CAST Tutorial
Causal Analysis using System Theory

STAMP approach to accident analysis

STAMP Workshop

March 26, 2013

MIT Portugal

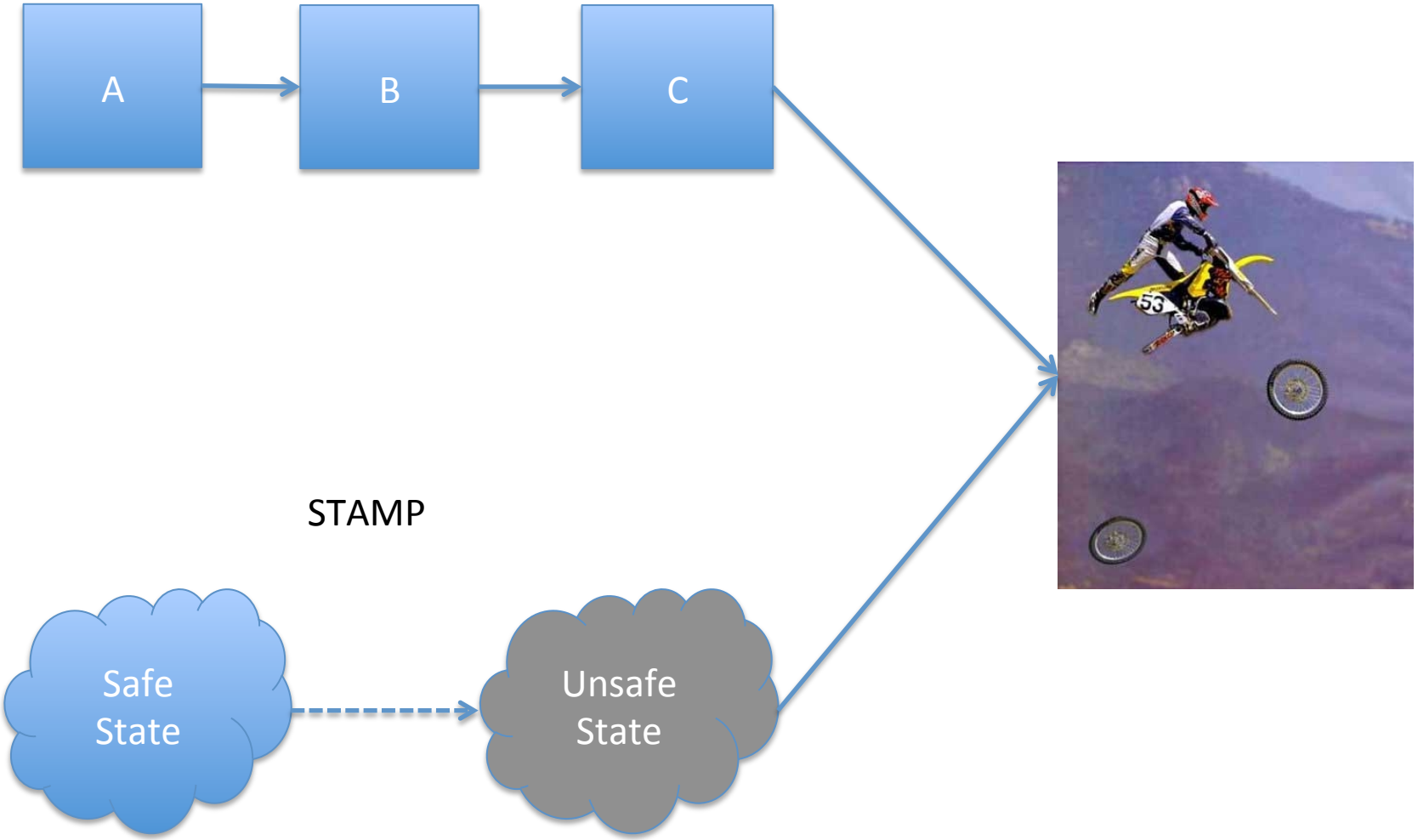
Akamai

CAST Tutorial

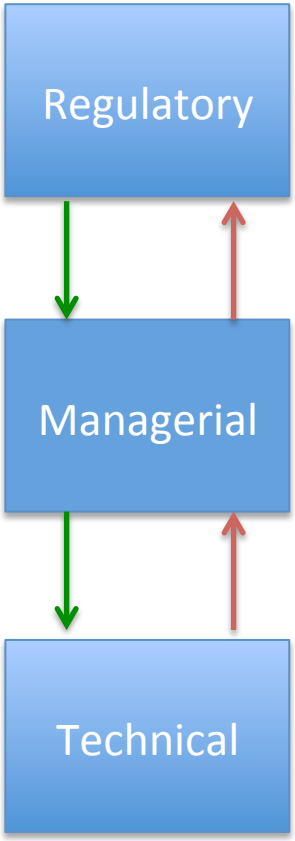
- Intro to STAMP
- Intro to CAST
- Work an example
- Discussion

Chain of Events

Models of Accident Causation



Model and Method: Why STAMP and CAST?



STAMP: Accident Causation Model

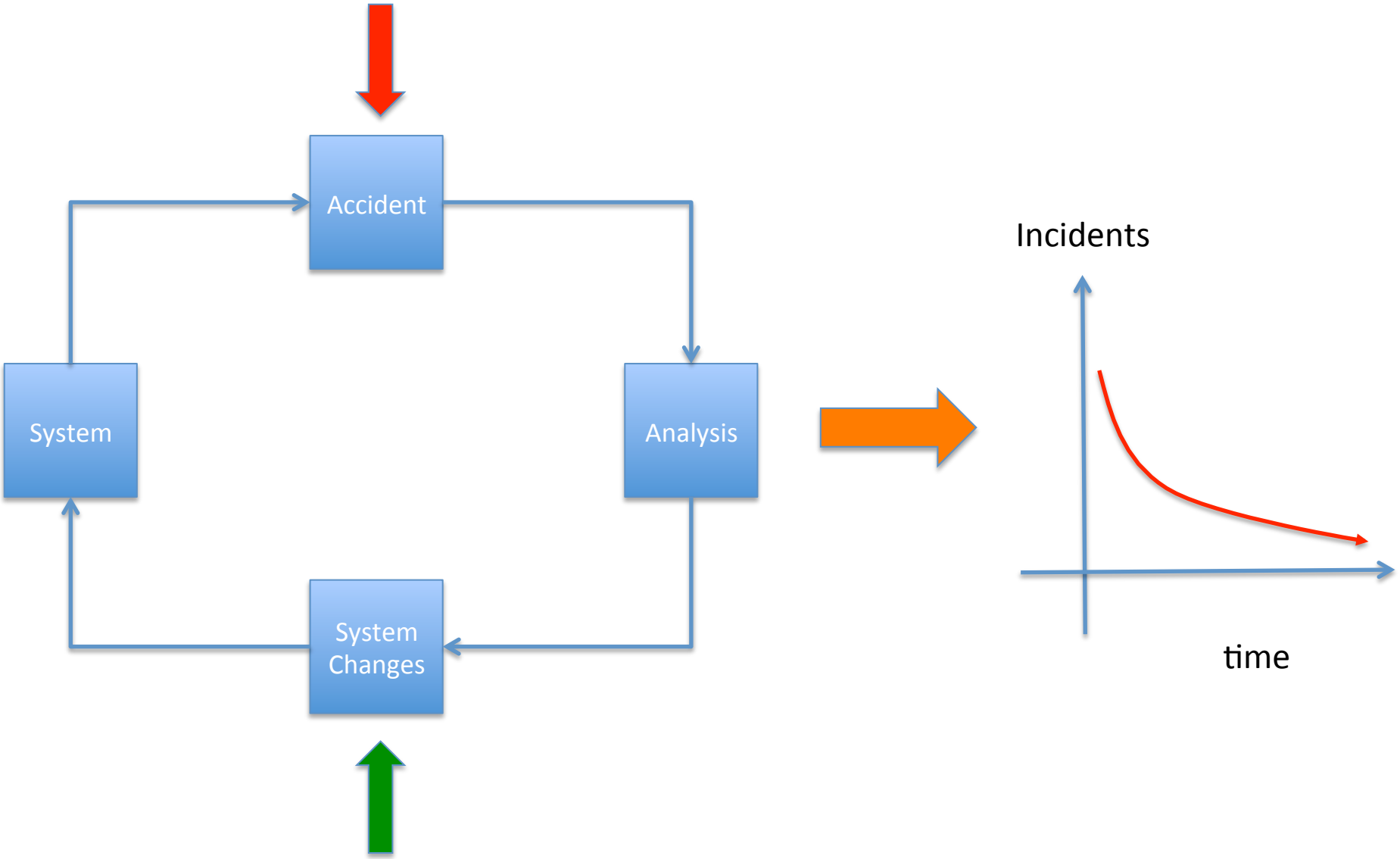
Accidents arise from complex, dynamic processes, not linear chain of events

Accidents are a control problem, not a failure problem

Accidents prevented by enforcing constraints on component behavior and interactions

Leveson (2004, 2011), After Fleming (2013)

Why do Accident Analysis?



Goals for an Accident Analysis Technique

- Provide a framework or process to assist in understanding entire accident process and identifying systemic factors
- Get away from blame ("who") and shift focus to "why" and how to prevent in the future
- Goal is to determine
  - Why people behaved the way they did
  - Weaknesses in the safety control structure that allowed the loss to occur
- Minimize hindsight bias

Hindsight Bias

- After an incident
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided

"shoulda, coulda, woulda"

Overcoming Hindsight Bias

- Nobody comes to work to do a bad job.
  - Assume were doing reasonable things given the complexities, dilemmas, tradeoffs, and uncertainty surrounding them.
  - Simply finding and highlighting people's mistakes explains nothing.
  - Saying what did not do or what should have done does not explain why they did what they did.
- Investigation reports should explain
  - Why it made sense for people to do what they did rather than judging them for what they allegedly did wrong and
  - What changes will reduce likelihood of happening again

CAST

1. Identify system hazard violated and the system safety design constraints
2. Construct the safety control structure as it was designed to work
    1. Component responsibilities (requirements)
    2. Control actions and feedback loops
3. For each component, determine if it fulfilled its responsibilities or provided inadequate control.
    1. Context
    2. Process Model Flaws

CAST (2)

4. Examine coordination and communication

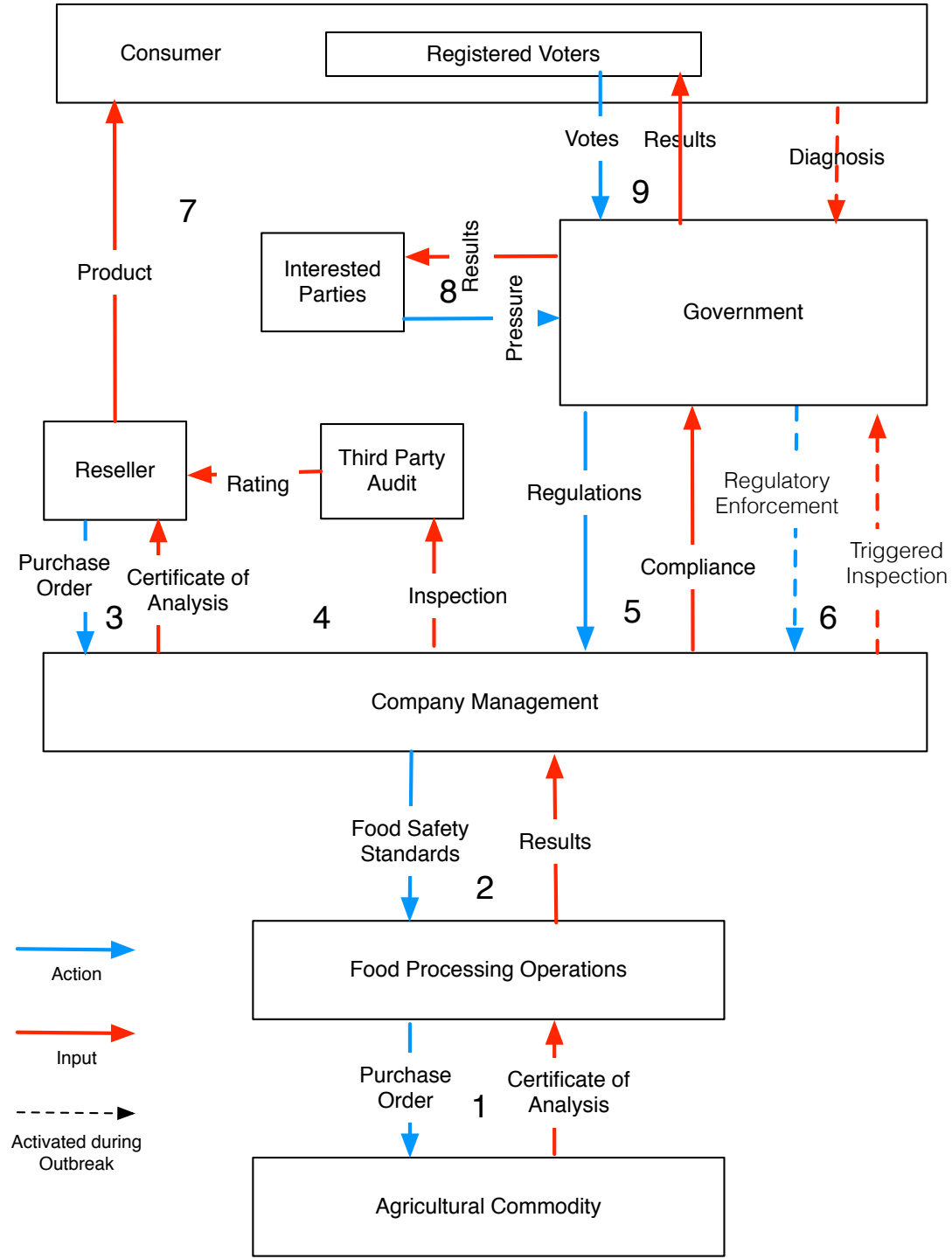
5. Consider dynamics and migration to higher risk

6. Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.

7. Generate recommendations

1. Identify system hazard violated and the system safety design constraints

Hazard	Safety Constraint	Safety Constraint Violated
Pathogenic Bacteria	No pathogenic bacteria in food at point of consumption	**35 *Salmonella enterica* serotype Typhimurium isolates were detected in 16 states by PulseNet**
Metal or other foreign object	No metal or other foreign objects > 1 mm in size	
Toxins	Aflatoxin < 20 ppb(FDA 2000)	



2. Construct the safety control structure as it was designed to work

- Component responsibilities (requirements)
- Control actions and feedback loops

3. For each component, determine if it fulfilled its responsibilities or provided inadequate control

Loop	Safety Resposibilities	Inadequate control action	Context in which decisions made	Process or Mental model flaws
2	Ensure building and equipment are maintained to prevent egress or growth of pathogens	Building had openings that allowed pests and rainwater to enter	No plant manager on site from April to Sep	?
3	Maintain adequate sanitation and pest control to prevent pathogens from entering the production environment	Pest control did not function, equipment not properly sanitized	No plant manager on site from April to Sep	?
7	No product is shipped to customers that contains pathogens	Product shipped that tested positive with a negative retest	Financial pressure Action had been taken before without negative consequences	OK to ship product on negative retest
8	No product is shipped to customers that contains pathogens	Certificate of analysis did not reflect positive salmonella test	Financial pressure Action had been taken before without negative consequences	OK to ship product on negative retest Cannot afford to scrap product when contamination is in question

CAST (2)

4. Examine coordination and communication

5. Consider dynamics and migration to higher risk

6. Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.

7. Generate recommendations

CAST Exercise

1) Choose an accident you are familiar with to analyze using CAST
2) Determine the proximate events in the actual accident you chose
3) Identify the system hazard violated and the system-level safety constraints
4) Construct the safety control structure as it was designed to work
    a) Identify the major controllers and other components
    b) Identify the roles and responsibilities for each controller
    c) Draw the control structure around the components
    d) Label the possible control actions for each controller
    e) Label the possible feedback information for each controller

Choose a controller to analyze further:

1) Identify inadequate control actions that violated safety-related responsibilities
2) Identify any process model flaws that contributed to inadequate control
3) Identify other contextual factors that contributed to inadequate control

Simmons Airlines/American Eagle Flight 3641

Outline

- Proximal Even Chain and Accident Report Summary
- CAST

Flight Summary

- Saab 340B with 2 pilots, 1 flight attendant, 23 passengers
- Departed Dallas/Fort Worth International (DFW) -> Baton Rouge Airport (BTR) 2140 CST 01FEB1994 in VMC conditions
- Emergency deadstick (Engine out) landing at False River Air Park, New Roads, LA
- Significant damage to aircraft
- 0 fatalities, 1 minor injury
- Cited cause of the accident:
  - Double flameout due to engine operation in the beta range

Flight Summary Ctd.

- Aircrew:
  - Captain: Flying Pilot. >20,000 hrs total; 300 in Saab 340. Transitioned from Jetstream 31 and Shorts 360 <1 yr earlier
  - First Officer: Monitoring Pilot. 6,500 hrs total; 1,700 in Saab 340. Qualified as Saab 340 Captain. Acted as Captain for 2 flights earlier that day
  - Flight attendant finished flight attendant training 8 months prior
- VMC conditions
- Expected to arrive within 5 mins of scheduled time.

Saab 340B

- Regional twin-engine turboprop (36 passengers)
- 413 in service used by 61 carriers in 30 countries
- Powerplant: 2 GE CT7-9B 1870 shp turboprops
- N349SB acquired in November 1993. 528.3 hrs on the aircraft with last inspection at 399.6 hrs. Preventive service check performed the morning of the accident at 516.8 hrs
- Engines new at purchase

Flight Narrative

- Houston ATC cleared to descend from FL 220 to 11,000 ft.
- On descent, overspeed warning sounded for 13 seconds
- BTR ATIS information W: winds light and variable, runways 22R and 31 in use
- Slight confusion with VOR and ILS approach for 13 at BTR
- Switch to Baton Rouge Approach. Captain requested straight in approach to runway 13 (opposite active) to expedite arrival.

Flight Narrative

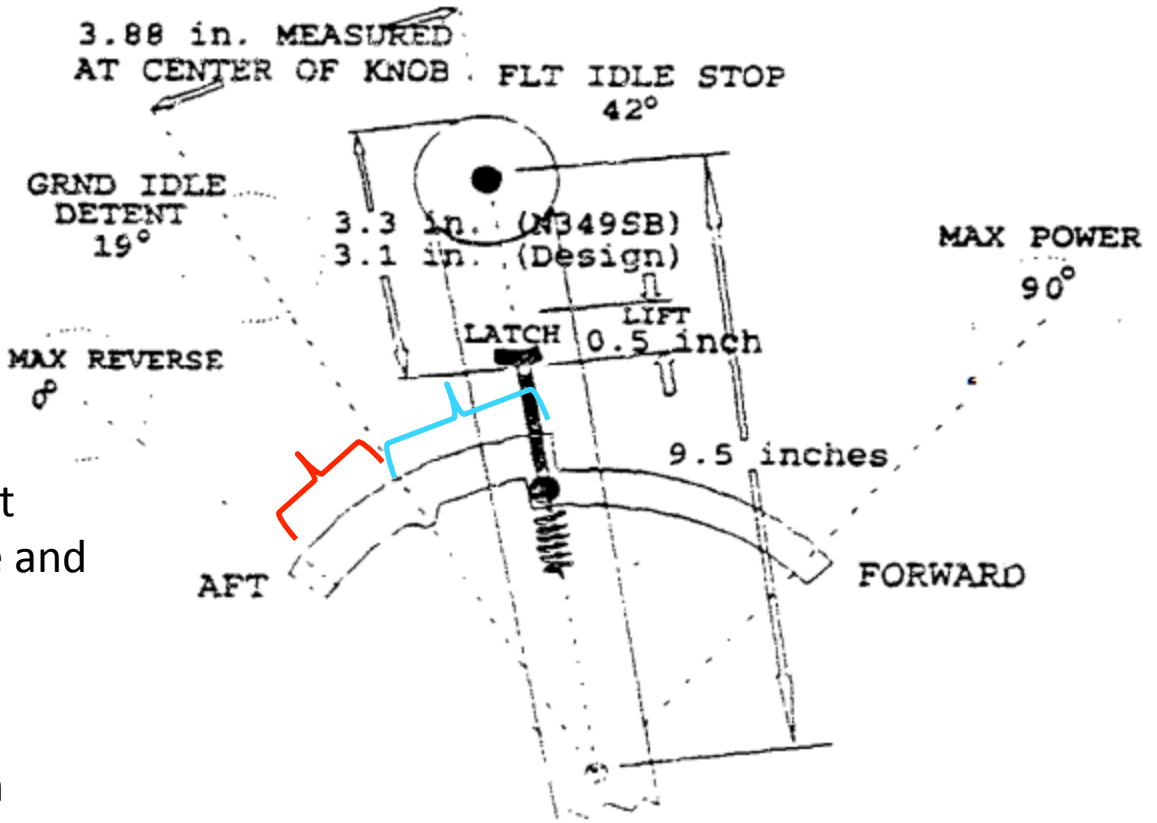
- High ground speed (tailwind at altitude) “Man, we’re almost the speed of heat here…” Throttles already at flight idle setting
  - Left Captain with little flexibility to slow aircraft without overshooting runway 13; “Maximum performance descent requiring the best flying technique from the crew to slow and descend the airplane.”
  - Reliant on experience and rules of thumb for touchdown and rollout calculations dependent on altitude, airspeed and winds
- Turbulence as descending from 12,000 to 10,000 requiring slowing
  - Too fast for gear or flaps
- Moved throttle into beta (ground operation only) range to increase drag.
  - Hit ground idle detent 8.5 s later.
  - Throttles stopped 4in aft of flight idle stop (slightly past ground idle detent and into thrust reversing region)

Saab 340B Throttle

Thrust reducing (flattening propeller pitch)

Thrust reversing (negative propeller pitch)

Throttle controls fuel flow in the flight mode up to 75%. In 75%-100% range and in ground operation (beta) range, it controls propeller pitch angle (beta). Turbine power section and propeller overspeed limiters are disabled when throttles are moved into beta range. Turbine power section connected to propeller through reduction gears.



NOTES:

1. Left latch movement began with 3.0 pounds of lift and topped at 7.0 pounds.
   Right latch movement began with 3.0 pounds of lift and topped at 5.5 pounds.
   Saab design calls for beginning of 2.5 pounds and 7.0 pounds at .5 inch lift.
2. Dimensions measured on N349SB and confirmed with Saab documents.

Flight Narrative

- CVR and FDR recorded propeller speed >1,500 RPM (max allowable 1,250)
- Throttle abruptly moved above flight idle stop
- Master Caution warning sounded 4 seconds after moved into thrust reversing

FO: “What happened?”

Captain: “What the [expletive]?”

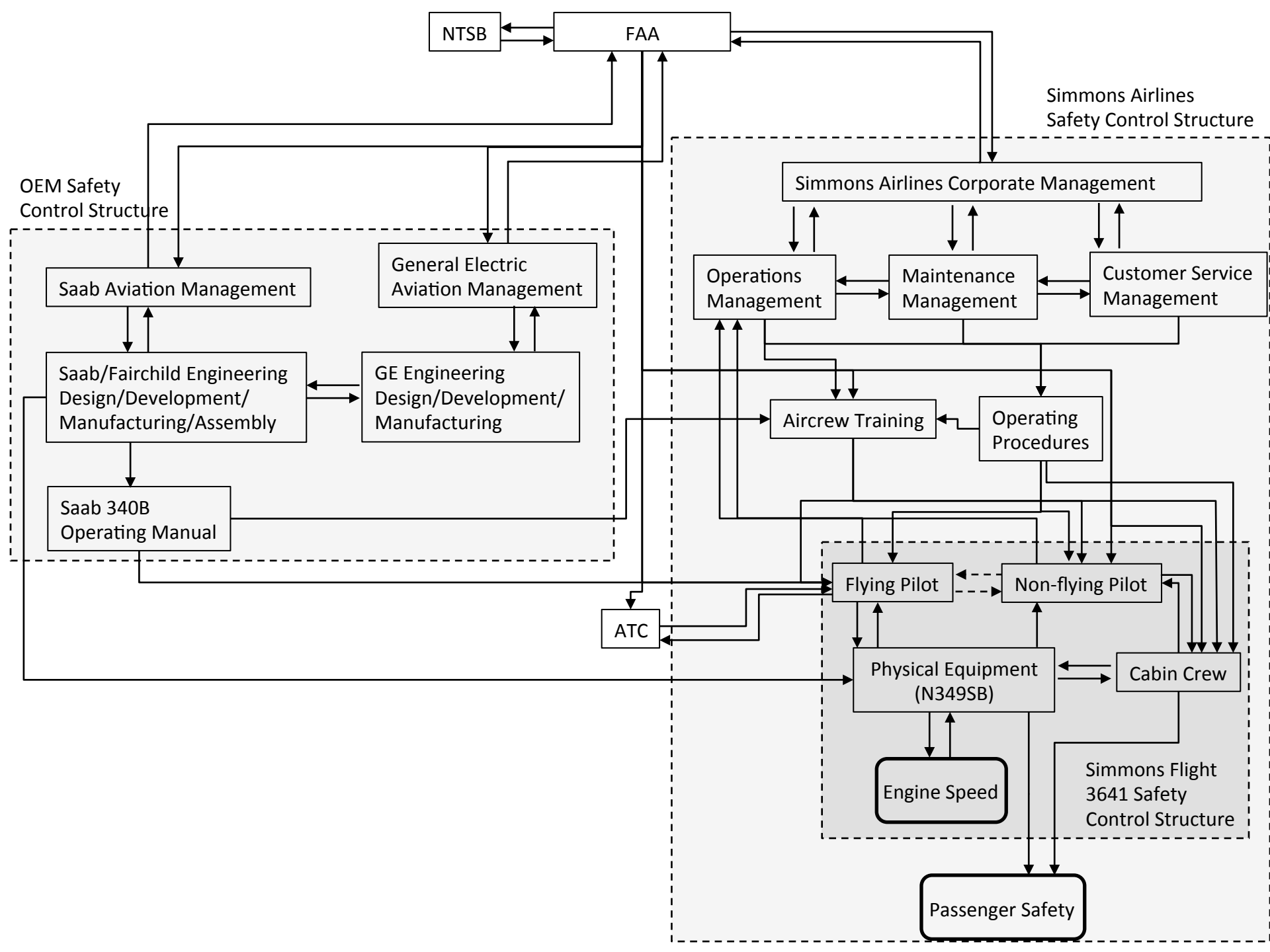
- Both engines flame out due to overspeed damage to turbine power section
- FO informs pilot that False River Air Park (lit 5000 ft runway) is directly below them
- Perform Engine Failure checklist while pilot performs spiral descent to airpark. Restart attempts failed.
- FO gives passenger/flight attendant briefing on BTR ATC frequency, not cabin public address
- Landed fast and long. Bounced and skidded off runway with no brakes. Went through soft grass, over 25ft wide ditch, through chainlink and barbed wire fences, and came to rest in sugar cane field. $1.75 M in damage
- Flight attendant injured back while opening exit door

NTSB Causes and Recommendations

- NTSB assigned blame to the Captain for intentionally moving the throttles past the flight idle stops
  - Captain and FO did not recall intentional moving of throttle beyond flight idle stop
- NTSB reiterated several previous requests for positive lockout of throttle to prevent in-flight beta use
- Review of training manuals and procedures

Simmons 3641
CAST (Causal Analysis Based on STAMP)

"One goal of CAST is to get away from assigning blame and instead shift the focus to *why* the accident occurred and how to prevent similar losses in the future."
–Nancy Leveson, *Engineering a Safer* World, 349


NTSB
FAA
Simmons Airlines
Safety Control Structure
OEM Safety
Control Structure
Simmons Airlines Corporate Management
Saab Aviation Management
General Electric
Aviation Management
Operations
Management
Maintenance
Management
Customer Service
Management
Saab/Fairchild Engineering
Design/Development/
Manufacturing/Assembly
GE Engineering
Design/Development/
Manufacturing
Aircrew Training
Operating
Procedures
Saab 340B
Operating Manual
Flying Pilot
Non-flying Pilot
ATC
Physical Equipment
(N349SB)
Cabin Crew
Engine Speed
Simmons Flight
3641 Safety
Control Structure
Passenger Safety

Losses

- Damage to aircraft
- Damage to infrastructure
- Injury of passenger
- Damage to reputation of Airline

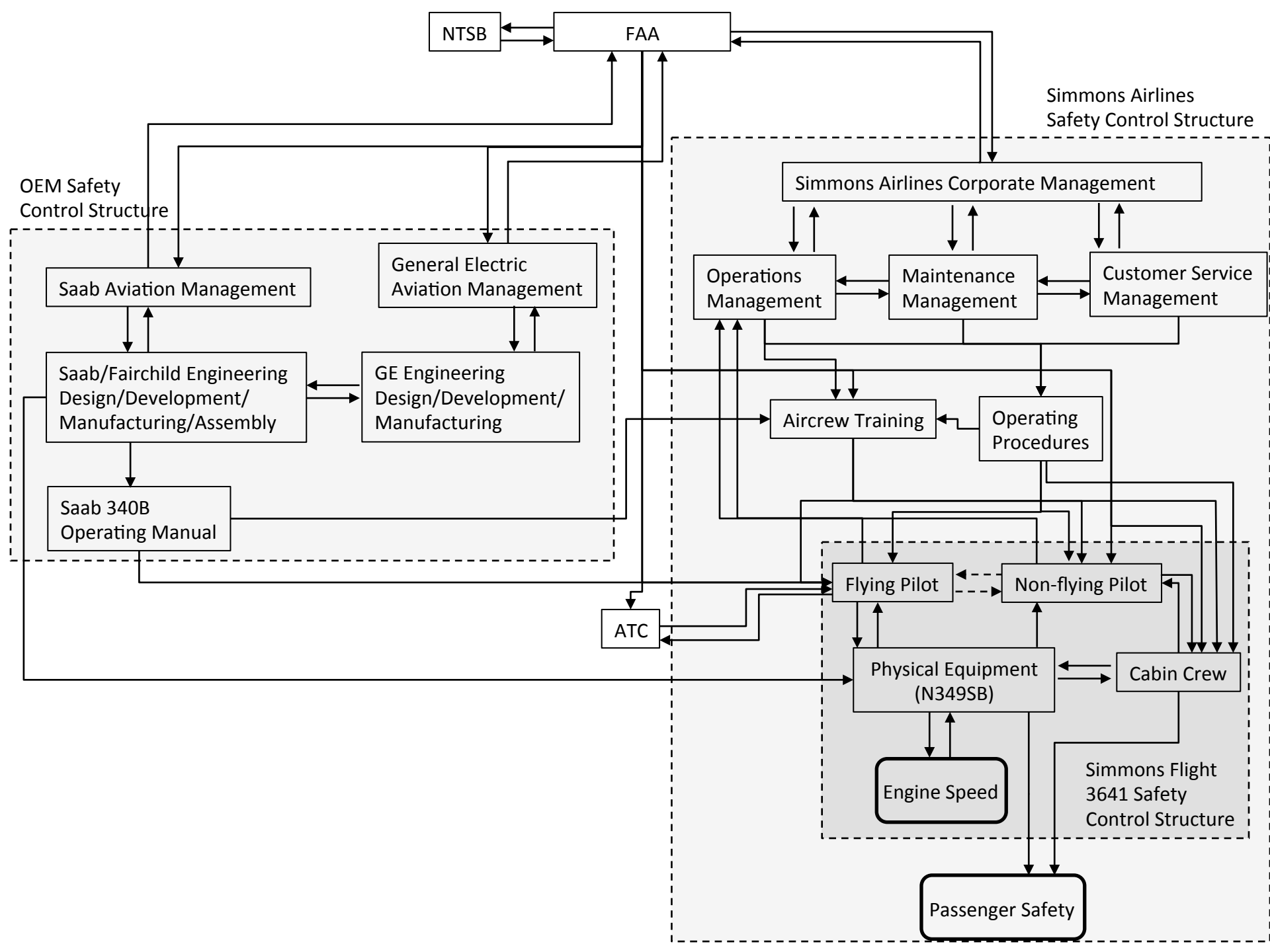
Hazards and System Constraints

Simmons Airlines Safety Control Structure- *Aircraft Damage, Passenger Discomfort, Reputation Damage*

- System level constraints:
  - *Aircraft must not be damaged*
  - *Passengers must be safe and comfortable at all times*
  - *Reputation of the airline must not be tarnished*

Simmons Flight 3641 Safety Control Structure- *Aircraft Damage* and *Passenger Injury*

- System level constraints:
  - *Must maintain ability to safely fly passengers to their desired location*
  - *Emergency procedures must be in place for loss of aircraft control*
  - *Passenger safety must be maintained in normal/non-normal/emergency operating conditions*


NTSB
FAA
Simmons Airlines
Safety Control Structure
OEM Safety
Control Structure
Simmons Airlines Corporate Management
Saab Aviation Management
General Electric
Aviation Management
Operations
Management
Maintenance
Management
Customer Service
Management
Saab/Fairchild Engineering
Design/Development/
Manufacturing/Assembly
GE Engineering
Design/Development/
Manufacturing
Aircrew Training
Operating
Procedures
Saab 340B
Operating Manual
Flying Pilot
Non-flying Pilot
ATC
Physical Equipment
(N349SB)
Cabin Crew
Engine Speed
Simmons Flight
3641 Safety
Control Structure
Passenger Safety

Physical Aircraft Safety Controls

Safety Requirements and Constraints Violated:

- Maintain ability to sustain flight
- Maintain ability to navigate
- Remain within aircraft operating limitations
- Inform passengers of emergency state and procedures
- Execute emergency procedures
- Safely egress

Emergency and Safety Equipment (Controls) Partial List:

- Engine RPM indicator
- Throttle flight Idle stops
- Throttle thrust reverse detent
- Beta range visual indicator
- Airspeed aural warning
- Airspeed visual warning (airspeed indicator)
- Passenger/crew restraint systems
- Aircrew emergency procedure training
- Passenger emergency procedure preflight brief
- Passenger emergency egress procedure card
- Emergency procedure checklists
- Emergency gear lowering

Physical Aircraft Safety Controls Ctd.

Failures and Inadequate Controls

- Inadequate navigation tools to maintain crew situational awareness
- Inadequate information concerning conditions at altitude (tailwind and turbulence)
- Inadequate indication of aircraft performance limitations
- Inadequate airspeed controls
- Inadequate protection against operating in beta range
- No protection against engine overspeed in beta range
- Inadequate indication of engine operating state (beta range)
- Inadequate crew warning for engine overspeed: No warning, only indicator
- Inadequate specificity with Master Caution warning system
- Failure to effectively execute an engine out landing
- Inadequate cabin crew execution of egress procedures
- Inadequate communication of emergency status and procedures to cabin crew/passengers
- No Emergency Brakes

Physical Contextual Factors

- 528.3 hrs on the aircraft with last inspection at 399.6 hrs. Preventive service check performed the morning of the accident at 516.8 hrs
- Engines new at purchase
- No Minimum Equipment List (MEL) or other discrepancies at dispatch
- Propeller is directly connected to the turbine section through a reduction gear box
- Propeller/turbine governors only effective in flight range

Middle Management Level Analysis

- Operations Manager
  - Safety Related Responsibilities
    - Develop company operating procedures that ensure safety
    - Provide aircrew training on safety
    - Update operations procedures to meet FAA Part 121 requirements
  - Context
    - Under pressure to ensure efficiency: Minimize delays and minimize expenses
    - All operating procedures must meet or exceed FAA Part 121 requirements
  - Unsafe control actions
    - Pressure pilots to minimize delays
    - Pressure pilots to avoid missed approaches (company policy?)
    - Not requiring engine out landing training
  - Process Model Flaws
    - Focused on efficiency
    - Little feedback from aircrews on safety
    - Assumption that compliance with FAA regulations ensures safety

Middle Management Level Analysis Ctd.

- Pilots
  - Safety Related Responsibilities
    - Maintain safe flight
    - Follow emergency procedures
    - Report equipment discrepancies
    - Report safety hazards?
    - Challenge other pilot on checklists/decisions
  - Context
    - Highly Experienced
    - Pushed to minimize delays/avoid missed approaches
    - Night
    - Don't question the Captain culture?
    - Beta used before with no consequences and operational benefit
  - Unsafe Decisions and Control Actions
    - Straight in landing requiring maximum performance descent at night
    - Continuing approach with overspeed warning
    - Did not slip aircraft (passenger comfort?)
    - Moving throttle below flight idle stops?
    - Poorly executed deadstick landing
    - Neglecting to turn on emergency cabin lights
    - Emergency status and procedures not communicated to cabin crew/cabin (transmitted to BTR, not cabin crew)
  - Process model flaws
    - Believed could improve operational performance by using thrust reversing in flight and had not observed uncontrolled flight previously
    - Possible mode confusion –did not know operating in beta range
    - Believed could execute rapid descent
    - Did not consider winds aloft?
    - Thought broadcasting on cabin PA system

Middle Management Level Analysis Ctd.

- Cabin Crew
  - Safety Related Responsibilities
    - Maintain passenger safety and comfort
    - Brief passengers on egress procedures
    - Lead egress of passengers
  - Context
    - Inexperienced
    - Unsure of situation
    - Stressed?
    - Lower status than pilots
  - Unsafe Decisions and Control Actions
    - Did not inform pilots of observed hazardous engine events
    - Failure to inform cabin of impending emergency landing
    - Did not ask pilots of status (did not want to interrupt)
  - Process model flaws
    - Believed pilots would inform of emergency state
    - Thought should not interrupt/challenge pilots

Middle Management Level Analysis Ctd.

- Air Traffic Control
  - Safety Related Responsibilities
    - Maintain aircraft separation
    - Inform pilots of weather in area (ATIS) and PIREPs
    - Efficiently prioritize and move aircraft
    - Assist in emergency landings and procedures
  - Context
    - Winds light and variable at surface
    - Two runways in use
    - Pressured to expedite operations
    - Knew Simmons 3641 executing emergency landing
  - Unsafe Decisions and Control Actions
    - Did not inform crew that transmitted emergency landing brief to BTR, not cabin
    - Did not dedicate a controller to Simmons 3641 (necessary?)
  - Process model flaws
    - Believed Simmons 3641 could execute the straight in approach requested

Upper Management Level Analysis

- FAA
  - Safety Related Responsibilities
    - Registration of aircraft
    - Certification of aircraft airworthiness (FAR 23, 25) & operating manuals (operating under Part 121)
    - Issuing airworthiness directives
    - Certification of airline operating procedures
    - Certification of aircrew training
    - Certification of ATC training
    - Certification of maintenance
    - Checking compliance with regulations
  - Context
    - Issued airworthiness directive to have operating manuals prohibit beta use in flight after several crashes involving turboprop beta use in flight
    - Pressure to effectively handle safety issues in manner that will minimize costs to airlines/ manufacturers
  - Unsafe Decisions and Control Actions
    - Issued AD that emphasized information already in flight manuals. Added explanation, but insufficient and incorrect (Beta use did not cause immediate loss of control)
    - Deemed equipment changes not required for all turboprop types
    - Initial FAR 23.1155/25.1155 requirements insufficient for safe operation
  - Process model flaws
    - Acting slowly to address a known issue
    - Believed changes in operating procedures would be sufficient and treated required action to previous accidents as addressed and closed

Upper Management Level Analysis Ctd.

- NTSB
  - Safety Related Responsibilities
    - Accident investigation and recommendations
  - Context
    - Investigated several previous crashes involving turboprop beta use in flight
  - Unsafe Decisions and Control Actions
    - No confirmation of sufficient action on safety recommendations
  - Process model flaws
    - Only required to report accident causes and recommendations to FAA. No ability for oversight of FAA action on recommendations to ensure sufficient

Upper Management Level Analysis Ctd.

- Simmons Airlines/American Eagle
  - Safety Related Responsibilities
    - Train aircrew on aircraft operation and emergency procedures
    - Follow FAA regulations
    - Create safety culture
  - Context
    - Subsidiary of American Eagle
    - Stock price constant at ~$40/share (no indication of financial pressures)
  - Unsafe Decisions and Control Actions
    - Did not train aircrews in engine-out landings
    - Pressure aircrews to minimize delays
  - Process model flaws
    - Relied on FAA certification and inspections to ensure safe aircraft and safe operating procedures

Upper Management Level Analysis

- Saab/GE
  - Safety Related Responsibilities
    - Provide aircrew and passengers with safety restraints and emergency equipment
    - Minimize risk of operating in a hazardous state
    - When emergency/failures occur, ensure critical systems function
    - Provide aircraft operations manuals that include safety critical and emergency procedures
  - Context
    - 340B more powerful, longer range version of the 340A
    - 340B met requirements stipulated in FAR 23 and 25 by design
    - 340B sales slowing
  - Unsafe Decisions and Control Actions
    - Did not provide aircrew with sufficient means to slow aircraft
    - Did not provide sufficiently positive means of preventing beta use in flight
    - Designed engine speed controls in manner that makes them ineffective in beta
    - Did not design brakes to work in engine out scenario
  - Process model flaws
    - Relied on FAA certification requirements to stipulate necessary safety features

Recommendations

- Physical Equipment and Design
  - Add physical stops preventing pilots from moving throttles into beta range in flight
  - Improve salience of operating mode indicators
  - Retain engine speed governors while in beta range
  - Add airbrakes/spoilers
  - Improved navigation and performance capability indicators
  - Improved airport facilities status (NOTAM) transmission
  - Improved salience of engine overspeed warning
  - Emergency brakes
  - Alter repetitive actions that are common in one flight condition that are hazardous in another in order to remove habituated actions from creating safety risks

Recommendations Ctd.

- Upper Management
  - Establish a means for another agency (NTSB) to monitor and approve FAA actions concerning safety recommendations
  - Remove disincentives (if any) to make safe decisions (go-around/delay penalties)
  - Providing improved tool for feedback concerning operating procedures and equipment design to ensure operational workarounds are safe (remove overreliance on FAA safety certification)
  - Improve rationale for operations limitations in flight manuals
  - Address aircrew CRM and possible "Captain is always right" mentality. Improve discussion of decisions and challenge, then action. Plan continuation bias training
  - Address safety culture and company priorities. Safety first, then efficiency.
  - Provide refresher engine out training for aircrew
  - Emphasize information flow during emergency procedures

- Middle Management
  - Better communicate decisions and possible alternatives to crewmembers
  - Improve information flow and team mentality of flight crew
  - With Aircrew/ATC, reinforce the purpose of ATC is safety and mistakes should be admitted and corrected
  - Improve feedback concerning unsafe conditions (remove overreliance on FAA certification for safety)

References

- Dismukes, Key, Benjamin A. Berman, and Loukia D. Loukopoulos. “Chapter 16: Simmons.” *The Limits of Expertise: Rethinking Pilot Error and the Causes of Airline Accidents*. Aldershot: Ashgate, 2007. Print.
- Leveson, Nancy. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT, 2011. Print.
- NTSB:AAR 94/06. 27 Sep. 1994. Retrieved 20 Nov. 2011, from http://www.airdisaster.com/reports/ntsb/AAR94-06.pdf
- Saab, “Saab 340B/B*plus*.” Retreieved 20 November 2011, from http://www.saabaircraftleasing.com/prod/datasheets/340B_JAR.pdf
- “Saab 340.” *Wikipedia*. Retrieved 20 Nov. 2011, from <http://en.wikipedia.org/wiki/Saab_340>.