MIT ESD
Engineering Systems Division

AERO ASTRO

Assuring Safety of NextGen Procedures

Prof. Nancy Leveson

Cody H. Fleming

M. Seth Placke

Outline

- Motivation
- Propose Accident Model
- Hazard Analysis Technique
- Current and Future Work

Motivation

Air Traffic Management systems are rapidly evolving in complexity:

- Increased use of decision support tools
- Coupling of traditionally de-coupled systems
- Desire to increase the pace of development and implementation

Examples:

- Clearance-Based Operations → Trajectory-Based Operations
- VOX Communication → Data-Link Communication

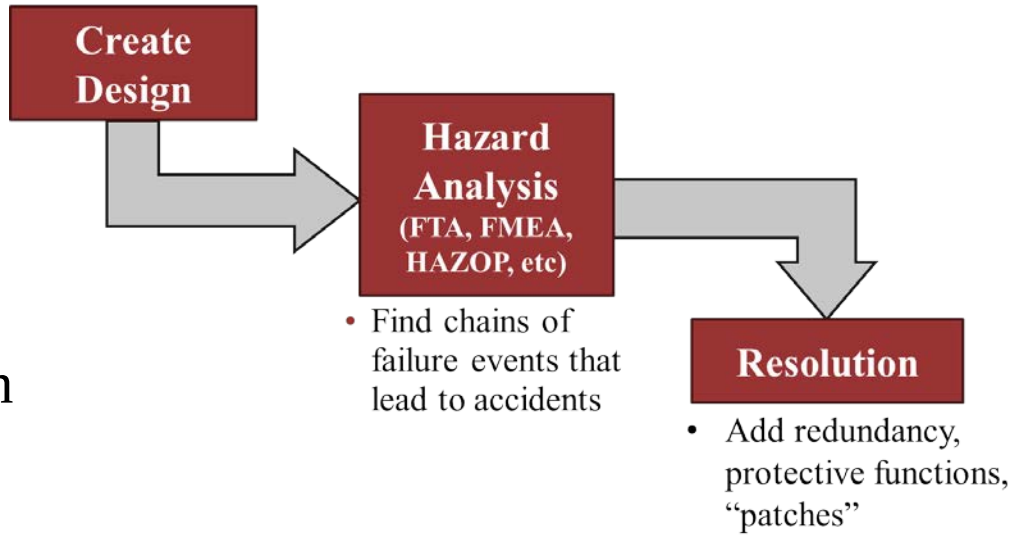
Traditional Methods and Process

Historically view safety as a failure problem:

- Chain of event accident models
- Mitigation is focused on establishing barriers between events and/or preventing component failures

Areas for improvement:

- Human error
- Software behavior
- Socio-technical factors
- Evolution and adaptation



(Vincoli, 1993); (Bahr, 1997); (FAA SSH, 2000); (AF SSH, 2000)

Goals for a New Approach

Support a safety-driven design process where:

- Hazard analysis influences and shapes early design decisions
- Hazards analysis is iterated and refined as the design evolves

Hazard analysis that:

- Captures accidents resulting from component interaction, not just failures
- Can appropriately treat increased reliance on software and human interaction with automation

Systems Approach to Safety:

System-Theoretic Accident Model and Processes

STAMP Model

- Accidents involve complex dynamic **processes** involving humans, machines and their environment.
- Treat accidents as a **control problem**.
- Prevent accidents by enforcing constraints on system behavior and component **interactions**.
- Captures more causes of accidents:
  - Component failure accidents
  - Unsafe interaction among components
  - Complex human and software behavior
  - Design errors
  - Flawed requirements

(Leveson, 2003); (Leveson, 2011)

Safety as a Dynamic Control Problem

Hazardous events are the *result* of inadequate control

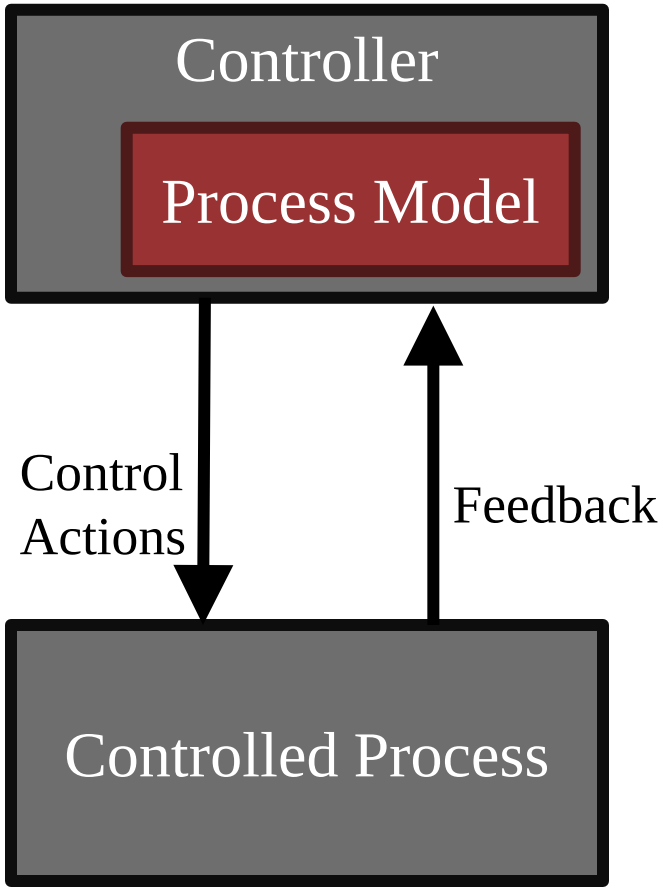
- Hazardous events occur when safety constraints are not enforced in system design and/or operations

Examples of inadequate control:

- O-ring did not control propellant gas release by sealing the gap in the field joint of the Challenger Space Shuttle
- Software did not adequately control descent speed of Mars Polar Lander

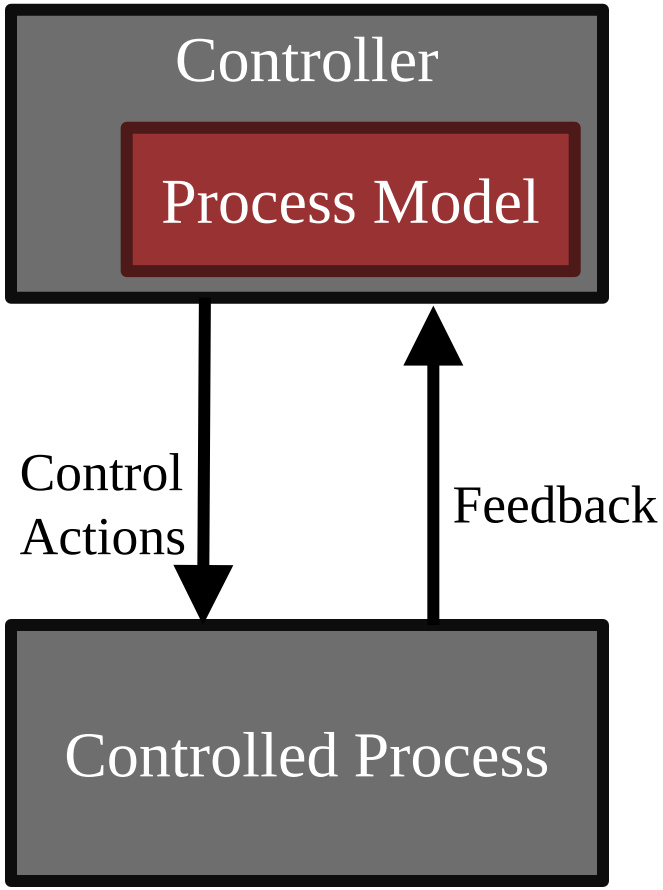
Goal: Design an effective system control structure that eliminates or reduces adverse events

STAMP (System-Theoretic Accident Model and Process)



- Controllers use a **process model** to determine control actions.
- Accidents often occur when the **process model** is incorrect.
- **Process Model**:
  - Model of the current system state
  - Understanding of how the system state may change

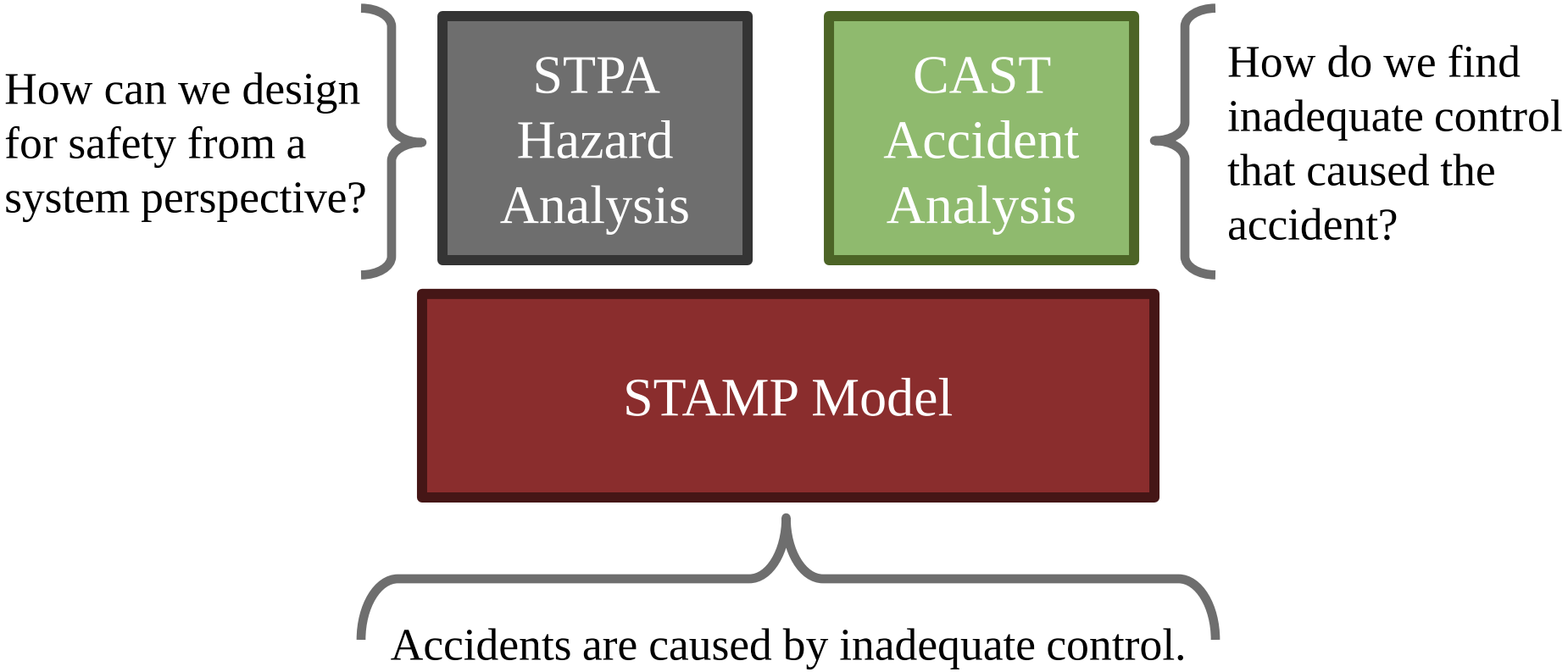
STAMP (System-Theoretic Accident Model and Process)



Four types of hazardous control actions:

- Commands required for safety are not given
- Unsafe commands are given
- Potentially safe commands are given too early, too late
- Control stops too soon or applied too long

STAMP Based Tools

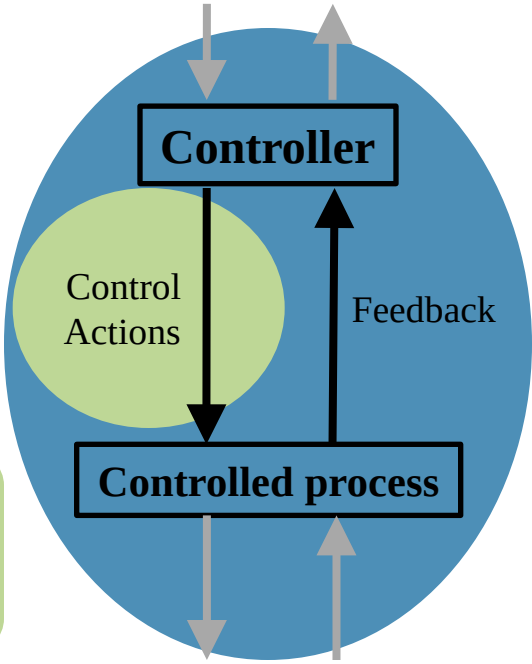


STPA (System-Theoretic Process Analysis)

STPA Hazard Analysis

STAMP Model

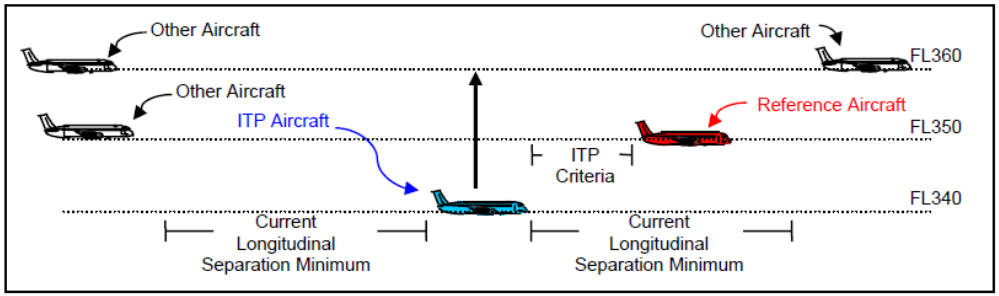
- Built on STAMP model
- Begins by identifying system control structure and undesired losses
- Identify hazardous control actions and safety constraints
- Identify scenarios that lead to violation of safety constraints

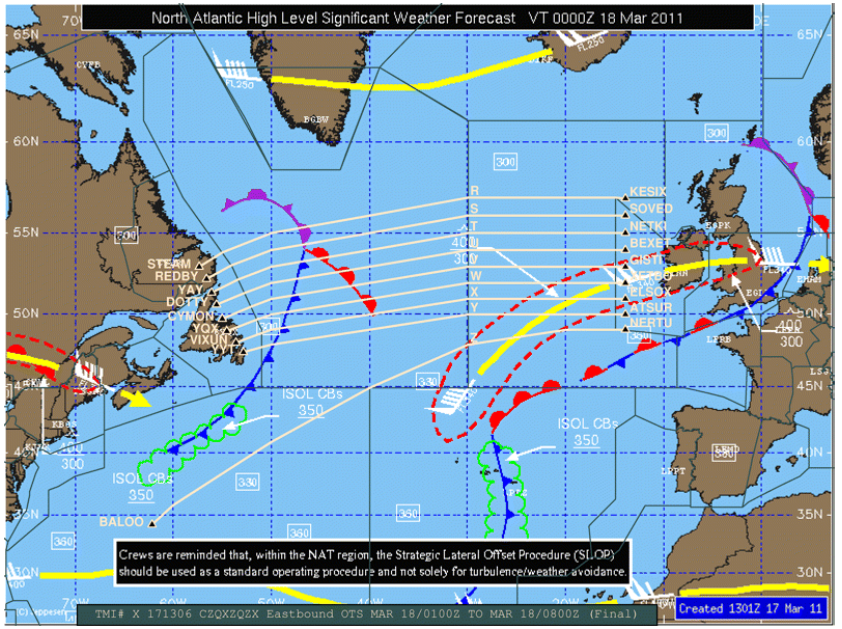


(Leveson, 2011)

NextGen In-Trail Procedure (ITP)

- ITP – new procedure for increased efficiency in oceanic airspace
  - Designed for oceanic and remote airspaces not covered by radar.
  - Permits climbs and descents using new reduced longitudinal separation standards.
  - More frequent FL changes.

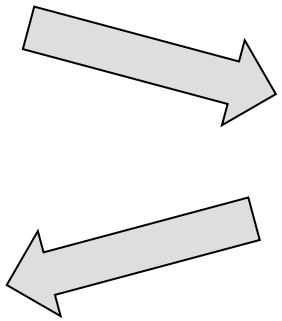




NextGen In-Trail Procedure (ITP)

Flight Crew

1. Check that ITP requirements are met and request clearance from ATC



Air Traffic Controller

2. Evaluate ITP request and approve if the criteria are satisfied

3. Upon receiving clearance:
   - Recheck criteria
   - Execute if satisfied
   - Report execution

Involves multiple aircraft, crew, communications (ADS-B, GPS), ATCO

STPA Process

1. Define accidents and hazards
2. Develop the system control structure
   - Identify major components and controllers
   - Label the control/feedback arrows
3. Identify Unsafe Control Actions (UCAs)
   - Derive corresponding safety constraints
4. Identify Causal Factors
   - Identify controller process models
   - Analyze controller, control/feedback paths and processes

Definitions

Accident:

- An undesired or unplanned event that results in a loss.
  - Loss: life, injury, property, pollution, mission, etc…
  - May involved environmental factors *outside our control*.

Hazard:

- A system state or set of conditions that, together with a particular set of worst-case conditions, will lead to an accident (loss).
- Something we can *control* in the design.

Definitions from *Engineering a Safer World*

Accidents and Hazards

Accidents:

1. Two Aircraft Collide
2. Aircraft Crashes into Terrain or Ocean

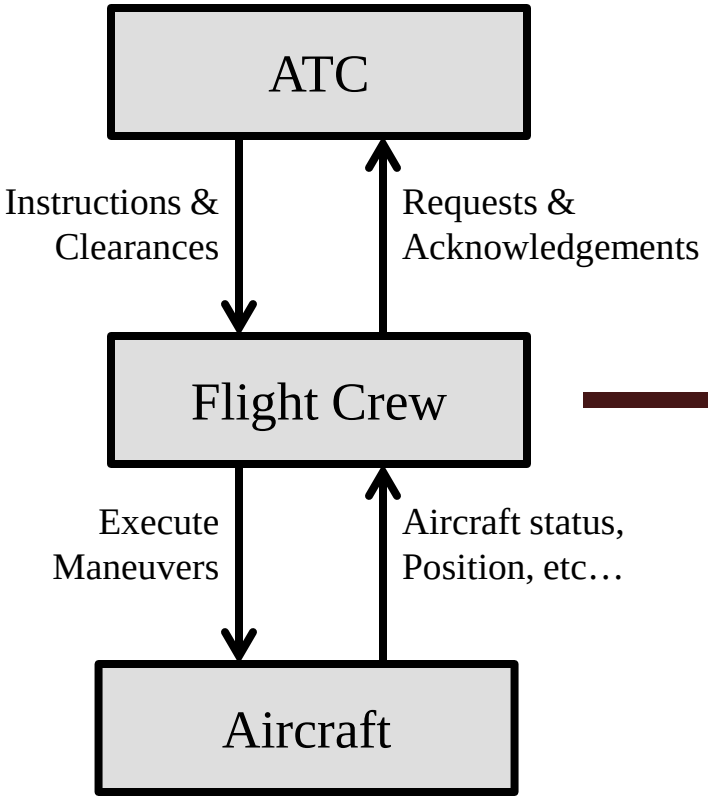
Hazards:

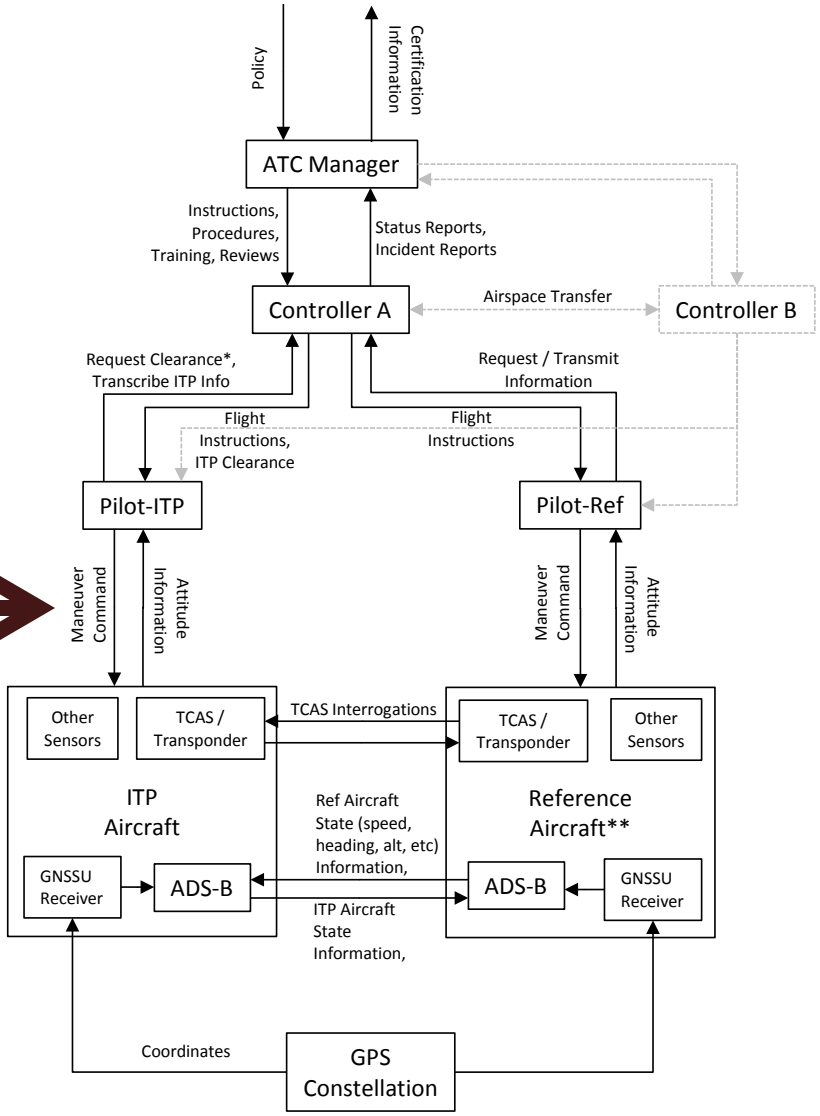
1. A pair of controlled aircraft violate minimum separation standards (LOS)
2. Aircraft enters unsafe atmospheric region
3. Aircraft enters uncontrolled state
4. Aircraft enters unsafe attitude
5. Aircraft enters a prohibited area

System Control Structure

- Functional representation of the system
- May or may not be the same as a physical system representation
- Begin with high-level representation and refine as needed
- Identify and document:
  - Safety related responsibilities of each controller
  - Available control actions
  - Available feedback paths and mechanisms

ITP Control Structure





Identify Unsafe Control Actions

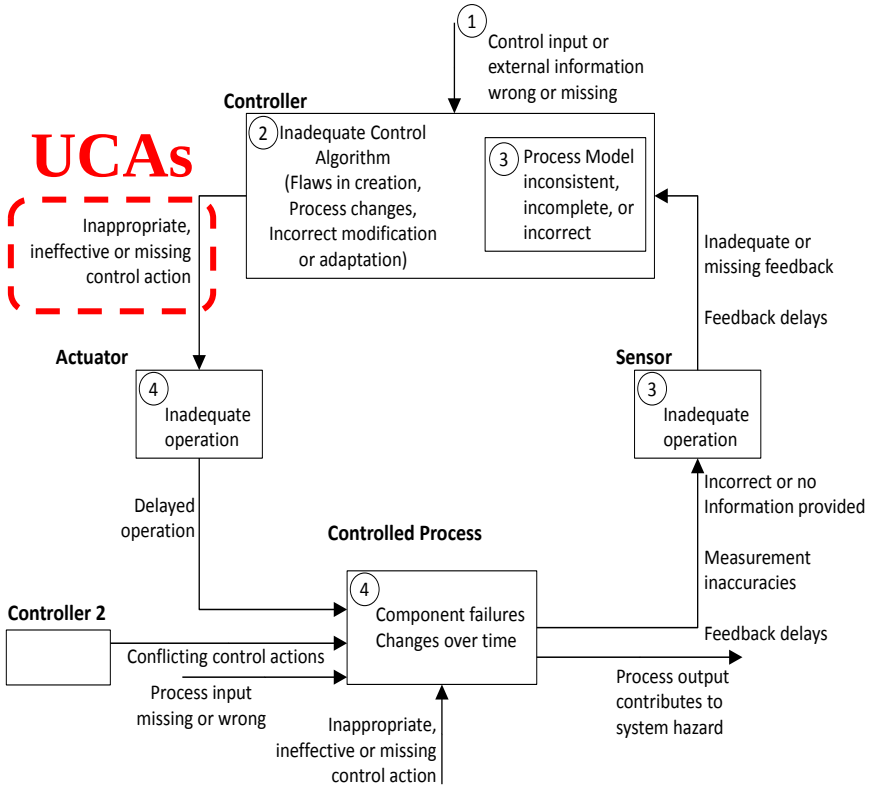
- How can a control action lead to H-1: Loss Of Separation…?

Flight Crew Action	Required action not provided	Unsafe action provided	Incorrect Timing/Order	Too Soon/Long
Execute Passing Maneuver	Pilot does not execute maneuver & aircraft remains in-trail	ITP executed when not approved ITP executed when criteria are not satisfied ITP executed with incorrect climb rate, final altitude, etc…	Crew starts maneuver late after having re-verified ITP criteria Pilot throttles before achieving necessary altitude	ITP aircraft levels off above/below requested FL. ITP maintains passing speed after maneuver.

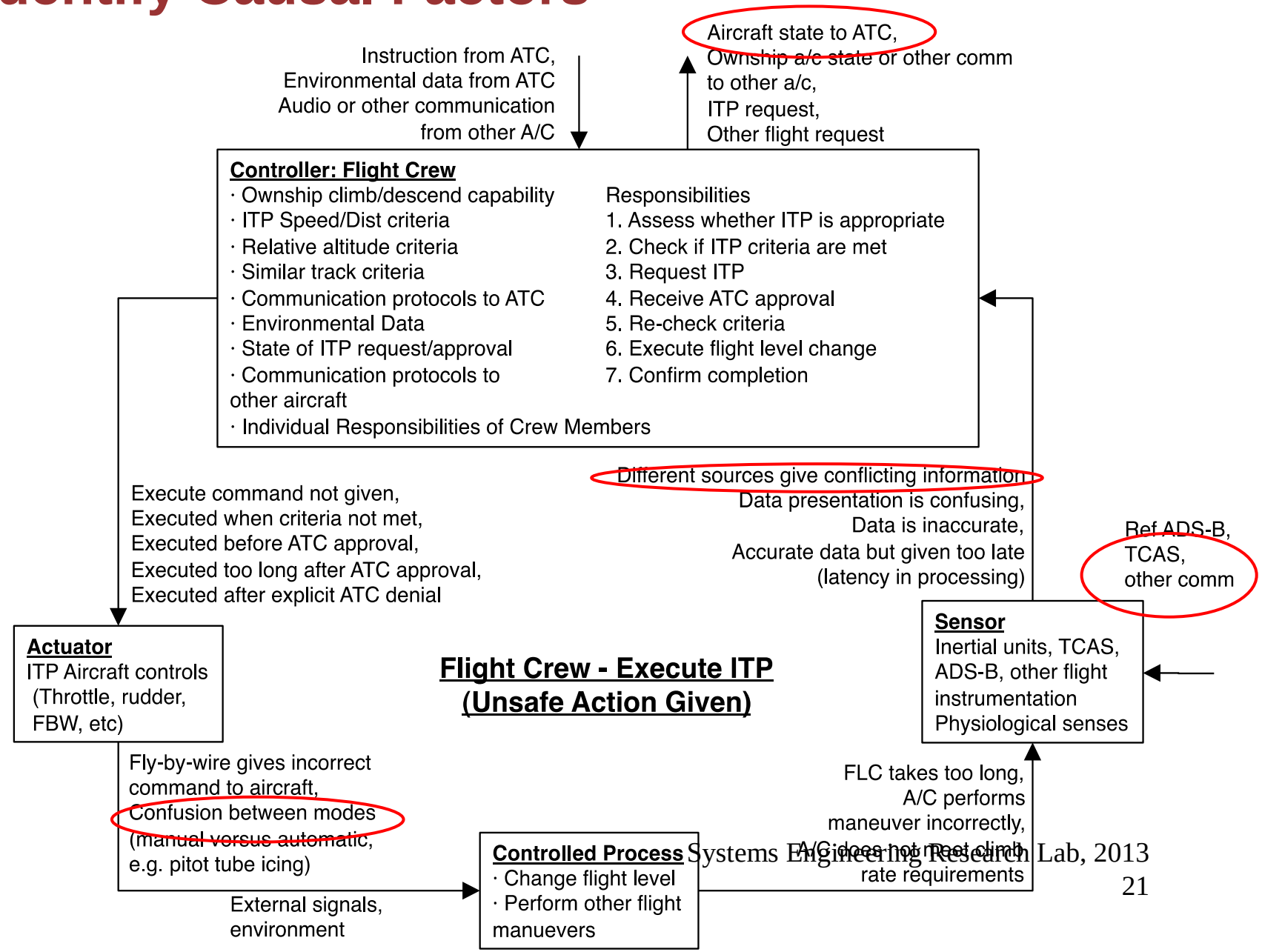
*High level examples for illustration

Identify Causal Factors

- Use guidewords and control loop to identify scenarios leading to unsafe control.
- Potential causes for unsafe control may be:
  - Eliminated during design
  - Used to produce detailed functional requirements on system components.



Identify Causal Factors



Example cause found by STPA

- **Accident:** Two Aircraft Collide
- **Hazard:** A pair of controlled aircraft violate minimum separation standards (LOS)
- **An Unsafe Control Action:** ITP executed when criteria are not met
- **Selected Causal Factors:**
  - Different data sources give inconsistent or incorrect information
  - Clearance is given to the wrong aircraft b/c of id mismatch
  - Flight Crew does not re-check to ensure conditions have not changed

Safety Guided Design

- ITP analysis is still the evaluation of an existing system.
- How can we use STAMP/STPA to 'build-in' safety?
  - Use control structure and unsafe control actions to assess system architecture choices
  - Evaluate design assumptions at a high level before implementation
  - Identify significant changes from legacy systems and their propagation through the system

Conclusions

- The STAMP model provides new insight for safety engineering
  - Accidents are the result of dynamic processes
  - Hierarchical system control is necessary for hazard mitigation
- STPA has successfully been used to evaluate existing ATC designs
  - Identified 19 additional safety requirements for ITP
- Initial work using STPA for safety-guided design is ongoing:
  - Currently evaluating TBO and intermediate technologies (TBFM, GIM-S, FIM-S) during development

Questions?

More Information…

- MIT Group Site: psas.scripts.mit.edu/home
  - Papers/Theses demonstrating STAMP/STPA in a variety of fields
  - Presentations from 2012 & 2013 STAMP workshops
  - Information regarding new methods and tools associated with the STAMP accident model