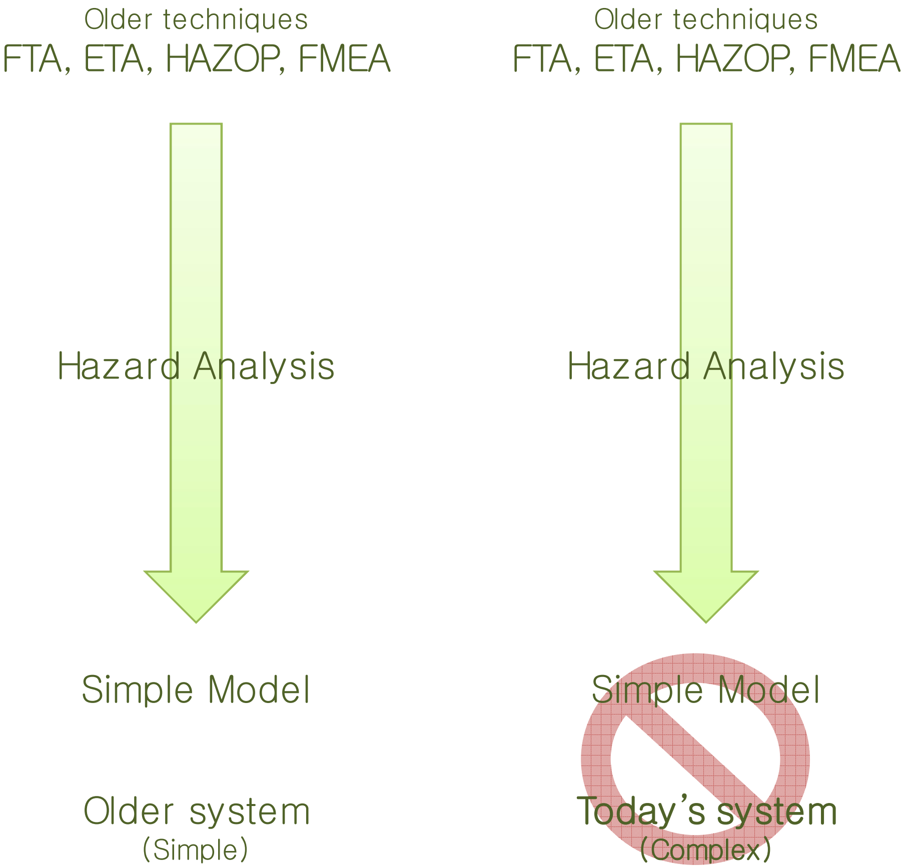
Hazard Analysis

Simple Model

Older system

(Simple)

STPA?



Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Older system
(Simple)

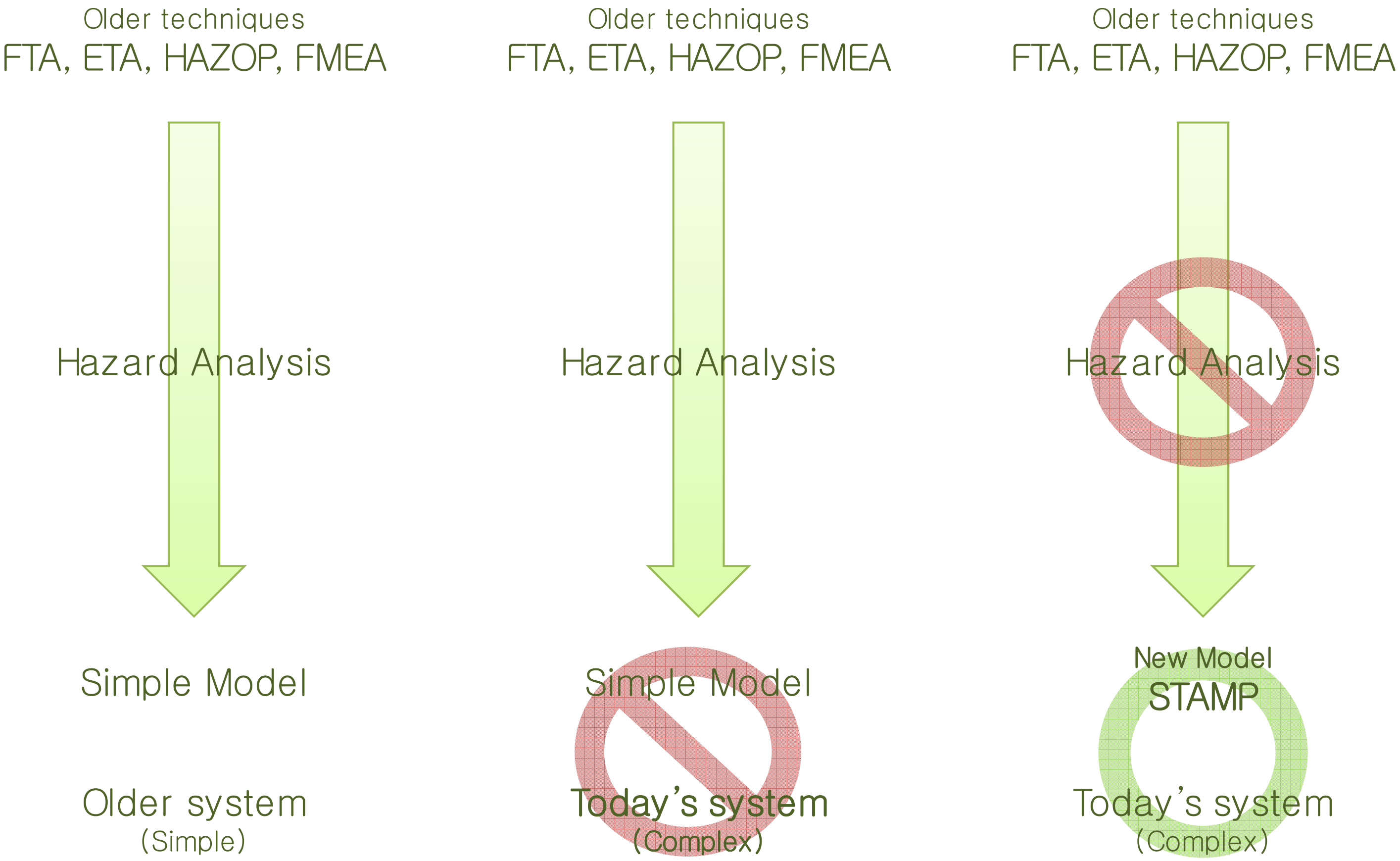
Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Today's system
(Complex)

STPA?



Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Older system
(Simple)

Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Today's system
(Complex)

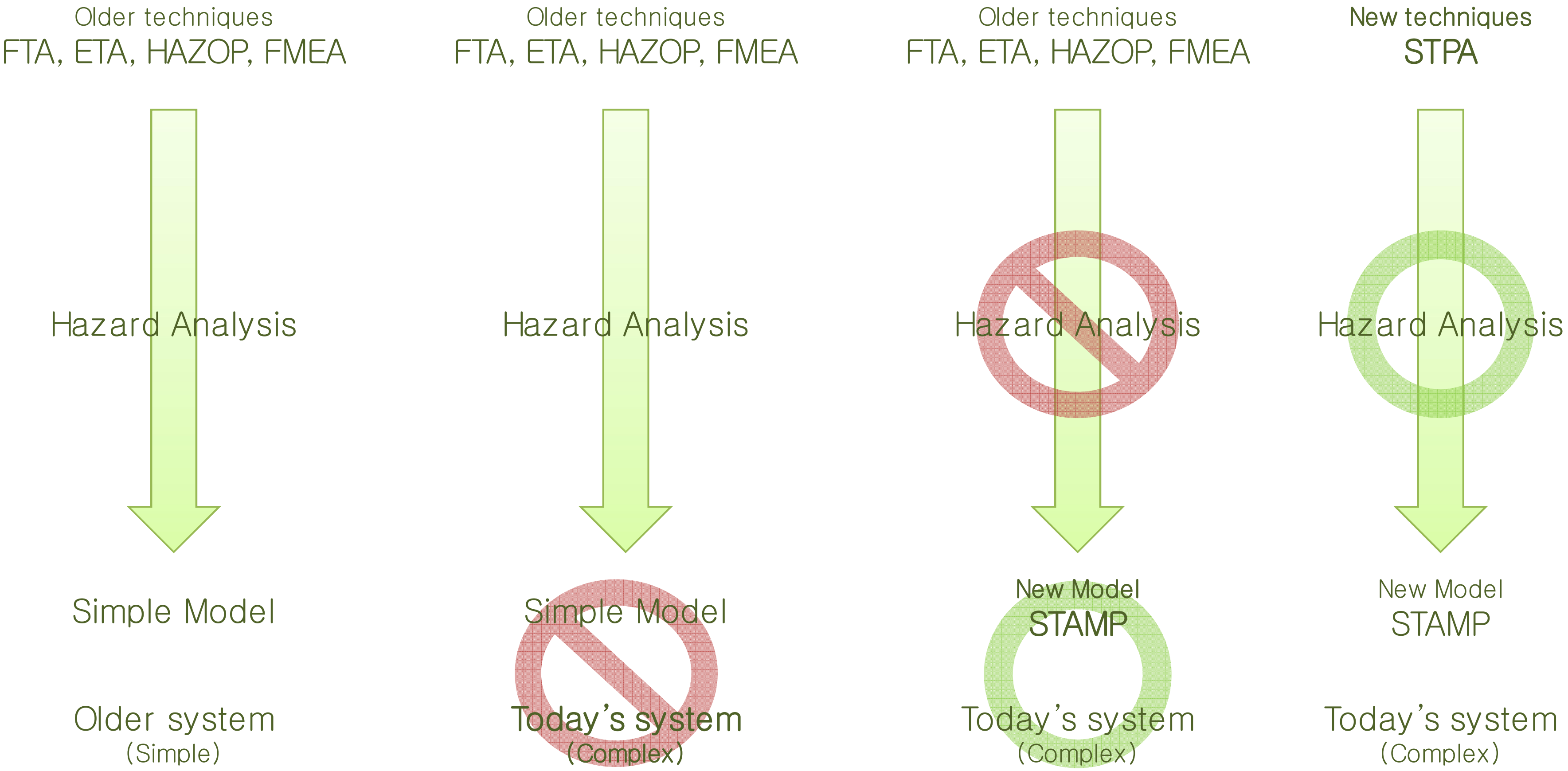
Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

New Model
STAMP

Today's system
(Complex)

STPA?



Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Older system
(Simple)

Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

Simple Model

Today's system
(Complex)

Older techniques
FTA, ETA, HAZOP, FMEA

Hazard Analysis

New Model
STAMP

Today's system
(Complex)

New techniques
STPA

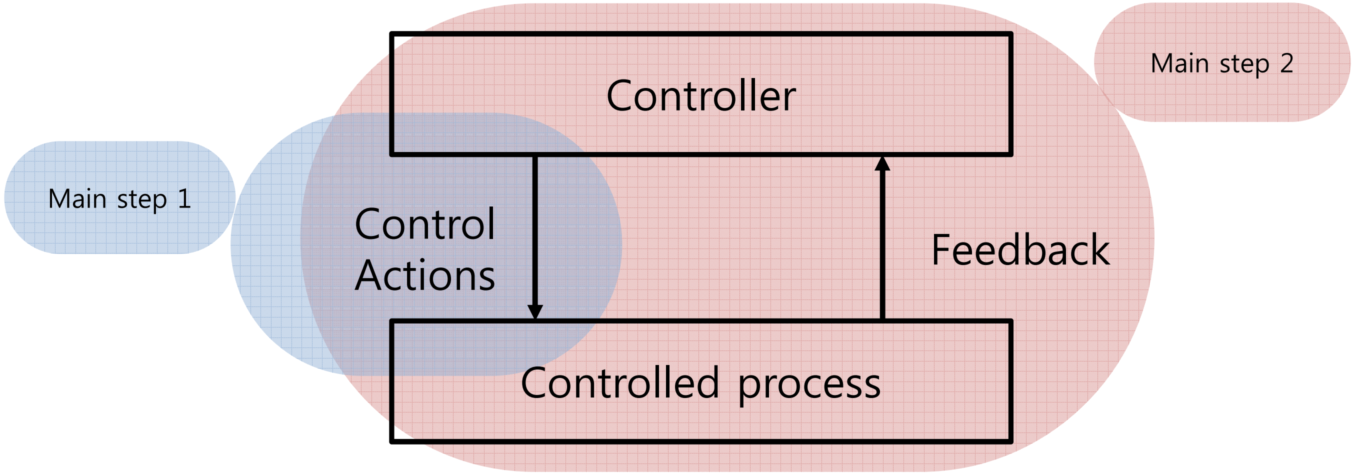
Hazard Analysis

New Model
STAMP

Today's system
(Complex)

STPA Process

- Identify the hazards
- Construct the control structure
- Main step 1: Identify unsafe control actions
- Main step 2: Identify causes of unsafe control actions



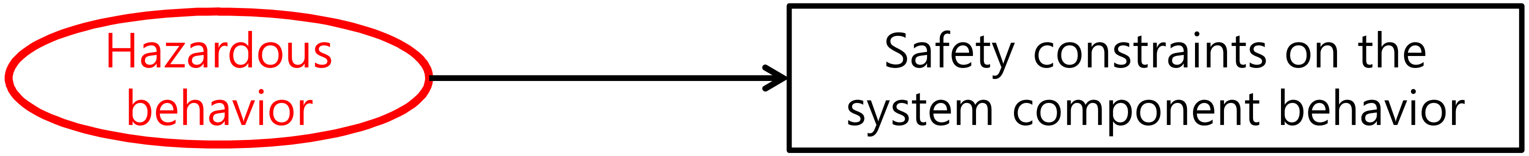
STPA Process: Main step 1

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states from inadequate control or enforcement of the safety constraints, which can occur because:
   a. A required control action is *not* provided or not followed;
   b. An incorrect or unsafe control action *is* provided;
   c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence;
   d. A correct control action is stopped too soon.

Control Action	**Not Given or not followed**	**Given Incorrectly**	**Wrong Timing or Order**	**Stopped too soon**
…	…	…	…	…
…	…	…	…	…

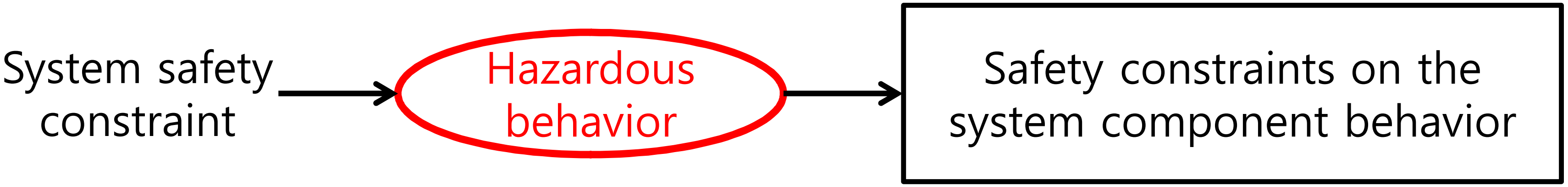
STPA Process: Main step 1

Control Action	Not Given or not followed	Given Incorrectly	Wrong Timing or Order	Stopped too soon
…	…	…	…	…
…	…	…	…	…



Hazardous behavior

Safety constraints on the system component behavior



System safety constraint

Hazardous behavior

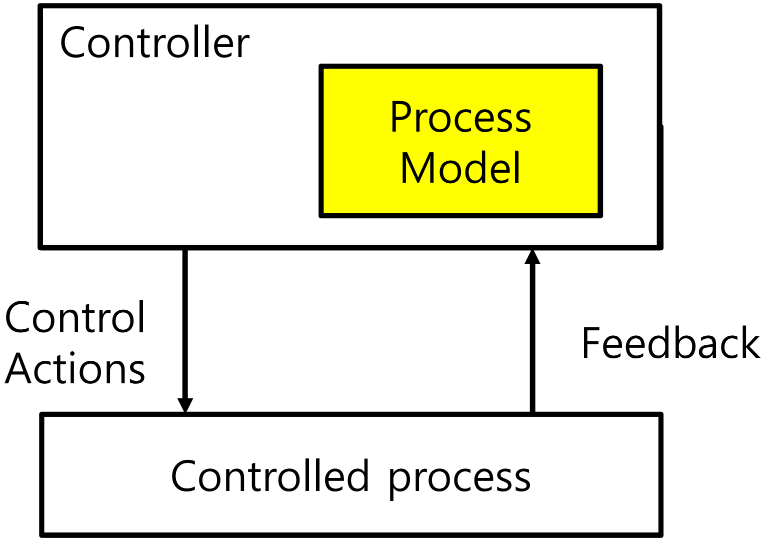
Safety constraints on the system component behavior

STPA Process: Main step 2

2. Determine how each potentially hazardous control action identified in step 1 could occur.
   a. Augment the control structure with process models for each control component.
   b. For each unsafe control action, examine the parts of the control loop to see if they could causes it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.
   c. Consider how the designed controls could degrade over time and build in protection.

STPA Process: Main step 2> a.

2. Determine how each potentially hazardous control action identified in step 1 could occur.
   a. Augment the control structure with process models for each control component.



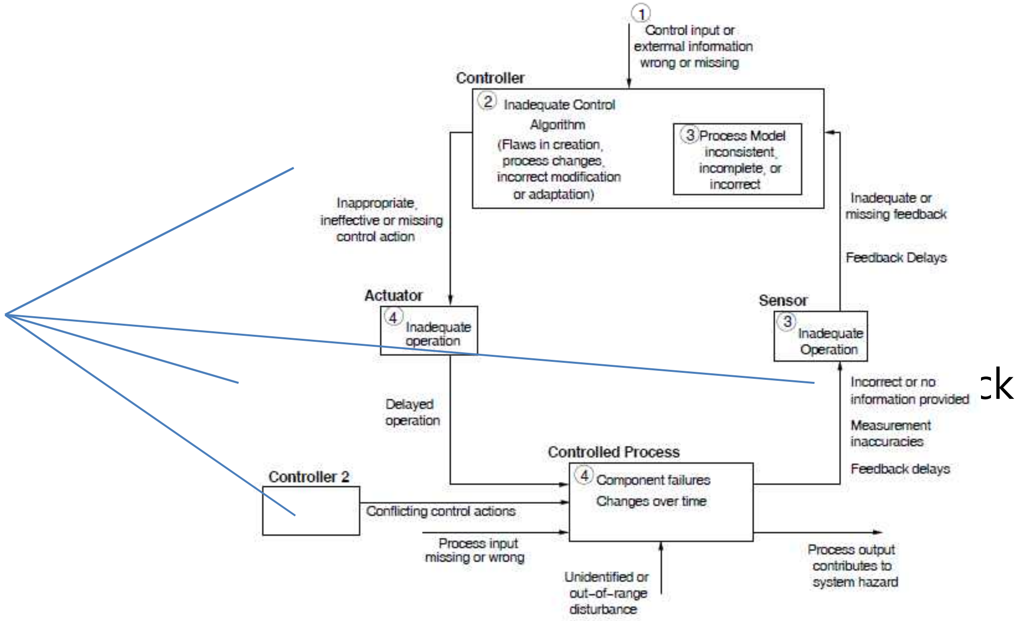
STPA Process: Main step 2> b.

2. Determine how each potentially hazardous control action identified in step 1 could occur.

   b. For each unsafe control action, examine the parts of the control loop to see if they could causes it.

Hazardous control actions

(Identified in Step 1)


1
Control input or external information wrong or missing
Controller
2 Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
3 Process Model inconsistent, incomplete, or incorrect
Inappropriate, ineffective or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
4 Inadequate operation
Sensor
3 Inadequate Operation
ck
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controlled Process
4 Component failures
Changes over time
Controller 2
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

STPA Process: Main step 2> c.

2. Determine how each potentially hazardous control action identified in step 1 could occur.
   c. Consider how the designed controls could degrade over time and build in protection, including
      I. *Management of change procedures* to ensure safety constraints are enforced in planned changes.
      II. *Performance audits* where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that violated the safety constraints can be detected.
      III. *Accident and incident analysis* to trace anomalies to the hazards and to the system design.

A simple example: Generic interlock

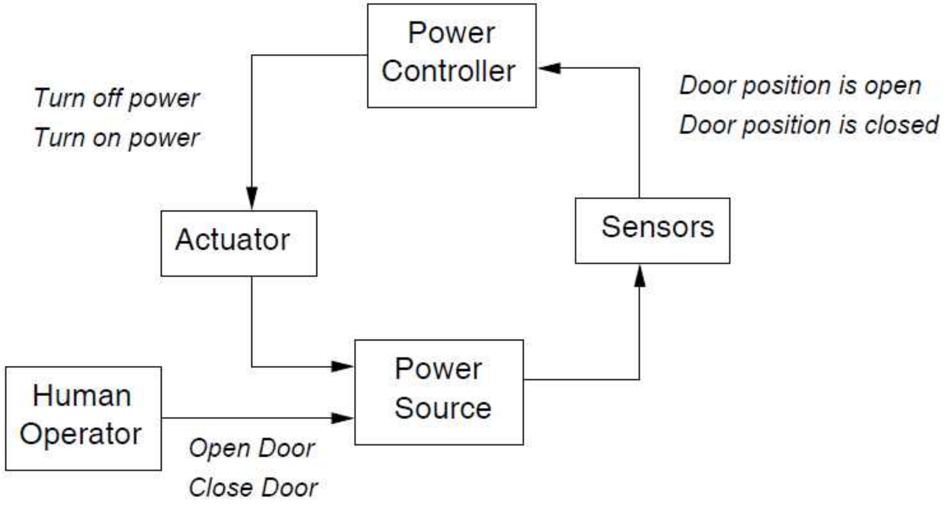
HAZARD: Human exposed to high energy source

SYSTEM SAFETY CONSTRAINT: The energy source must be off whenever the door is not completely closed.

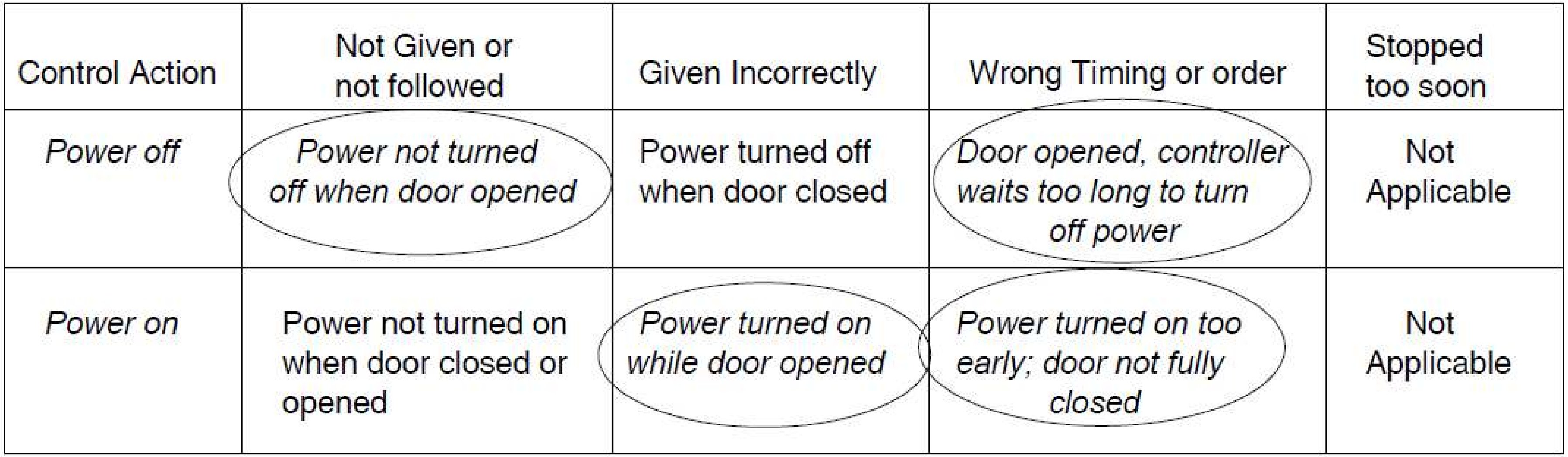
FUNCTIONAL REQUIREMENTS of the Power Controller:

(1) Detect when the door is opened and turn off the power

(2) When the door is closed, turn on the power

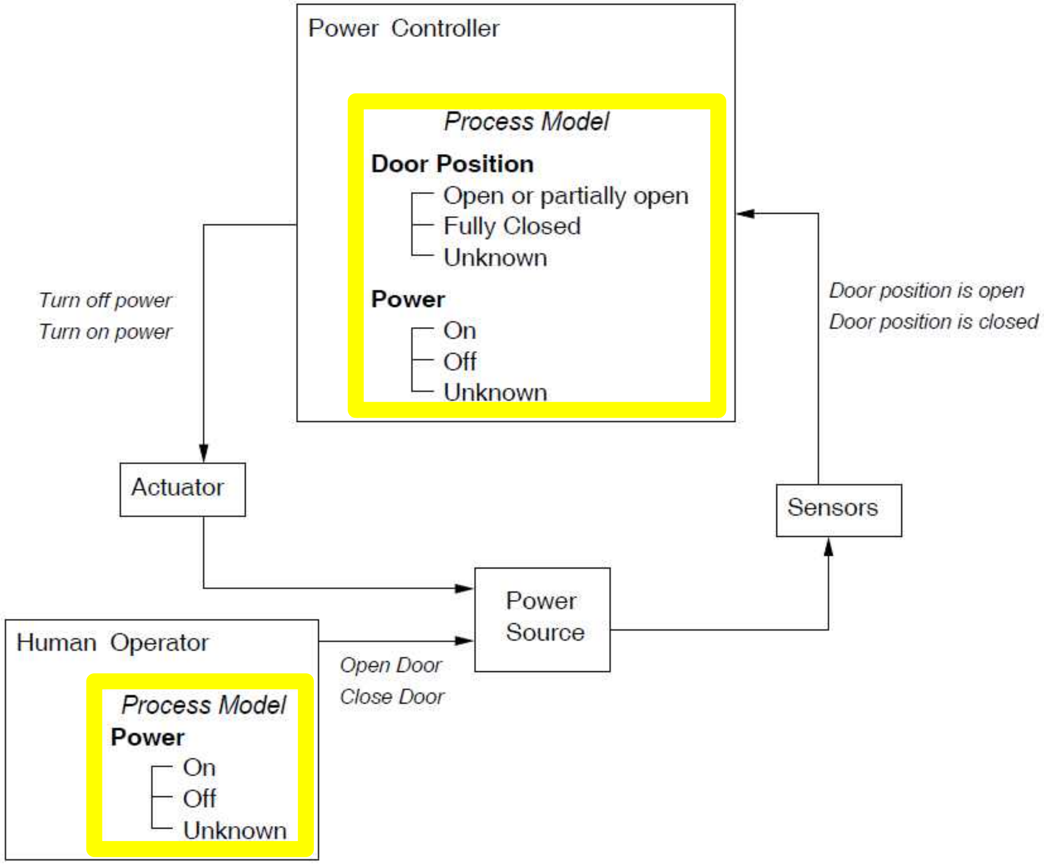


A simple example: Step 1

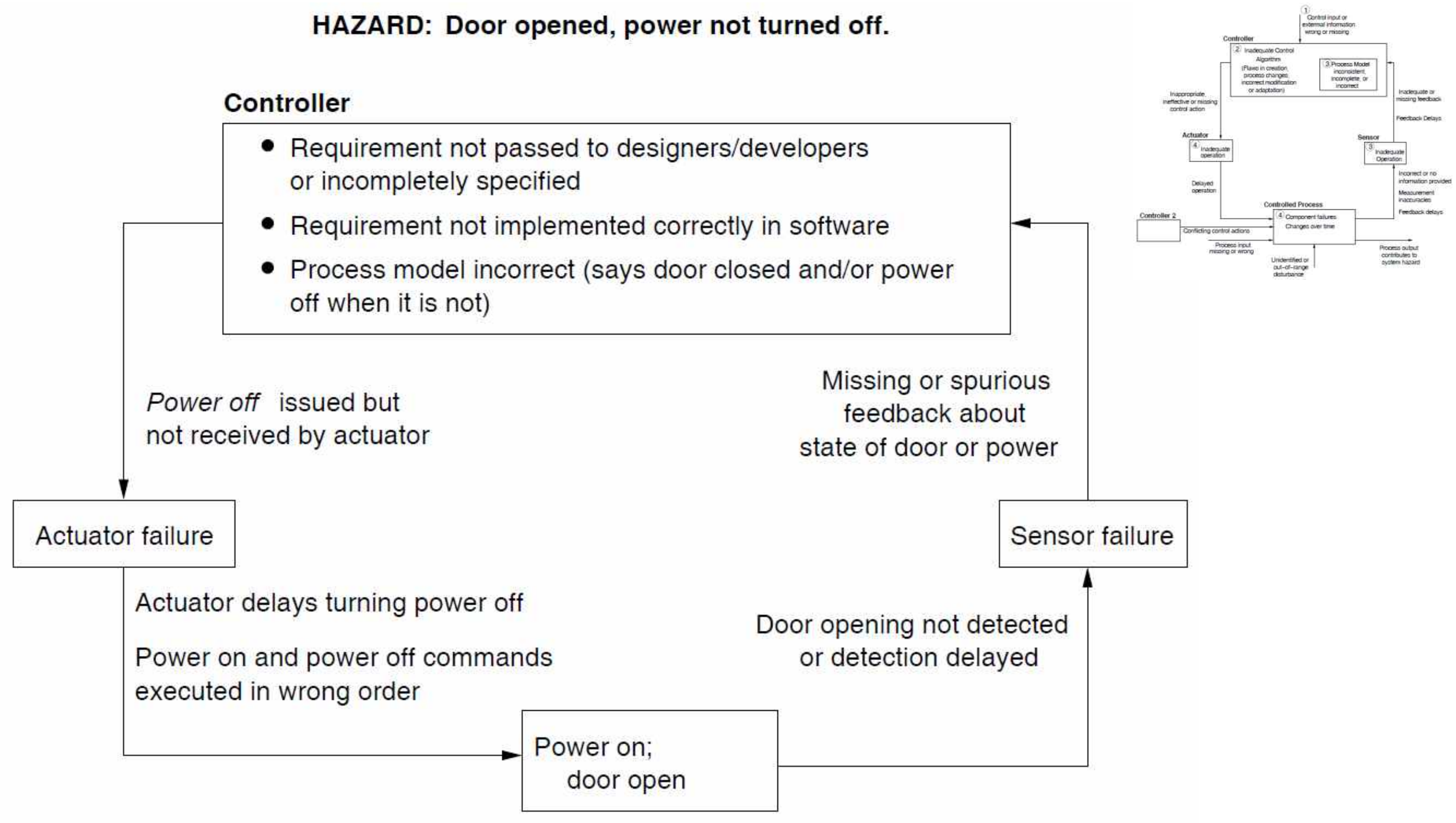


Control Action	Not Given or not followed	Given Incorrectly	Wrong Timing or order	Stopped too soon
Power off	*Power not turned off when door opened*	Power turned off when door closed	*Door opened, controller waits too long to turn off power*	Not Applicable
Power on	Power not turned on when door closed or opened	*Power turned on while door opened*	*Power turned on too early; door not fully closed*	Not Applicable

A simple example: Step 2a



A simple example: Step 2b



HAZARD: Door opened, power not turned off.

Controller

- Requirement not passed to designers/developers or incompletely specified
- Requirement not implemented correctly in software
- Process model incorrect (says door closed and/or power off when it is not)

Power off issued but not received by actuator

Missing or spurious feedback about state of door or power

Actuator failure

Sensor failure

Actuator delays turning power off

Power on and power off commands executed in wrong order

Door opening not detected or detection delayed

Power on; door open

1 Control input or external information wrong or missing
Controller
2 Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
3 Process Model inconsistent, incomplete, or incorrect
Inappropriate, ineffective or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
4 Inadequate operation
Sensor
3 Inadequate Operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controlled Process
4 Component failures
Changes over time
Controller 2
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

SIMPLE STPA EXERCISE

STPA Process

- Identify accidents and hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table: Not given, Given incorrectly, Wrong timing, Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Identify accidents and hazards

Accident (Loss): ?

Identify accidents and hazards

Accident (Loss): Two aircraft collide

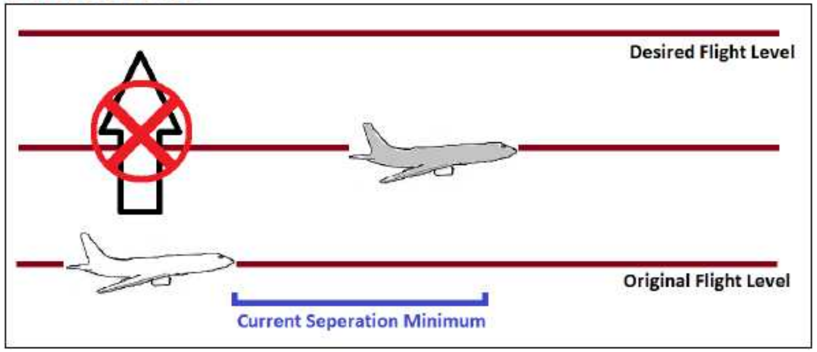
Identify accidents and hazards

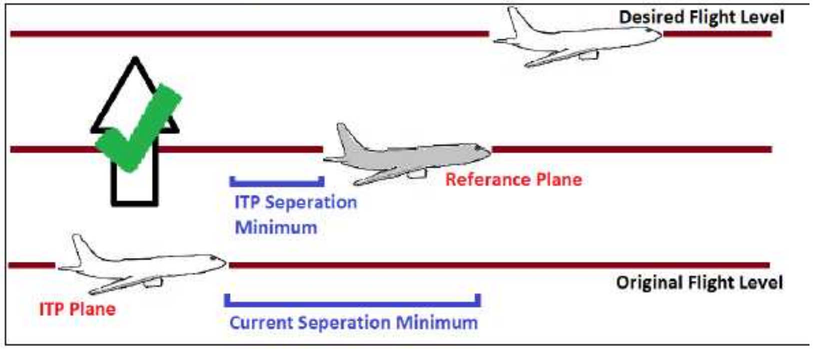
Accident (Loss): Two aircraft collide
Hazard: ?

Identify accidents and hazards

Accident (Loss): Two aircraft collide
Hazard: Two aircraft violate minimum separation

Draw the control structure

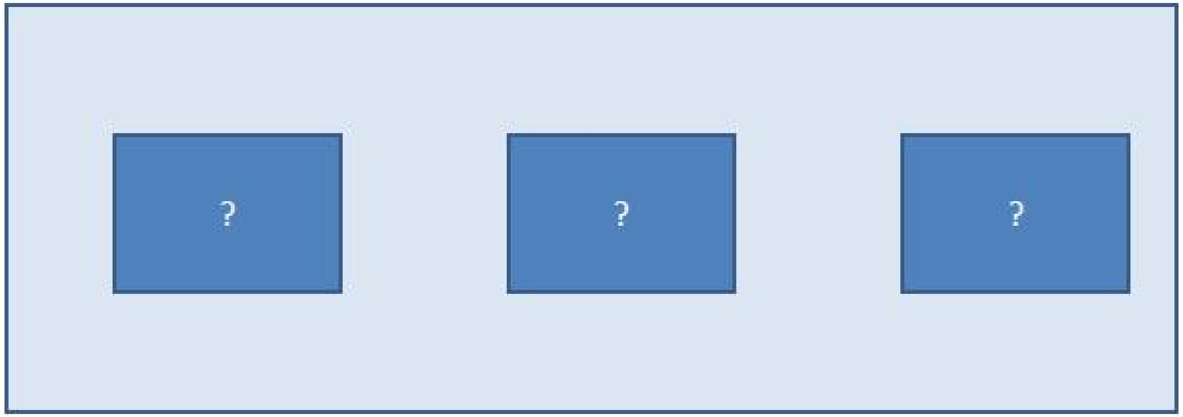

Current State


Proposed Change

- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

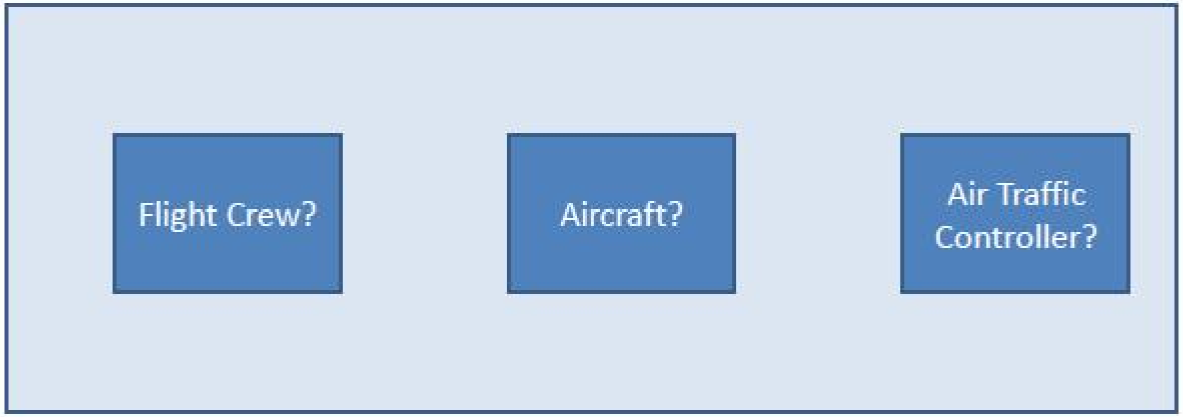
Draw the control structure

- High-level (simple) Control Structure
  - Main components and controllers?



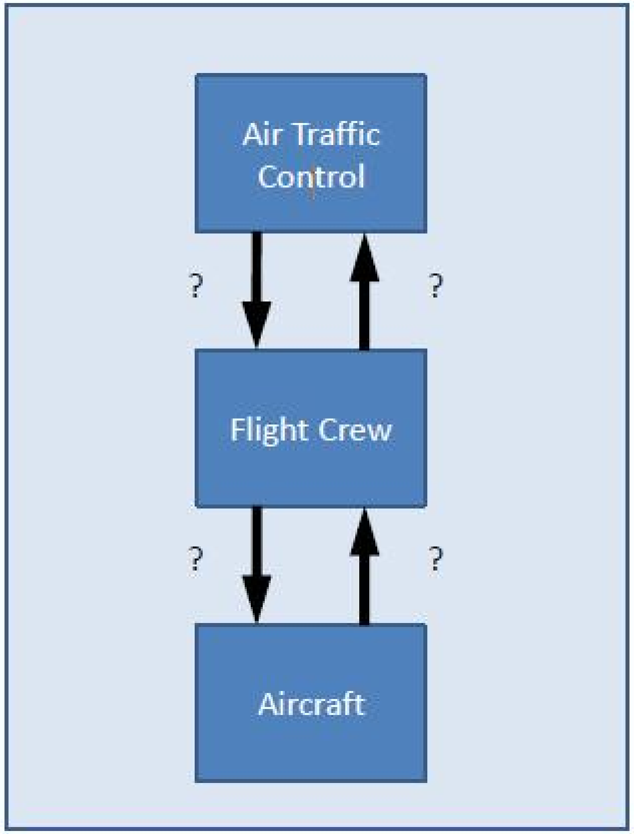
Draw the control structure

- High-level (simple) Control Structure
  - Who controls who?



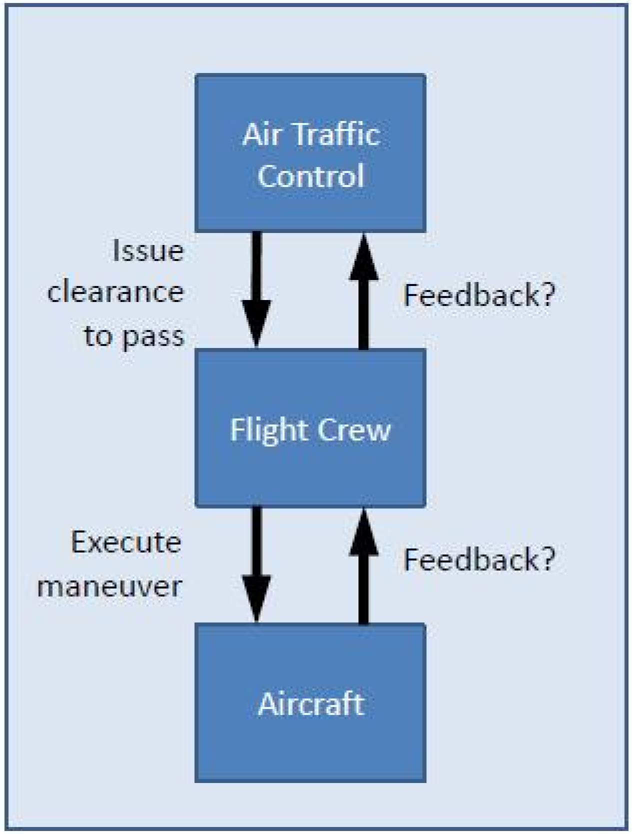
Draw the control structure

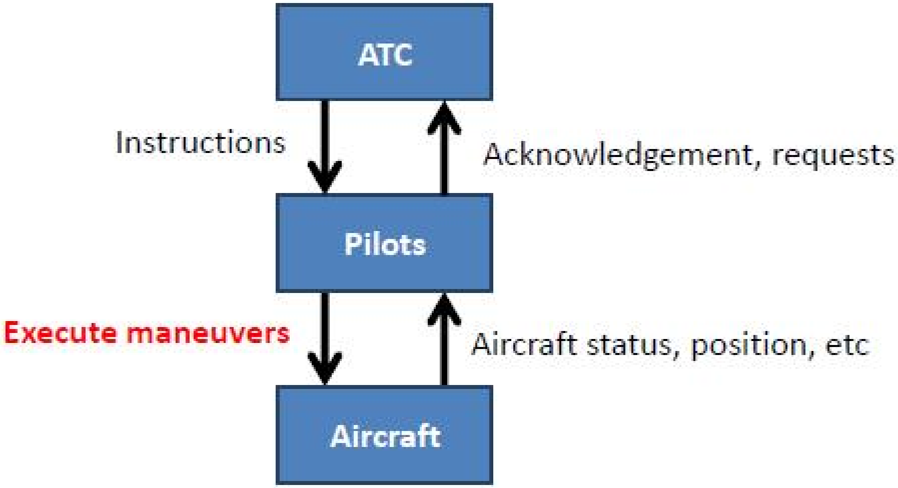
- High-level (simple) Control Structure
  - What commands are sent?



Draw the control structure

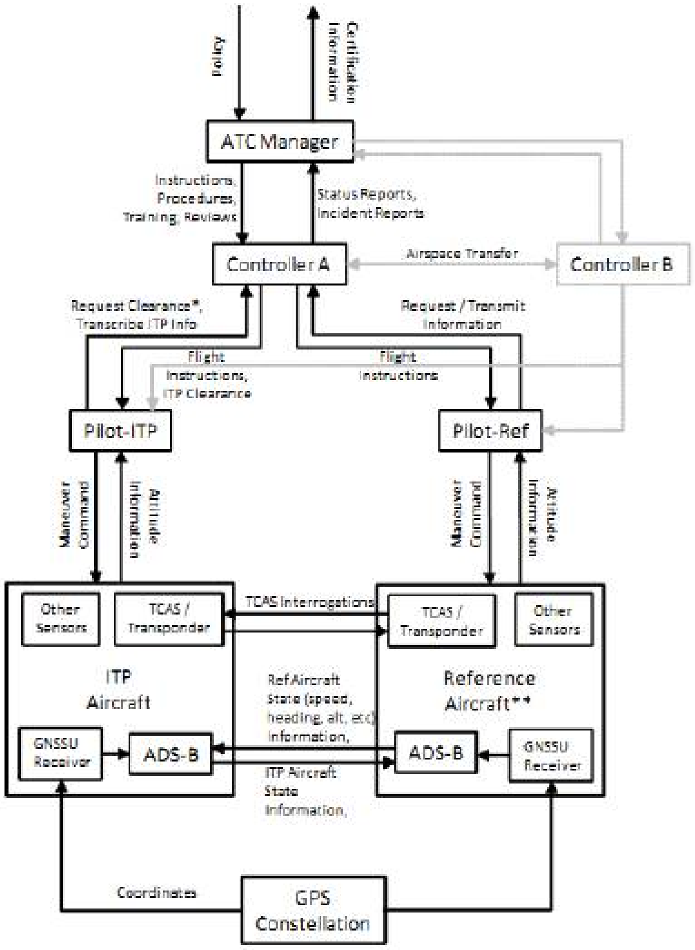
- High-level (simple) Control Structure



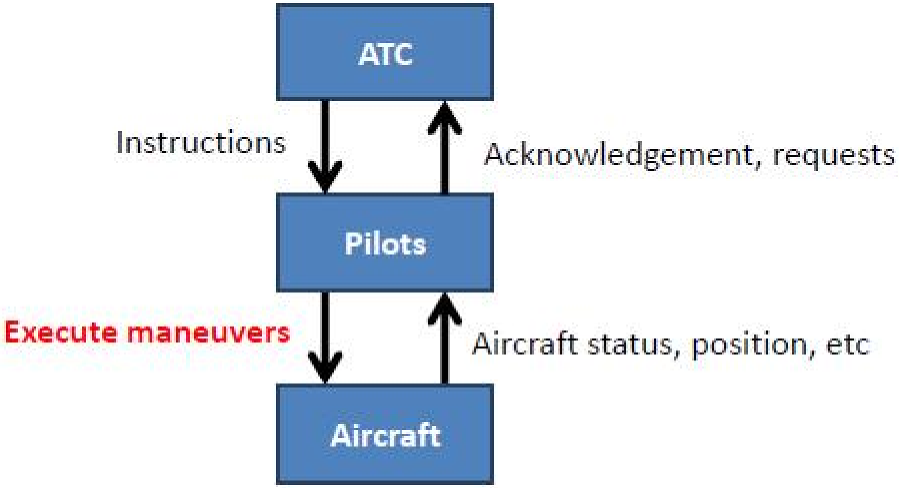


Draw the control structure

- More complex control structure

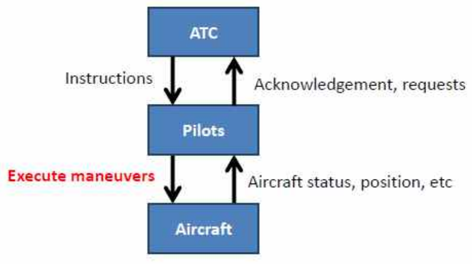


Identify Unsafe Control Actions



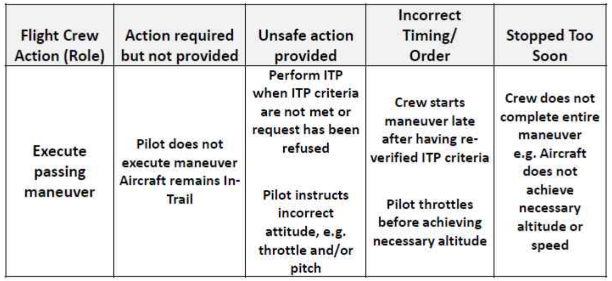
Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver	Pilot does not execute maneuver once it is approved			

Identify Unsafe Control Actions



Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Execute passing maneuver	Pilot does not execute maneuver Aircraft remains In-Trail	Perform ITP when ITP criteria are not met or request has been refused Pilot instructs incorrect attitude, e.g. throttle and/or pitch	Crew starts maneuver late after having re-verified ITP criteria Pilot throttles before achieving necessary altitude	Crew does not complete entire maneuver e.g. Aircraft does not achieve necessary altitude or speed

Identify Unsafe Control Actions

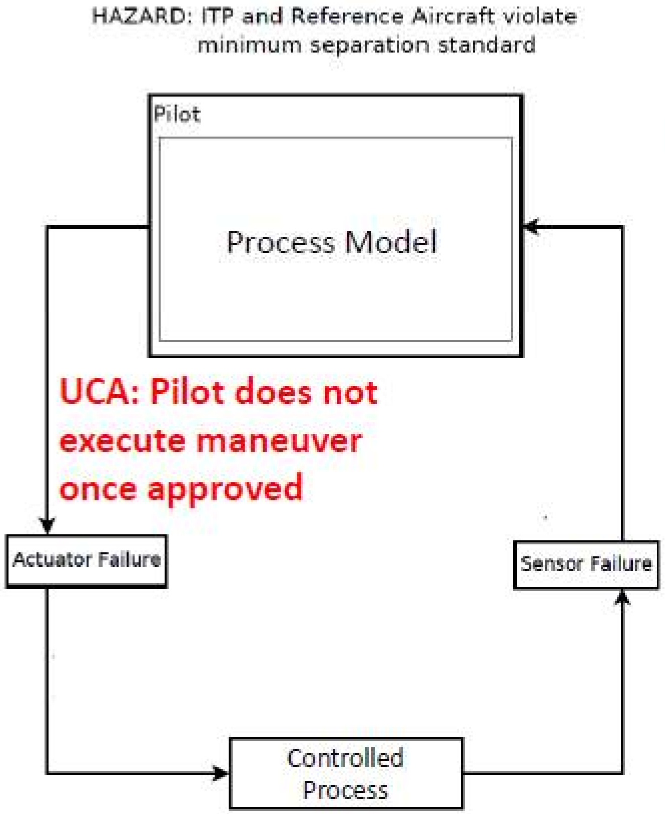


Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Execute passing maneuver	Pilot does not execute maneuver Aircraft remains In-Trail	Perform ITP when ITP criteria are not met or request has been refused Pilot instructs incorrect attitude, e.g. throttle and/or pitch	Crew starts maneuver late after having re-verified ITP criteria Pilot throttles before achieving necessary altitude	Crew does not complete entire maneuver e.g. Aircraft does not achieve necessary altitude or speed

Defining Safety Constraints

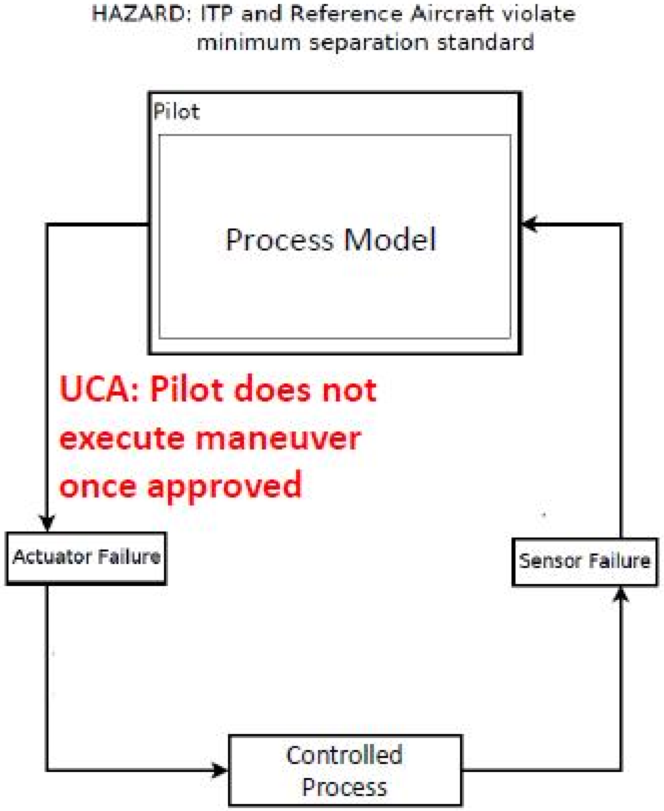
Unsafe Control Action	Safety Constraint
Pilot does not execute maneuver once it is approved	Pilot must execute maneuver once it is approved
Pilot performs ITP when ITP criteria are not met or request has been refused	Pilot must not perform ITP when criteria are not met or request has been refused
Pilot starts maneuver late after having re-verified ITP criteria	Pilot must start maneuver within X minutes of re-verifying ITP criteria

Identify causal factors


HAZARD: ITP and Reference Aircraft violate minimum separation standard
Pilot
Process Model
UCA: Pilot does not execute maneuver once approved
Actuator Failure
Sensor Failure
Controlled Process

- How could this action be caused by:
  - Process model
  - Feedback
  - Sensors
  - Etc?

Identify causal factors



HAZARD: ITP and Reference Aircraft violate minimum separation standard

Pilot

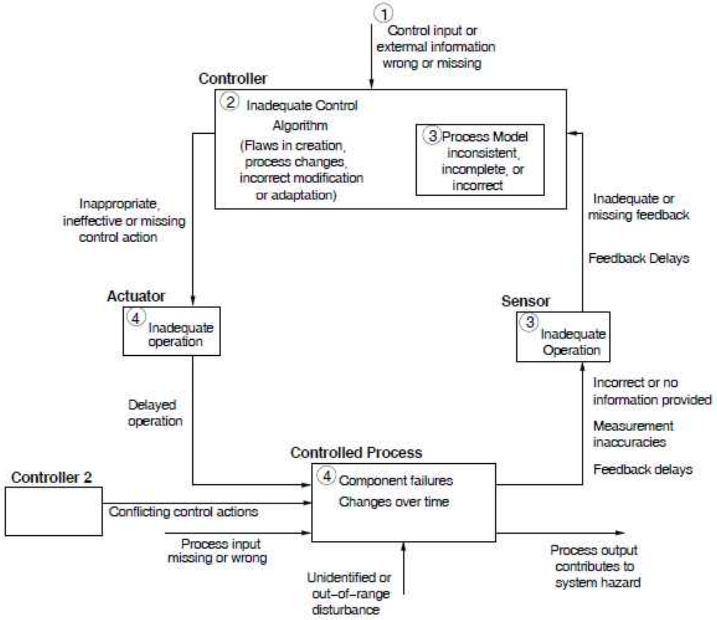
Process Model

UCA: Pilot does not execute maneuver once approved

Actuator Failure

Sensor Failure

Controlled Process



1 Control input or external information wrong or missing

Controller

2 Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

3 Process Model inconsistent, incomplete, or incorrect

Inappropriate, ineffective or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

4 Inadequate operation

Sensor

3 Inadequate Operation

Delayed operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controlled Process

4 Component failures

Changes over time

Controller 2

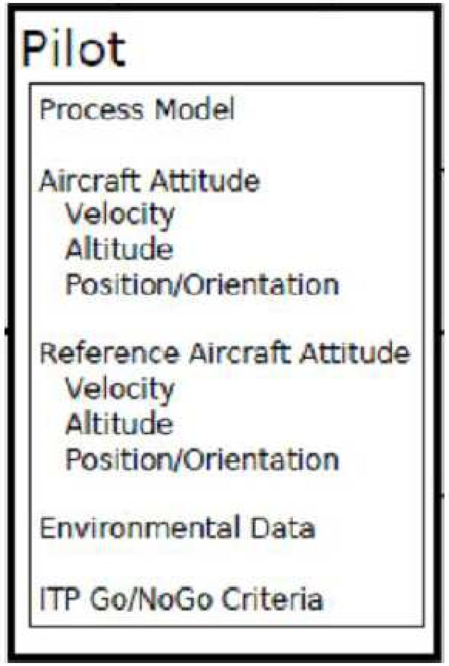
Conflicting control actions

Process input missing or wrong

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Identify causal factors



Pilot

Process Model

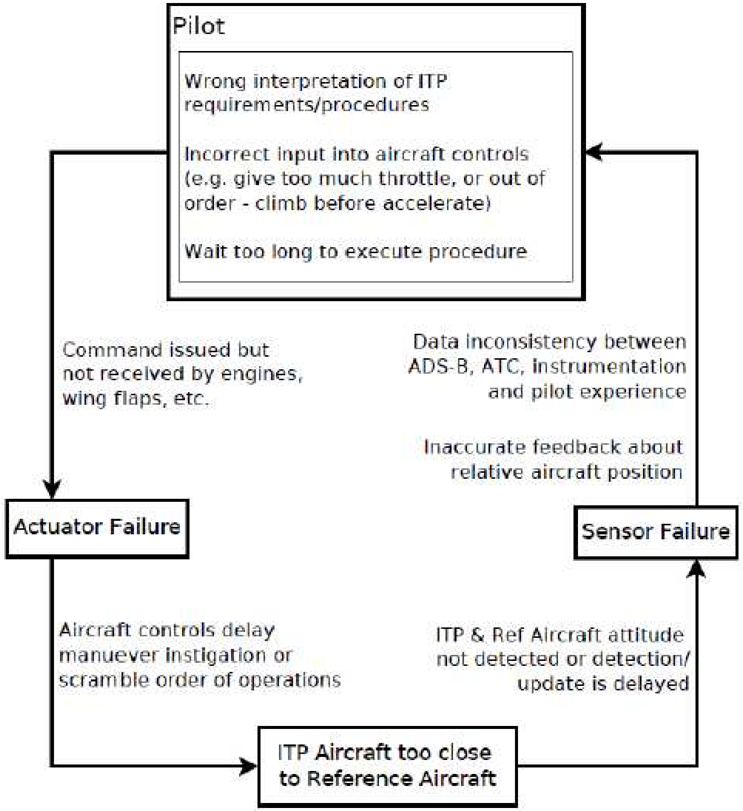
Aircraft Attitude
Velocity
Altitude
Position/Orientation

Reference Aircraft Attitude
Velocity
Altitude
Position/Orientation

Environmental Data

ITP Go/NoGo Criteria

HAZARD: ITP and Reference Aircraft violate minimum separation standard



Pilot

Wrong interpretation of ITP requirements/procedures

Incorrect input into aircraft controls (e.g. give too much throttle, or out of order - climb before accelerate)

Wait too long to execute procedure

Command issued but not received by engines, wing flaps, etc.

Data inconsistency between ADS-B, ATC, instrumentation and pilot experience

Inaccurate feedback about relative aircraft position

Actuator Failure

Sensor Failure

Aircraft controls delay manuever instigation or scramble order of operations

ITP & Ref Aircraft attitude not detected or detection/ update is delayed

ITP Aircraft too close to Reference Aircraft

THANK YOU