A New Approach to Certifying Safety in NextGen

PI: Nancy Leveson, Aero/Astro, MIT

Co-PI: Chris Wilkinson, Honeywell

NASA Aviation Safety Program Annual Technical Meeting

Saint Louis, 10 May 2011

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

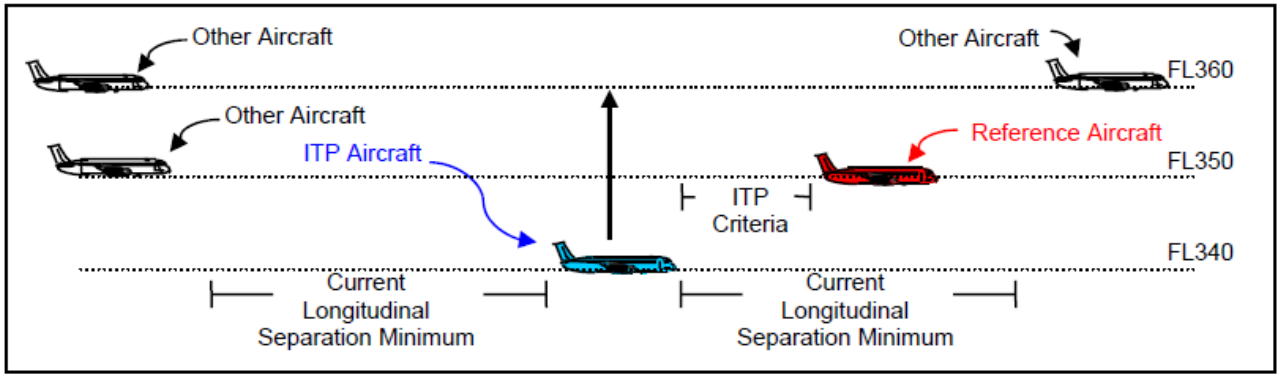
Outline

- Goals
- New Approach to Certification
- Preliminary Results

Research Goals

- Determine feasibility of applying systems theory concepts to assuring safety in NextGen
- Compare with current approach used in certifying NextGen components
- Demonstrate how changes to ATM system can be incrementally assured to be safe
- Define a methodology for assuring NextGen safety that uses
  - Executable, formally analyzable requirements specifications
  - Powerful hazard analysis methods to design and assure safety in NextGen procedures
- Evaluate commercial viability and practicality of approach
- Benchmark against current tools and methods used in aviation safety (e.g., ARP-4761, DO-178B(C))

In-Trail Procedure (ITP)



- Enables aircraft to achieve FL changes on a more frequent basis.
- Designed for oceanic and remote airspaces not covered by radar.
- Permits climbs and descents using new reduced longitudinal separation standards.
- Potential Benefits
  - Reduced fuel burn and CO2 emissions via more opportunities to reach the optimum FL or FL with more favorable winds.
  - Increased safety via more opportunities to leave turbulent FL.

ITP Procedure – Step by Step

Flight Crew

1. Check that ITP criteria are met.
2. If ITP is possible, request ATC clearance via CPDLC using ITP phraseology.

Air Traffic Controller

3. Check that there are no blocking aircraft other than Reference Aircraft in the ITP request.
4. Check that ITP request is applicable (i.e. standard request not sufficient) and compliant with ITP phraseology.
5. Check that ITP criteria are met.
6. If all checks are positive, issue ITP clearance via CPDLC.

8. When ITP clearance is received, check that ITP criteria are still met.
9. If ITP criteria are still met, accept ITP clearance via CPDLC.
10. Execute ITP clearance without delay.
11. Report when established at the cleared FL.

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

Why Need Something New

- System complexity increasing
  - Accidents no longer just caused by random component failure
  - Need to consider unplanned interactions among components
- New technology being introduced
- Software (automation) playing an increasingly important role
- Humans making more complex decisions. Integration of ground and air-based decision making

New Approach

- Similar to approach used to certify safety of TCAS
- New accident causality model (STAMP)
  - Based on system theory
  - Extends causality assumptions of traditional models
  - Handles new factors in NextGen
- New, more powerful hazard analysis methods
- New approach to requirements specification (Intent Specifications)
  - Executable, analyzable, easily readable
  - Includes design rationale, traceability
  - Developed for TCAS certification (still being used to evaluate safety of upgrades and changes) but has now been extended to include more features

STAMP (System-Theoretic Accident Model and Processes)

- Safety is a dynamic control problem, not just a failure problem.
- Losses are the result of complex processes, not simply chains of failure events
- Accidents can occur due to unsafe interactions among components, not just component failures
  - Component Failure Accidents
  - Component Interaction Accidents
- Systems are not static
  - Most major accidents arise from a slow migration of the entire system toward a state of high-risk.
  - Need to control and detect this migration

STAMP (2)

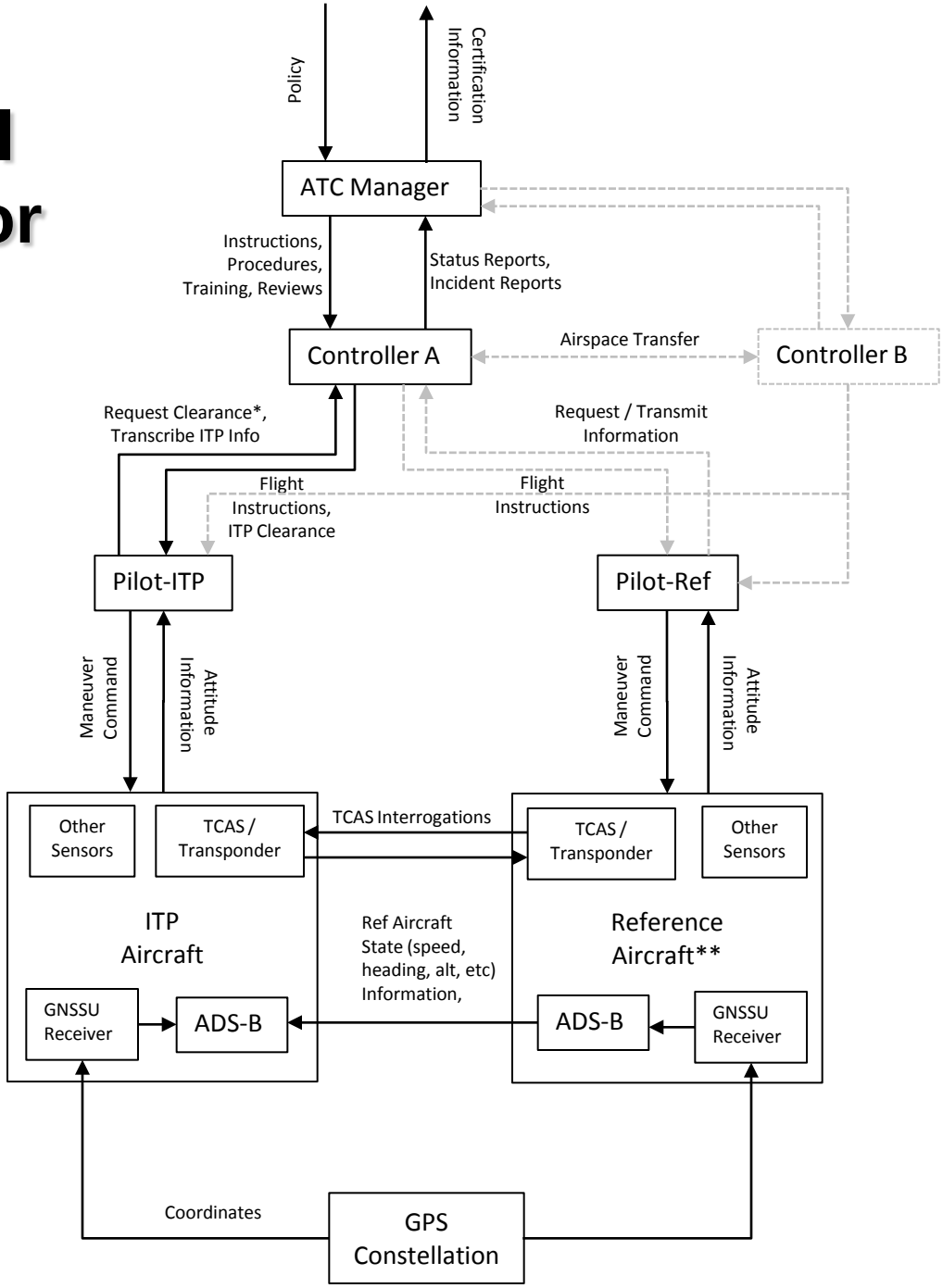
- Systems can be viewed as hierarchical control structures
  - Systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback loops of information and control
  - Controllers imposes constraints upon the activity at a lower level of the control hierarchy: safety constraints
- A change in emphasis:

"~~prevent failures~~"

↓

"enforce safety constraints on system behavior"

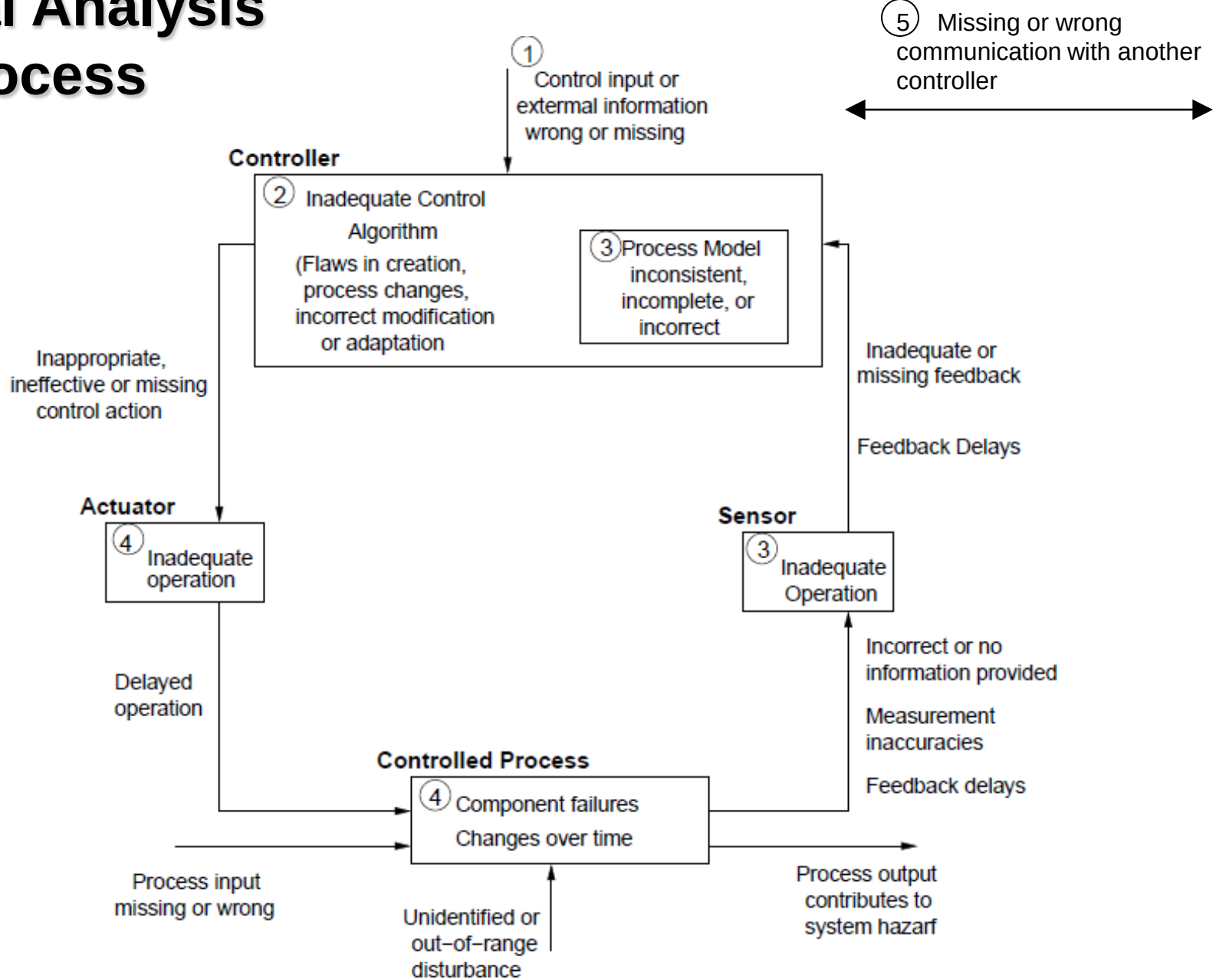
Example High-Level Control Structure for ITP



STPA
(System-Theoretic Process Analysis)

- Fault trees and event trees (used in safety analysis of ITP) limited in their power
  - Most developed 40 years ago for much simpler electromechanical devices and systems.
  - Do not work well for software and for cognitively complex human decision making (slips vs. mistakes).
- STPA is new hazard analysis method based on STAMP
  - Define hazards and safety control structure
  - Identify potential for unsafe control of system
    - Control action required for safety not provided
    - Unsafe control action is provided
    - Potentially safe action but too early/late/out of sequence
    - Safe action stopped too soon
  - Identify causal factors for inadequate control actions

Causal Analysis Process



Preliminary Research Results (1)

1. Analysis of current approach to certifying ITP (and other NextGen components)
   - Non-standard definition of hazard.
     - Equate it to a failure (i.e., reliability to safety). Defines hazard as an event when system is in a faulted mode.
     - Leads to identification of non-hazards such as controller rejecting a valid ITP maneuver as hazards.
   - Incomplete: Overlooks important scenarios (causes) leading to hazards
   - Uses techniques developed for nuclear power plants, but not appropriate for aviation. Aviation has much more complexity and different design approaches for safety than the process industry.

Analysis of current approach (Con't)

- Focuses on nominal events, not the off-nominal events and conditions that usually lead to accidents
- Assumes failure modes are independent
- Human error analysis incomplete (treated like a physical failure). Oversimplifies role of humans in accidents.

- Does not mean that ITP is unsafe! (lots of other activities going on to ensure safety)
  - This grant evaluating certification approach for NextGen procedures, not safe design of them
  - Same approach also applies to safe design of NextGen.

Preliminary Results (2)

2. Applying our approach to ITP
   - Identified inadequate control actions leading to a hazard.
     - Use to create safety requirements
     - Use as beginning point for hazard causal analysis
     - Found missing safety requirements for ITP
   - Performed STPA on most of the inadequate control actions
     - Causes can be used to create new safety requirements on ITP implementations
     - Using STPA, we found causes not handled by ITP specification and certification approach

System Hazards for Flight Ops

- H-1: Controlled aircraft violate minimum separation standards
- H-2: Aircraft enters unsafe atmospheric region
- H-3: Aircraft enters uncontrolled state
- H-4: Aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss)
- H-5: Aircraft enters a prohibited area
- H-6: New NextGen equipment interferes with other safety-critical systems

Inadequate Control Actions

Control Action	Not Given or Executed	Executed Incorrectly	Incorrect Timing/Order	Stopped Too Soon
ATC approves ITP request	Approval not given even if criteria are met	Approval given when criteria are not met Approval given to incorrect A/C	Approval given too early Approval given too late	Message transmittal stopped too soon
ATC denies ITP request	ITP criteria not met but denial not given	Denial given even when criteria are met	Denial given too early Denial given too late	
ATC gives abort instruction	Aircraft should abort but instruction not given	Abort instruction given when abort is not necessary	Abort instruction given too late	

Comparison to Current Method

1. Identification of high level unsafe control actions that could lead to a hazardous state

   Examples of unsafe control actions related to inadequate ITP Flight Crew execution of ITP procedure

Unsafe (Hazardous) Control Action	DO-312	STPA
Execution of an ITP when not compliant with ITP Criteria	X	X
Execution of an ITP when not approved by ATC		X
ITP executed too soon, before approval		X
ITP executed too long after approval		X
ITP maneuver not completed	X	X

Comparison to Current Method (2)

2. Unsafe control actions and causal analysis are used to generate certification requirements (currently incomplete)

Safety Operational Requirements during Execution (DO-312)
SPR.9 The ITP flight crew shall maintain the required Mach number during the ITP maneuver.
SPR.10 During an ITP maneuver, the ITP flight crew shall not modify the ITP clearance based on the ITP Equipment.
SPR.11 If during an ITP maneuver the ITP flight crew detects that the climb/descent rate is not compliant, the crew shall attempt to rectify the deficiency.
SPR.12 If during an ITP maneuver, it is not possible to perform the ITP climb/descent, the ITP flight crew shall follow regional contingency procedures.
SPR.13 If the ITP flight crew detects a condition where the distance between the ITP and Reference Aircraft is reduced such that a significant reduction in safety or potential mid air collision is possible, the ITP flight crew shall follow regional contingency procedures.

Flight Crew - Execute ITP (Done Incorrectly)

Instruction from ATC,
Environmental data from ATC
Audio or other communication
from other A/C

Aircraft state to ATC,
Ownship a/c state or other comm
to other a/c,
ITP request,
Other flight request

Controller: Flight Crew

- Ownship climb/descend capability
- ITP Speed/Dist criteria
- Relative altitude criteria
- Position/velocity data quality criteria
- Similar track criteria

Algorithm

1. Assess whether ITP is appropriate
2. Check if ITP criteria are met
3. Reqest ITP
4. Receive ATC approval
5. Re-check criteria
6. Execute flight level change

SPR's focus on this part of control loop

SPR's miss interactions with other parts of the system

Execute command not given,
Executed when criteria not met,
Executed before ATC approval,
Executed too long after ATC approval,
Executed after explicit ATC denial

Different sources give conflicting information
Data presentation is confusing,
Data is inaccurate,
Accurate data but given too late
(latency in processing)

Actuator
ITP Aircraft controls
(Throttle, rudder,
FBW, etc)

:
l units, TCAS,
other flight
mentation
logical senses

Ref ADS-B,
TCAS,
other comm

And this part of control loop

Fly-by-wire gives incorrect
command to aircraft,
Confusion between modes
(manual versus automatic,
e.g. pitot tube icing)

Controlled Proces
- Change flight lev
- Perform other fli
manuevers

And this part of control loop

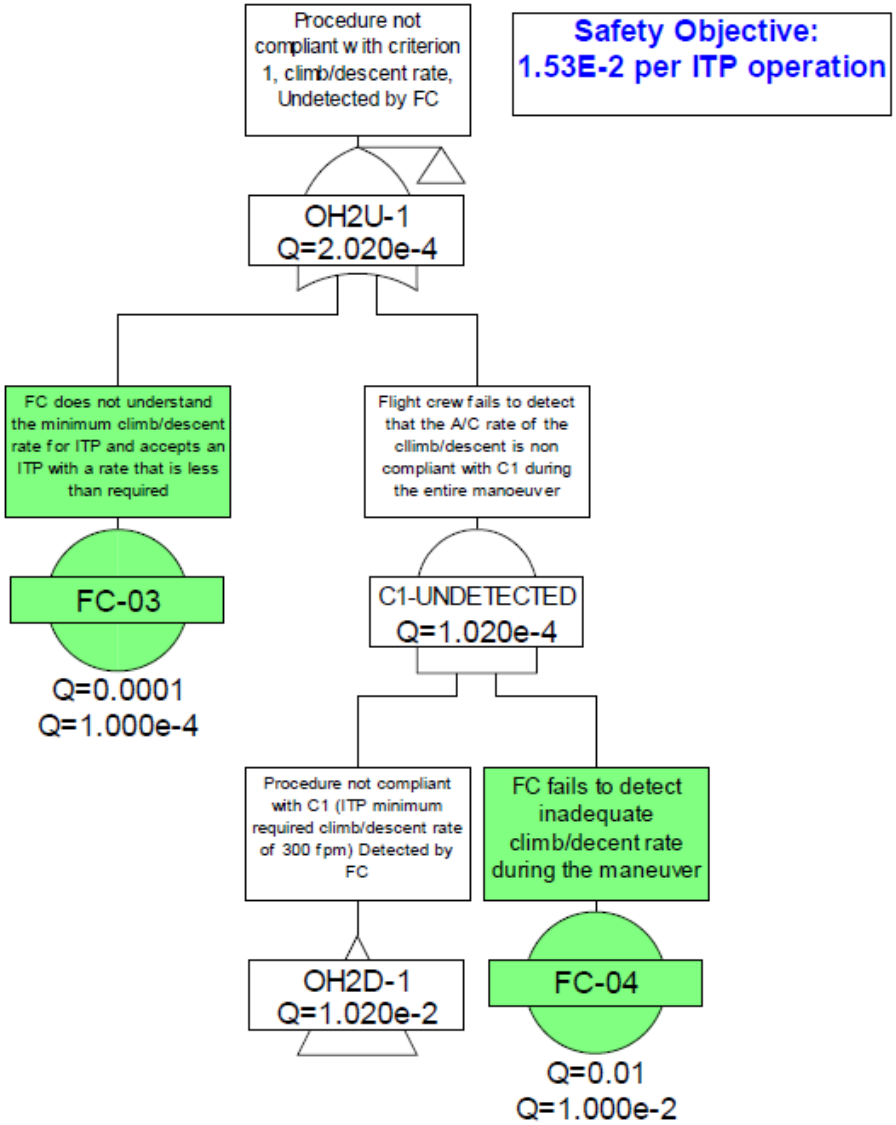
FLC takes too long,
A/C performs
maneuver incorrectly,
/C does not meet climb
rate requirements

External signals,
environment

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Comparison to Current Method (2)

- DO-312 begins with Operational Hazards (which are actually basic causes)
  - Then identify chains-of-events (fault trees) that could lead to basic causes
  - Each set of events is assigned a quantitative safety objective
- Human factors
  - Assigned probability of error
  - Provides little accounting for why errors may occur



Conclusions

- Current approach to certifying safety in NextGen is seriously flawed
- Extensions to approach used for TCAS would be more effective using
  - Extended accident causality model
  - New, more powerful hazard analysis techniques
  - Executable and analyzable intent specifications
- We will:
  - Demonstrate this on ITP
  - Document and evaluate an alternative method for certifying safety of NextGen additions to ATM system.