Aviation CAST Example

2026 STAMP Workshop

CAST Handbook

Rodrigo Rose

23 Mar 2026

Massachusetts Institute of Technology

http://sunnyday.mit.edu/CAST-Handbook.pdf

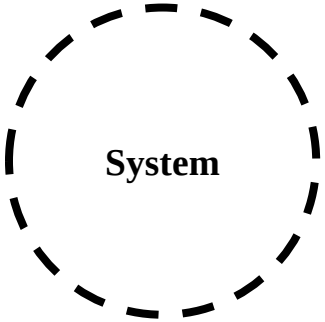
Disclaimer

This exercise is not meant to represent a complete analysis.
It is not meant to exhaustively demonstrate CAST.

This is not a training course.

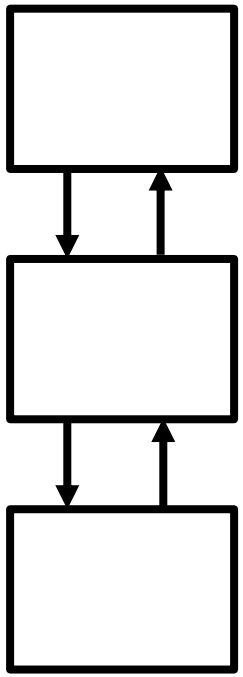
This simple exercise is only meant to quickly introduce some core concepts on a real-world example.

1. Assemble Basic Information → 2. Model Control Structure → 3. Analyze Each Component in a Loss → 4. Identify Control Structure Flaws → 5. Create Improvement Program



Environment

- **Accident**
- **Hazards**
- **Constraints**
- **Events**
- **Physical Loss**
- **Questions**



- **Contributions to accident**
- **Mental model flaws**
- **Context**
- **Questions**

- **Communication**
- **Coordination**
- **Safety Info System**
- **Culture**
- **Changes & Dynamics**
- **Economics**
- **Environment**
- **Questions**

- **Recommendations**
- **Implementation**
- **Feedback**
- **Follow-up**

1. Assemble Basic Information → 2. Model Control Structure → 3. Analyze Each Component in a Loss → 4. Identify Control Structure Flaws → 5. Create Improvement Program

Accident: Loss of TAM Linhas Aéreas Flight JJ3054

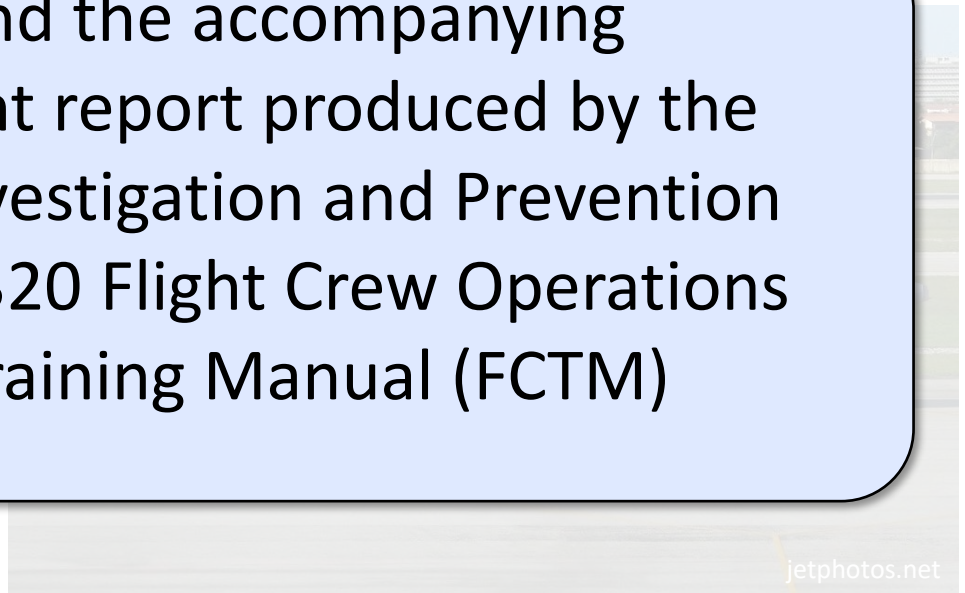
On 17 July 2007, at 18:54 local time, TAM Linhas Aéreas flight JJ3054, an Airbus A320, did not sufficiently decelerate upon landing at Congonhas (CGH) airport in São Paulo, Brazil, and overran the runway, crashing into a warehouse and claiming the lives of 199 people.



1. Assemble Basic Information → 2. Model Control Structure → 3. Analyze Each Component in a Loss → 4. Identify Control Structure Flaws → 5. Create Improvement Program

Accident: Loss of TAM Linhas Aéreas Flight JJ3054

On 17
Linha
A320
landi
Paulo
crashi
lives of 199 people.



The information in this example and the accompanying workbook comes from the accident report produced by the Brazilian Aeronautical Accident Investigation and Prevention Center (CENIPA) and the Airbus A320 Flight Crew Operations Manual (FCOM) and Flight Crew Training Manual (FCTM)



Accident: Loss of TAM Linhas Aéreas Flight JJ3054

System: Aircraft, crew, airport, airline/airport management, aircraft manufacturer regulatory bodies

Identify System Hazards:

- …
- …

Identify System Safety Constraints Violated:

System Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to a loss



Accident: Loss of TAM Linhas Aéreas Flight JJ3054

System: Aircraft, crew, airport, airline/airport management, aircraft manufacturer regulatory bodies

Identify System Hazards:

- H-1: Aircraft maneuvers out of approved airport zone
- H-2: Aircraft does not maintain adequate separation from undesired objects on the ground

Identify System Safety Constraints Violated:

System Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to a loss

1. Assemb
Informa

5. Create
nprovement
Program

Accident:

System: A
nufacturer
reg

Avoid common mistakes defining hazards:

- Define hazard at system level, not component level (ex: Aircraft ~~vs Engine~~)
- Avoid using word “fail” in hazards
- Refer to factors that can be controlled in design or operations
- Keep # of hazards small (no more than 7-10)
- Avoid ambiguous or recursive words (ex: “unsafe”, “accidental”)

Identify System Hazards:

- H-1: Aircraft maneuvers out of approved airport zone
- H-2: Aircraft does not maintain adequate separation from undesired objects on the ground

Identify System Safety Constraints Violated:

System Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to a loss



Accident: Loss of TAM Linhas Aéreas Flight JJ3054

System: Aircraft, crew, airport, airline/airport management, aircraft manufacturer regulatory bodies

Identify System Hazards:

- H-1: Aircraft maneuvers out of approved airport zone
- H-2: Aircraft does not maintain adequate separation from undesired objects on the ground

Identify System Safety Constraints Violated:

- SC-1: Aircraft must be able to come to a full stop before the end of the runway *[H-1]*
- SC-2: Aircraft must maintain separation standards from undesired objects on the ground *[H-2]*
- SC-3: If separation is not maintained, it must be detected and measures taken to prevent collision *[H-2]*

Goal: Figure out why the safety control structure did not do this



Analysis begins with the **physical process**

What inadequate controls allowed the **physical events** to occur?

Identify Physical Components:

- Aircraft systems – engines, thrust reversers, ground spoilers, brakes, wheels, cockpit interfaces/alarms
- Runway and airport infrastructure

Identify Failures:

- None

Identify Unsafe Interactions:

- Ground spoilers and brakes did not automatically deploy on touchdown
- Potential for hydroplaning on runway surface
- …

Identify Contextual Factors:

- Number 2 thrust reverser disabled for maintenance
- PR-MBK not fitted with alarm for when thrust lever positions were not in accordance with landing procedure

What questions are raised at this time that you would want to investigate?

Analysis

What in

Identify

- Aircraft systems – engines, thrust reversers, ground spoilers, brakes, wheels, cockpit interfaces/alarms
- Runway and airport infrastructure

Identify Failures:

- None

Identify Unsafe Interactions:

- Ground spoilers and brakes did not automatically deploy on touchdown
- Potential for hydroplaning on runway surface
- …

Identify Contextual Factors:

- Number 2 thrust reverser disabled for maintenance
- PR-MBK not fitted with alarm for when thrust lever positions were not in accordance with landing procedure



Potential Questions:

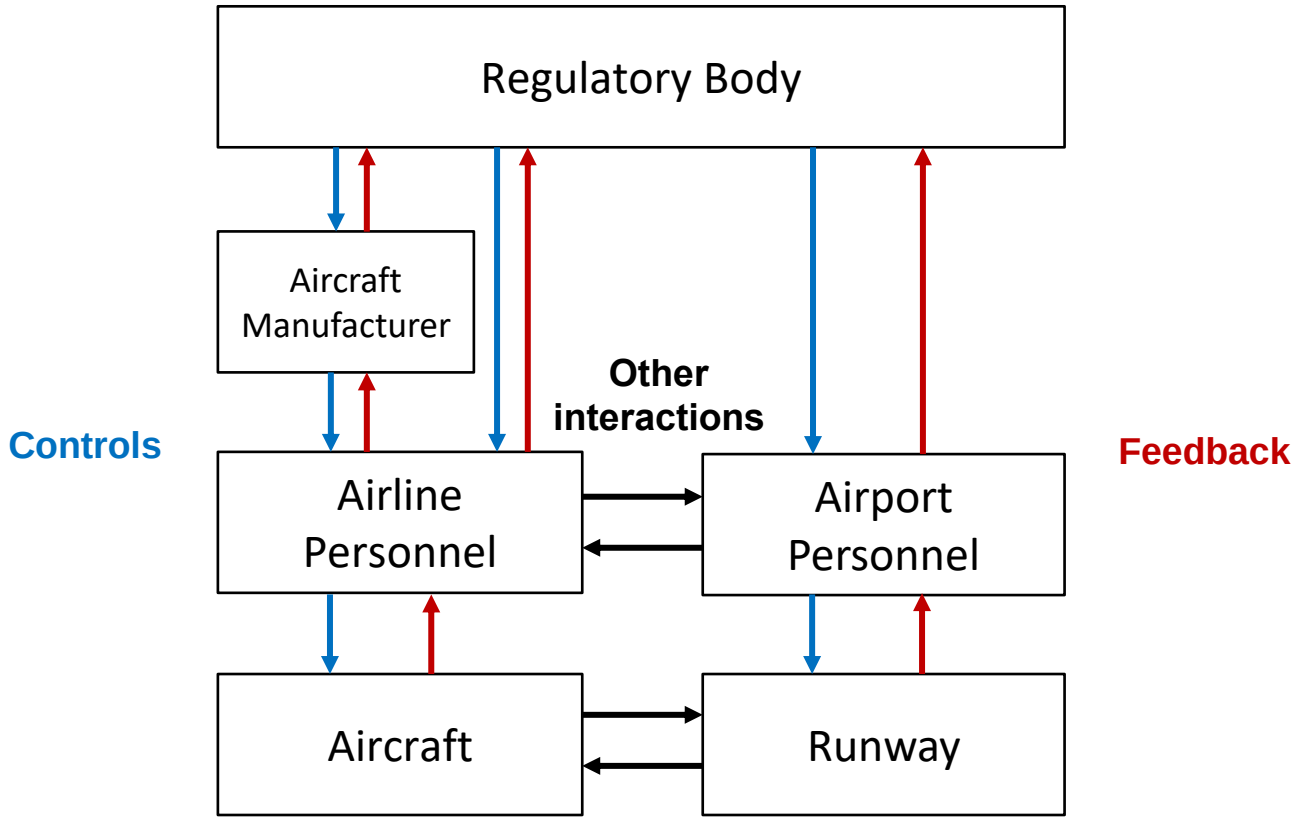
- Why did the auto-brake not automatically activate on touchdown?
- Why did the ground spoilers not automatically deploy on touchdown?
- What conditions allowed thrust reversers to deploy, but not other deceleration features?



It is helpful to start with a very **abstract**, **high-level** control structure that outlines the general controls for this type of event

Less important here than in STPA, but can help guide what specific components/ controllers you should consider investigating

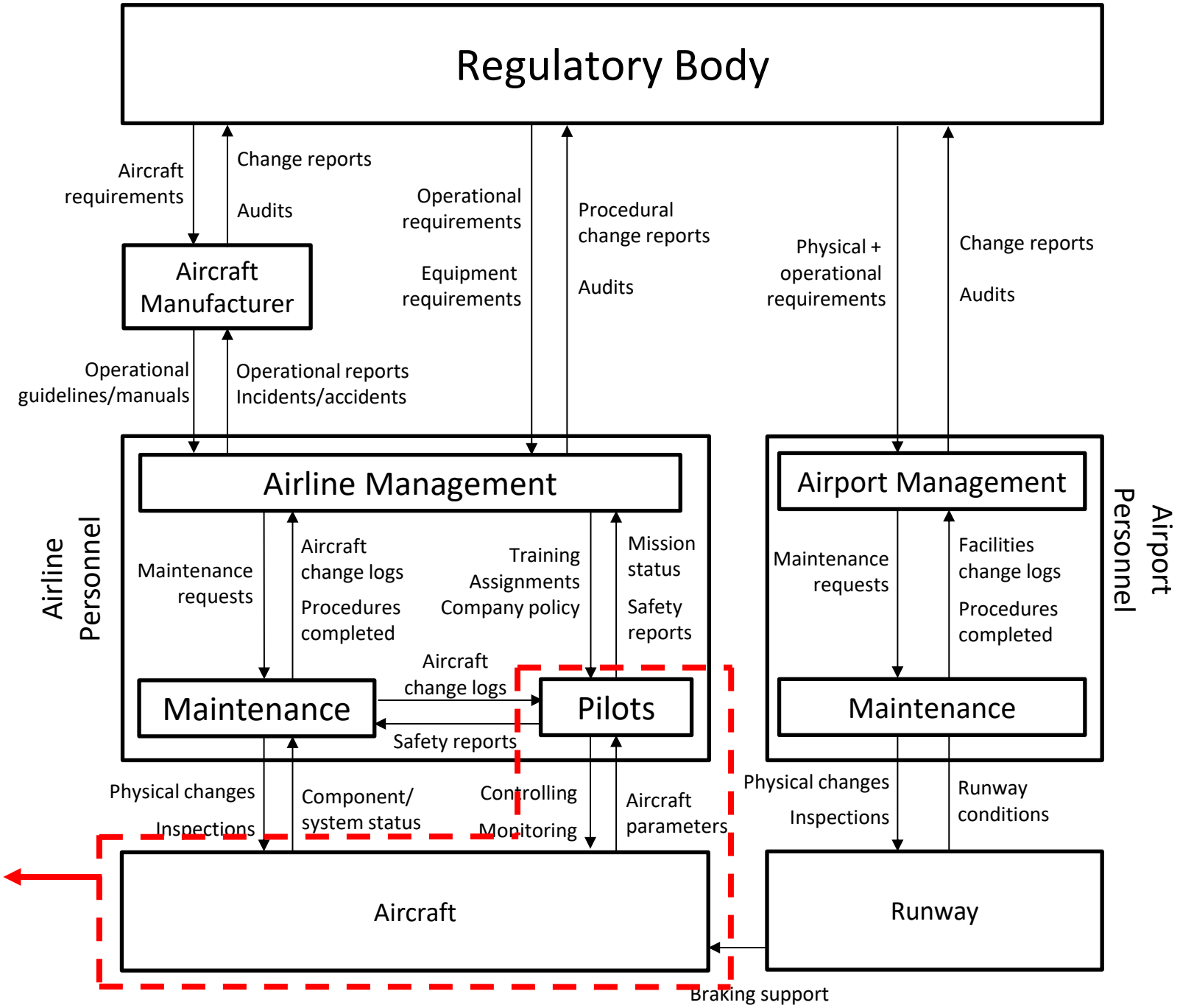
System: aircraft, crew, airport, airline/airport management, aircraft manufacturer regulatory bodies

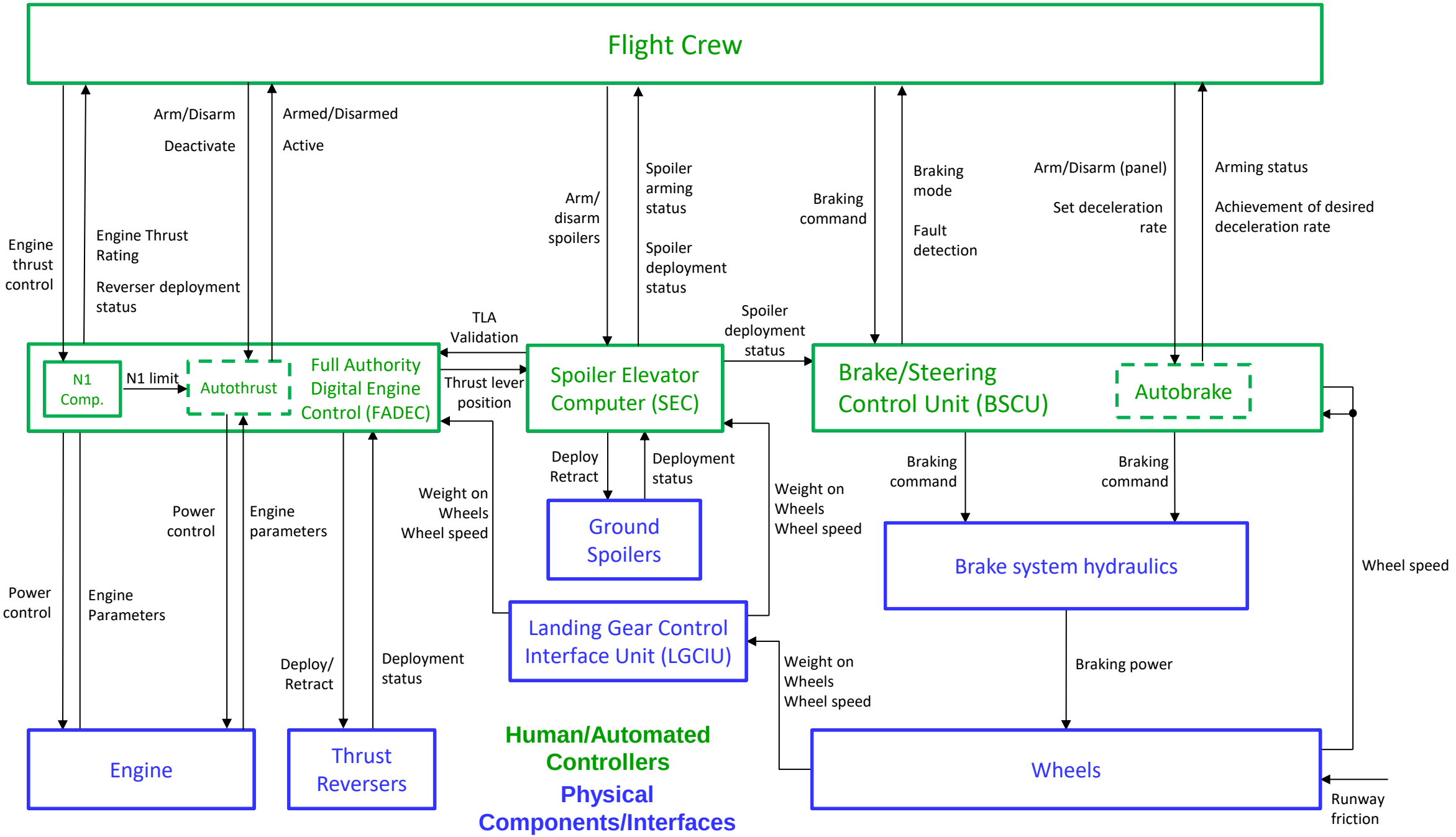


Control structure is **iteratively refined** as more information becomes available about the accident

If the control structure is not complete, that is **OK**

Further refinement to **physical systems** and **automated controllers**




Flight Crew
Arm/Disarm
Deactivate
Armed/Disarmed
Active
Engine thrust control
Engine Thrust Rating
Reverser deployment status
Arm/ disarm spoilers
Spoiler arming status
Spoiler deployment status
Braking command
Braking mode
Fault detection
Arm/Disarm (panel)
Set deceleration rate
Arming status
Achievement of desired deceleration rate
TLA Validation
Thrust lever position
Spoiler deployment status
N1 Comp.
N1 limit
Autothrust
Full Authority Digital Engine Control (FADEC)
Spoiler Elevator Computer (SEC)
Brake/Steering Control Unit (BSCU)
Autobrake
Deploy Retract
Deployment status
Braking command
Braking command
Power control
Engine parameters
Weight on Wheels Wheel speed
Ground Spoilers
Weight on Wheels Wheel speed
Brake system hydraulics
Wheel speed
Power control
Engine Parameters
Landing Gear Control Interface Unit (LGCIU)
Deploy/ Retract
Deployment status
Weight on Wheels Wheel speed
Braking power
Engine
Thrust Reversers
Wheels
Runway friction
Human/Automated Controllers
Physical Components/Interfaces



Control structure model is **not fixed** and will evolve as more is learned about the **accident** and about the **responsibilities** of each of the controllers

How does the analyst identify the responsibilities?

- Documentation (company manuals, government documents, etc.)
- Questioning human controllers about their own and others' responsibilities during the investigation
  - Confusion and inconsistencies here could be a clue as to why the accident occurred



Once the basic control structure and controls are identified, the next step is to show **why** the control structure (i.e., the current controls) did not prevent the accident

The goal

IS NOT

to assign blame to individuals or individual components

The goal

IS

to identify flaws in the control structure to understand why it made sense for controllers to act the way they did



There are several parts to the CAST analysis of each component:

Role the component played

- Component responsibilities related to the accident
- Component's contributions to the hazardous state (actions, lack of actions, etc.)

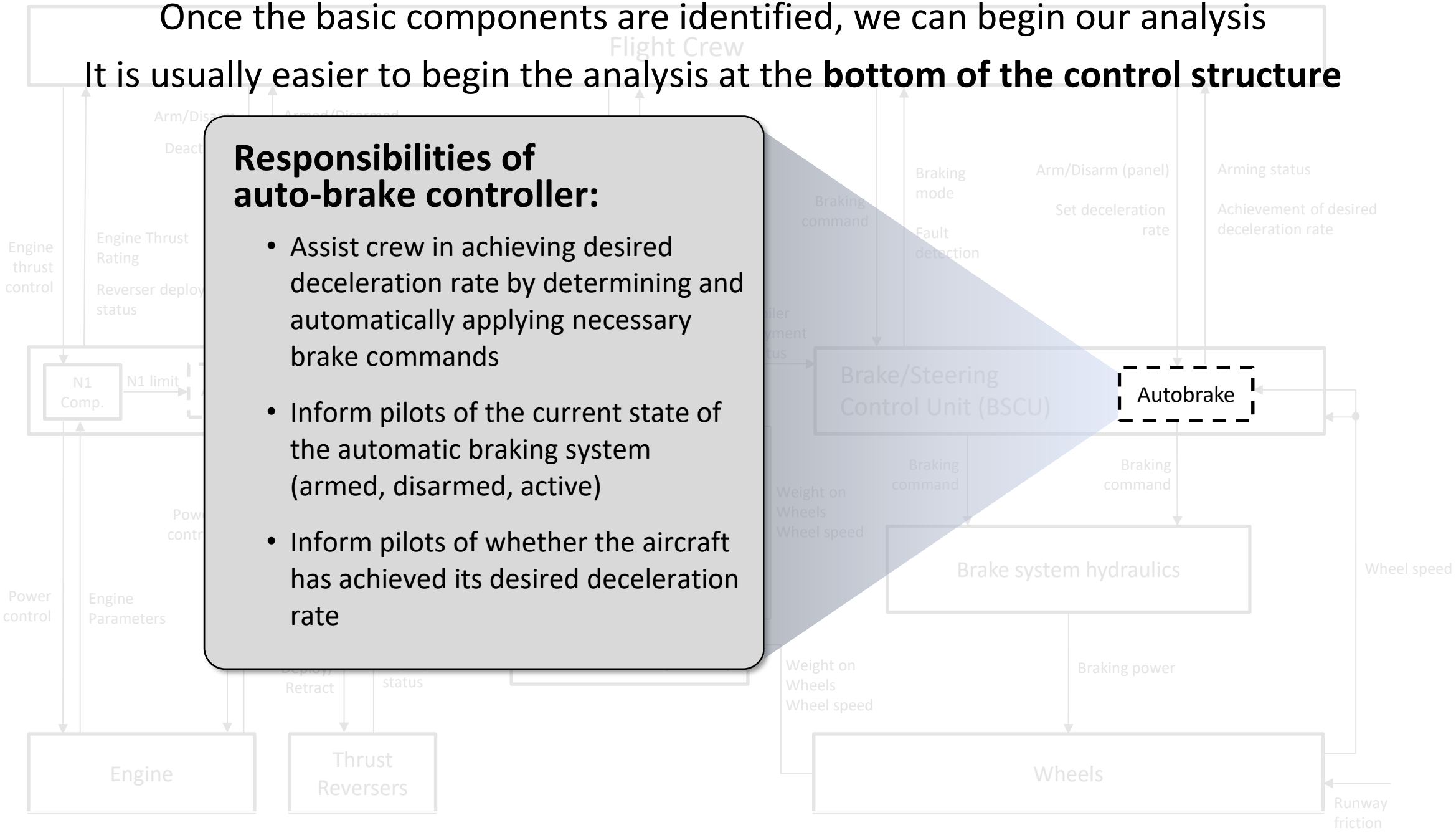
Why?

- Flaws in the mental/process model contributing to the action
- Contextual factors explaining the actions, decisions, and process model flaws

Questions to be answered later

Once the basic components are identified, we can begin our analysis

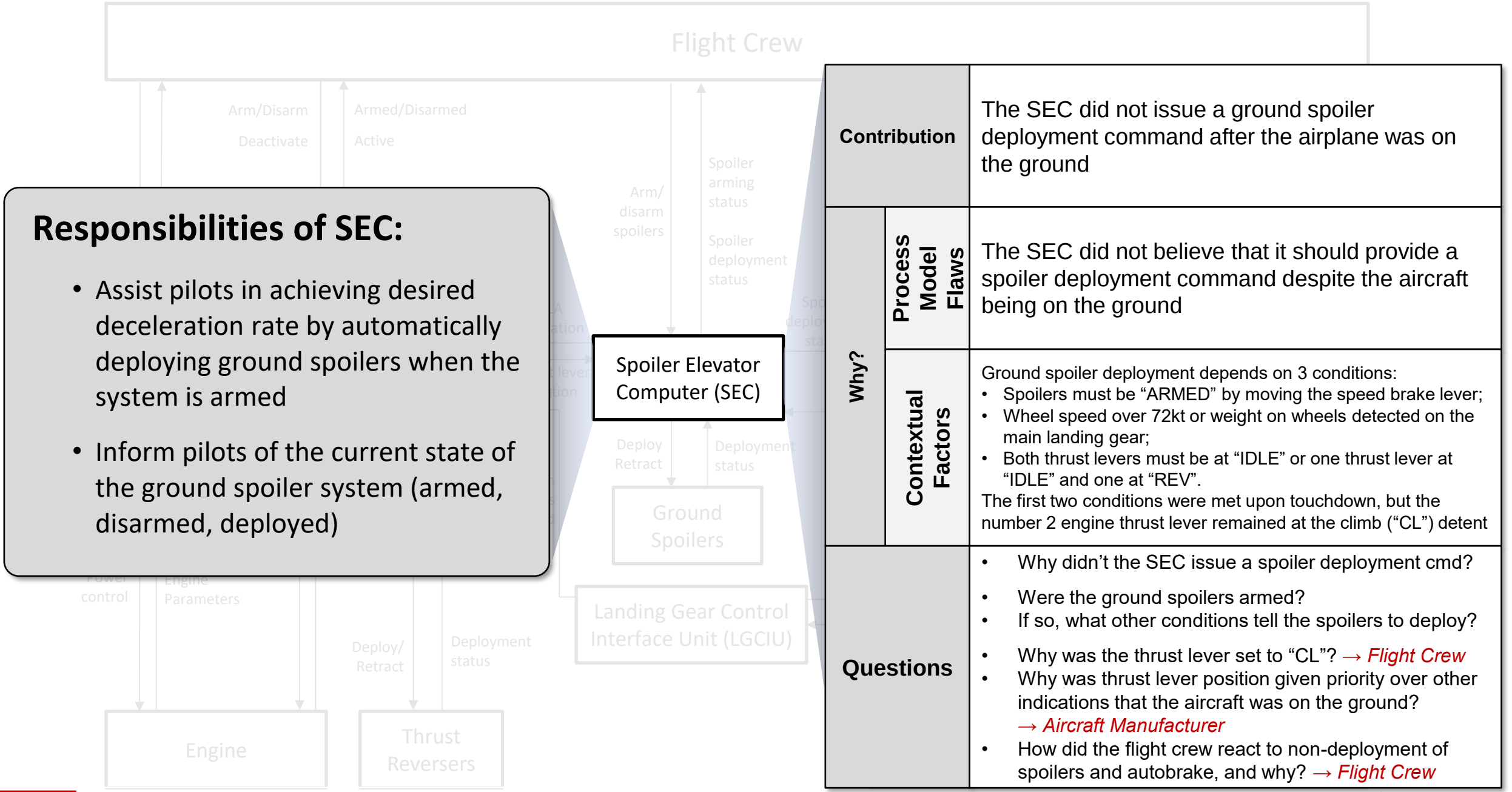
It is usually easier to begin the analysis at the **bottom of the control structure**



Responsibilities of auto-brake controller:

- Assist crew in achieving desired deceleration rate by determining and automatically applying necessary brake commands
- Inform pilots of the current state of the automatic braking system (armed, disarmed, active)
- Inform pilots of whether the aircraft has achieved its desired deceleration rate

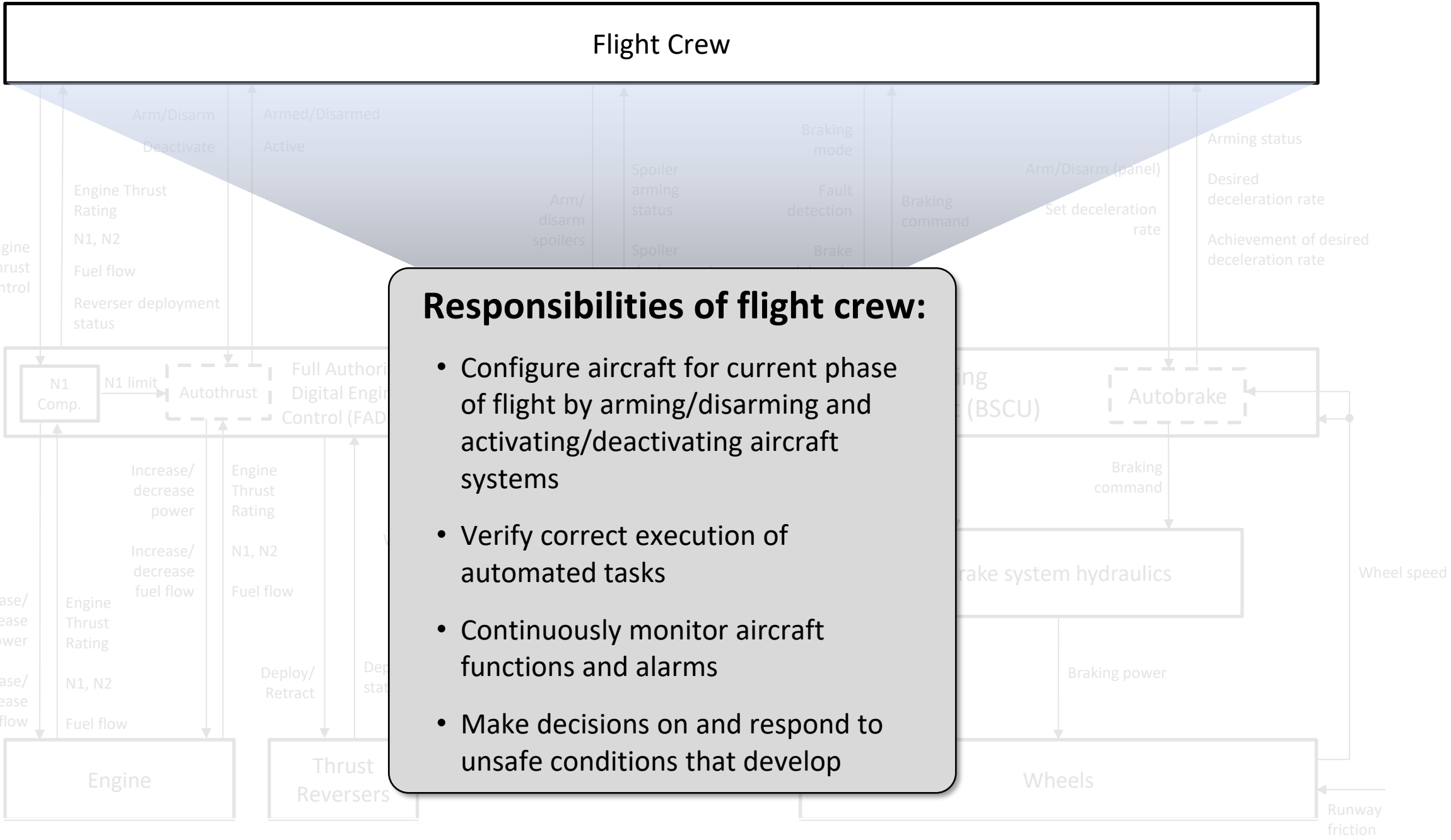
Contribution		The auto brake controller did not issue braking commands to the brake system hydraulics
Why?	**Process Model Flaws**	The auto brake controller did not believe it was in a situation where it should provide braking commands because conditions had not been met
	Contextual Factors	For autobrake to activate, it must be manually “ARMED” using the autobrake panel, subject to certain conditions. All conditions were met, so the system was armed. In LO and MED mode, the timing for autobrake activation is relative to ground spoiler deployment.
Questions		• Why did the autobrake controller not issue brake commands? • Was the auto brake armed at the time? • If so, what other conditions tell the auto brake to operate? • Why did the ground spoilers not deploy? → *SEC* • Why was the auto brake logic tied to ground spoiler activation? → *Aircraft Manufacturer*



Responsibilities of SEC:

- Assist pilots in achieving desired deceleration rate by automatically deploying ground spoilers when the system is armed
- Inform pilots of the current state of the ground spoiler system (armed, disarmed, deployed)

Contribution		The SEC did not issue a ground spoiler deployment command after the airplane was on the ground
Why?	**Process Model Flaws**	The SEC did not believe that it should provide a spoiler deployment command despite the aircraft being on the ground
	Contextual Factors	Ground spoiler deployment depends on 3 conditions: • Spoilers must be "ARMED" by moving the speed brake lever; • Wheel speed over 72kt or weight on wheels detected on the main landing gear; • Both thrust levers must be at "IDLE" or one thrust lever at "IDLE" and one at "REV". The first two conditions were met upon touchdown, but the number 2 engine thrust lever remained at the climb ("CL") detent
Questions		• Why didn't the SEC issue a spoiler deployment cmd? • Were the ground spoilers armed? • If so, what other conditions tell the spoilers to deploy? • Why was the thrust lever set to "CL"? → *Flight Crew* • Why was thrust lever position given priority over other indications that the aircraft was on the ground? → *Aircraft Manufacturer* • How did the flight crew react to non-deployment of spoilers and autobrake, and why? → *Flight Crew*



Responsibilities of flight crew:

- Configure aircraft for current phase of flight by arming/disarming and activating/deactivating aircraft systems
- Verify correct execution of automated tasks
- Continuously monitor aircraft functions and alarms
- Make decisions on and respond to unsafe conditions that develop

Flight Crew

Contribution		Upon hearing the “RETARD” command, pilot-in-charge (PIC) moved number 1 engine thrust lever to “IDLE” then “REV”, and left number 2 engine thrust lever at “CL”
Why?	**Process Model Flaws**	• PIC may have believed that the autothrust would automatically adjust the thrust rating on the number 2 engine without moving the thrust lever, but moving one lever to “REV” disengaged autothrust and locked the thrust on the number 2 engine • Cessation of the “RETARD” command would have indicated to PIC that levers were in the right position, an incorrect process model update
	Contextual Factors	• The old procedure for landing with just one thrust reverser required the pilot to first move both levers to “IDLE”, then move only one lever to “REV”. The new procedure required the pilot to move both thrust levers to “IDLE”, then both to “REV” • PIC had reported a minor headache earlier during the flight
Questions		• Why did the PIC not move the number 2 engine thrust lever to “IDLE” as well? • Were the pilots aware of the conditions for the “RETARD” command to shut off? → *Airline* • Why did the PIC select the old procedure for landing with just one thrust reverser? → *Crew*

Flight Crew

Contribution		PIC decided to perform a procedure not in accordance with the MMEL, which used to be a standard procedure but had since been replaced
Why?	**Process Model Flaws**	The PIC may have believed that performing the procedure in the MMEL (which would add at least 55m to the landing roll) would have been less safe, as it could have placed the plane at greater risk of overshooting the runway in the event of hydroplaning
	Contextual Factors	• PIC displayed anxiety with regards to wet runway conditions at Congonhas, as he directed the other pilot to contact ATC twice and ask about runway conditions • PIC knew of an accident the day before where a plane overshot runway 35L • PIC knew the aircraft was heavier than usual due to extra fuel brought from POA
Questions		• Why did the PIC select the old procedure for landing with just one thrust reverser? • Was the pilot aware of the reasons why the procedure was changed? → *Airline* • What kind of briefings had the pilots received on when to use either procedure? → *Airline* • How were the runway conditions at Congonhas? → *Airport Management/Maintenance* • Why did the pilots choose to go ahead with a landing they were anxious about? → *Crew*

Unanswered questions so far:

- How did the flight crew react to non-deployment of spoilers and autobrake, and why? → ***Flight Crew***
- Why did the pilots choose to go ahead with a landing they were anxious about? → ***Flight Crew***

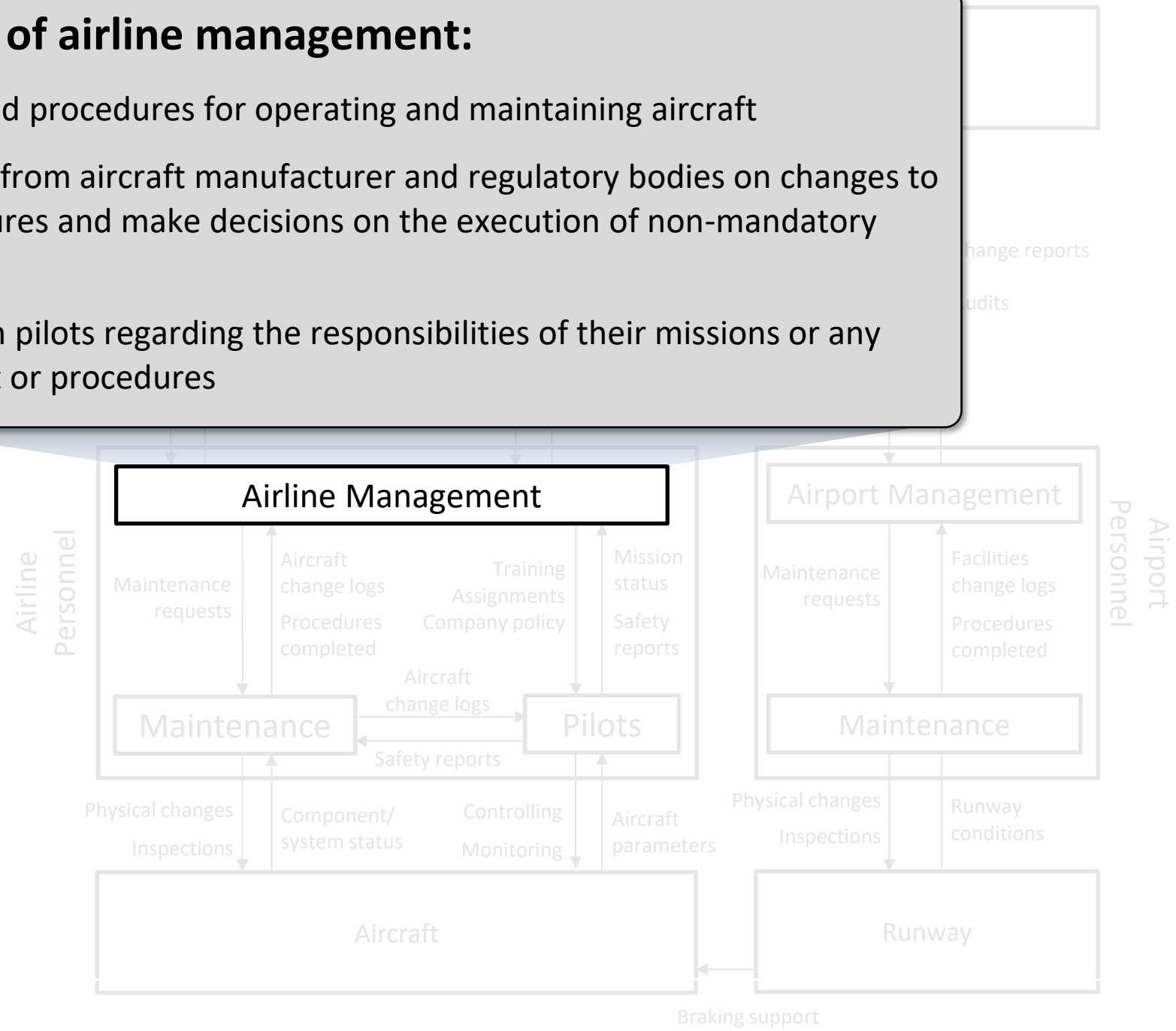
- Were the pilots aware of the conditions for the "RETARD" command to shut off? → ***Airline***
- Was the pilot aware of the reasons why the procedure was changed? → ***Airline***
- What kind of briefings had the pilots received on when to use either procedure? → ***Airline***

- How were the runway conditions at Congonhas? → ***Airport Management/Maintenance***

- Why was the auto brake logic tied to ground spoiler activation? → ***Aircraft Manufacturer***
- Why was thrust lever position given priority over other indications that the aircraft was on the ground for ground spoiler deployment? → ***Aircraft Manufacturer***

Responsibilities of airline management:

- Follow documented procedures for operating and maintaining aircraft
- Receive directives from aircraft manufacturer and regulatory bodies on changes to aircraft or procedures and make decisions on the execution of non-mandatory changes
- Communicate with pilots regarding the responsibilities of their missions or any changes to aircraft or procedures

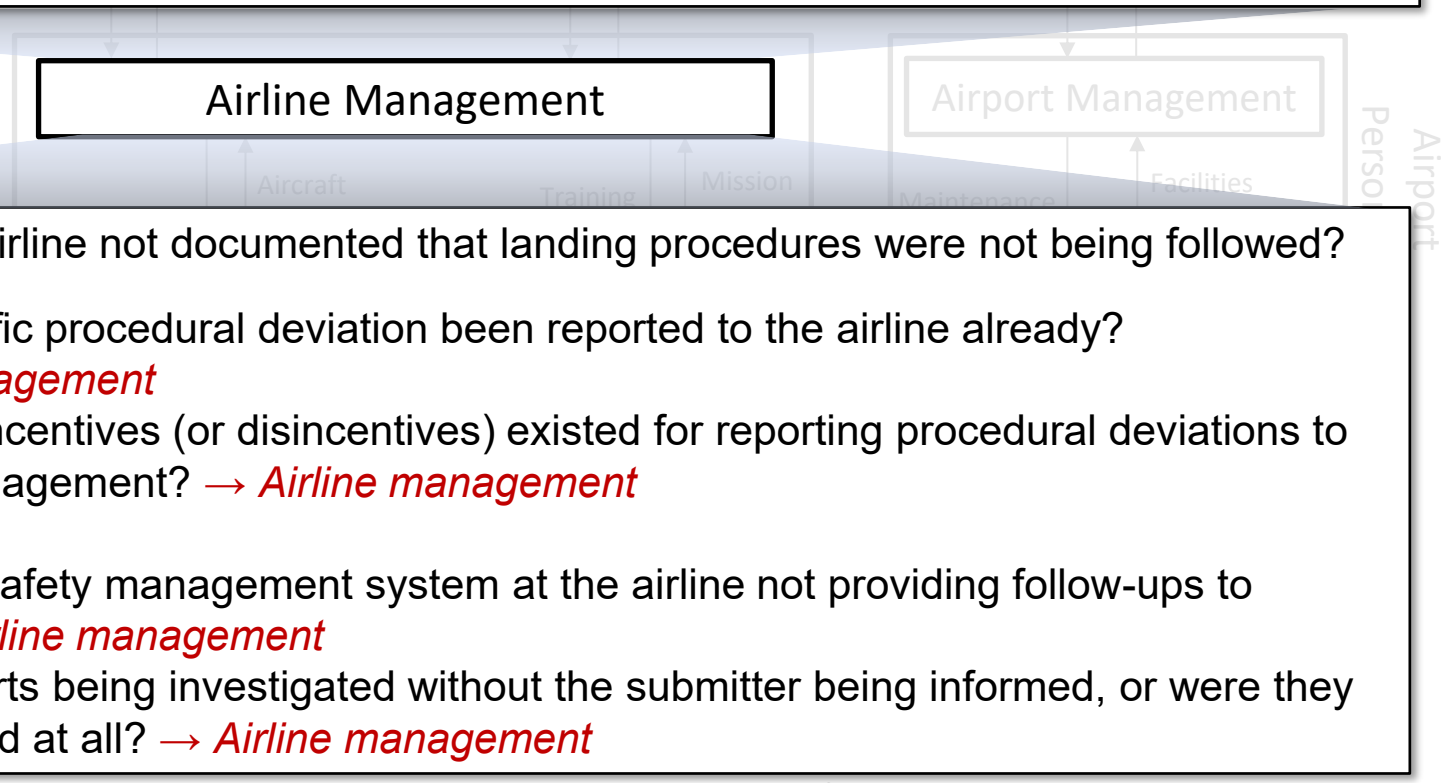


Contribution		Airline management did not directly inform their flight crews of the change to the procedure in the MEL for landing with one thrust reverser deactivated, which occurred in January 2007
Why?	**Process Model Flaws**	• Airline management believed pilots would become aware of the procedure by consulting the MEL before and during the flight. • Airline management may have believed the change was not safety critical enough to warrant new training
	Contextual Factors	There was a scarcity of safety-accredited personnel within the airline (21 people) who were spread out and moved between more than 30 physical locations

Airline Management

Questions	• Why did airline management not directly inform crews of the change in procedure? • What kind of analysis was conducted before making the decision to not directly inform pilots of this change? → *Airline management* • What kind of information had the airline received regarding the safety-criticality of this procedural change? → *Aircraft manufacturer* • Had airline management observed similar instances involving use of outdated procedures? → *Airline management* • What were the challenges to obtaining more safety-accredited personnel at the airline? → *Airline management*

Contribution		TAM management did not document or issue corrective action when, over the last 28 landings with a deactivated thrust reverser, 5 different procedures were used for landing
Why?	**Process Model Flaws**	• Management was only aware of procedural deviations when those were reported • Management may have believed that critical safety issues would be brought to their attention by senior pilots (outside of the regular safety management system) as this was common practice at the company
	Contextual Factors	Company employees did not feel encouraged to report deviations from procedure or safety concerns, as they typically got no follow-up

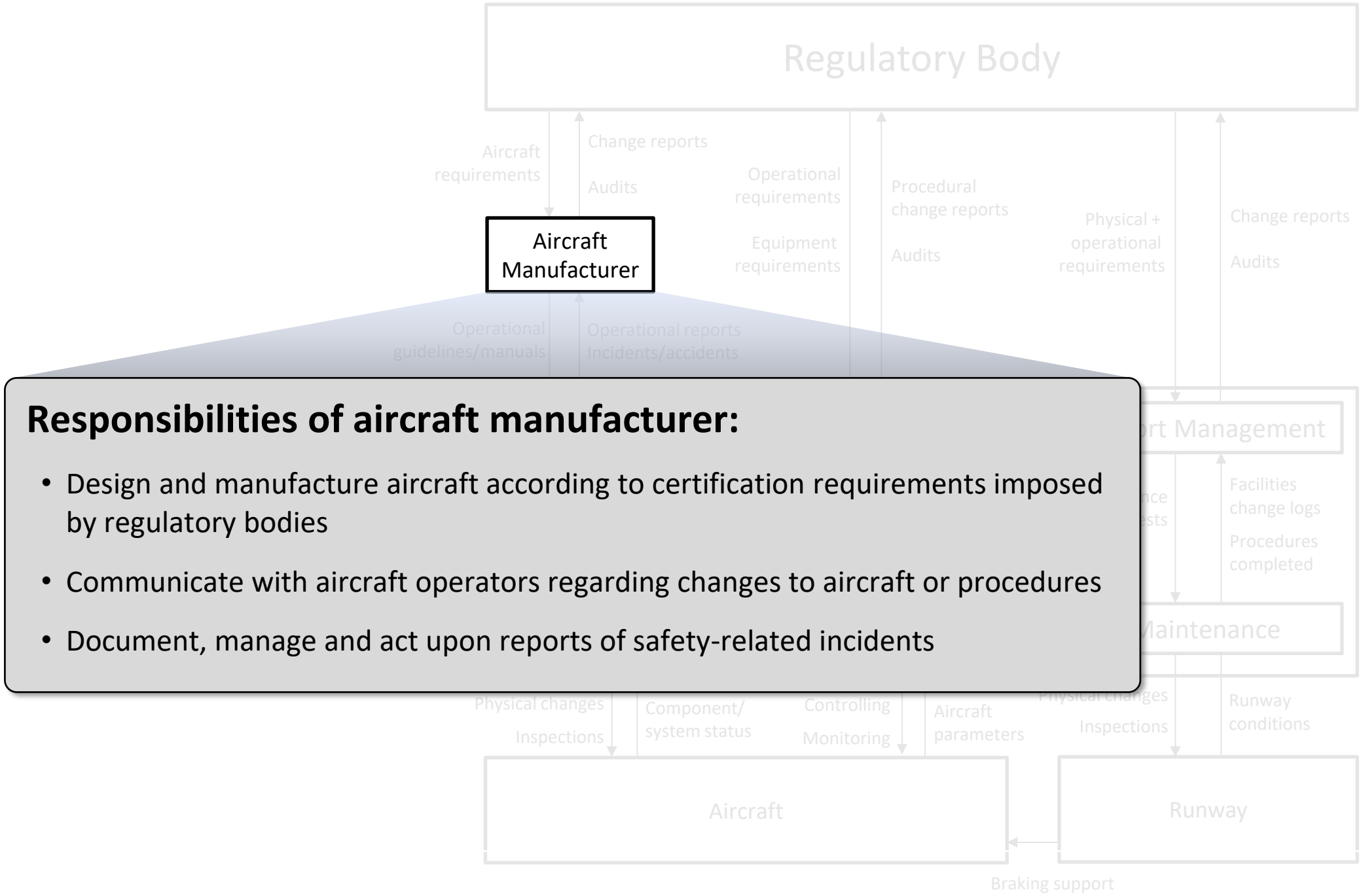


Questions	• Why had the airline not documented that landing procedures were not being followed? • Had this specific procedural deviation been reported to the airline already? → *Airline management* • What kind of incentives (or disincentives) existed for reporting procedural deviations to the airline management? → *Airline management* • Why was the safety management system at the airline not providing follow-ups to reports? → *Airline management* • Were the reports being investigated without the submitter being informed, or were they not investigated at all? → *Airline management*

More unanswered questions:

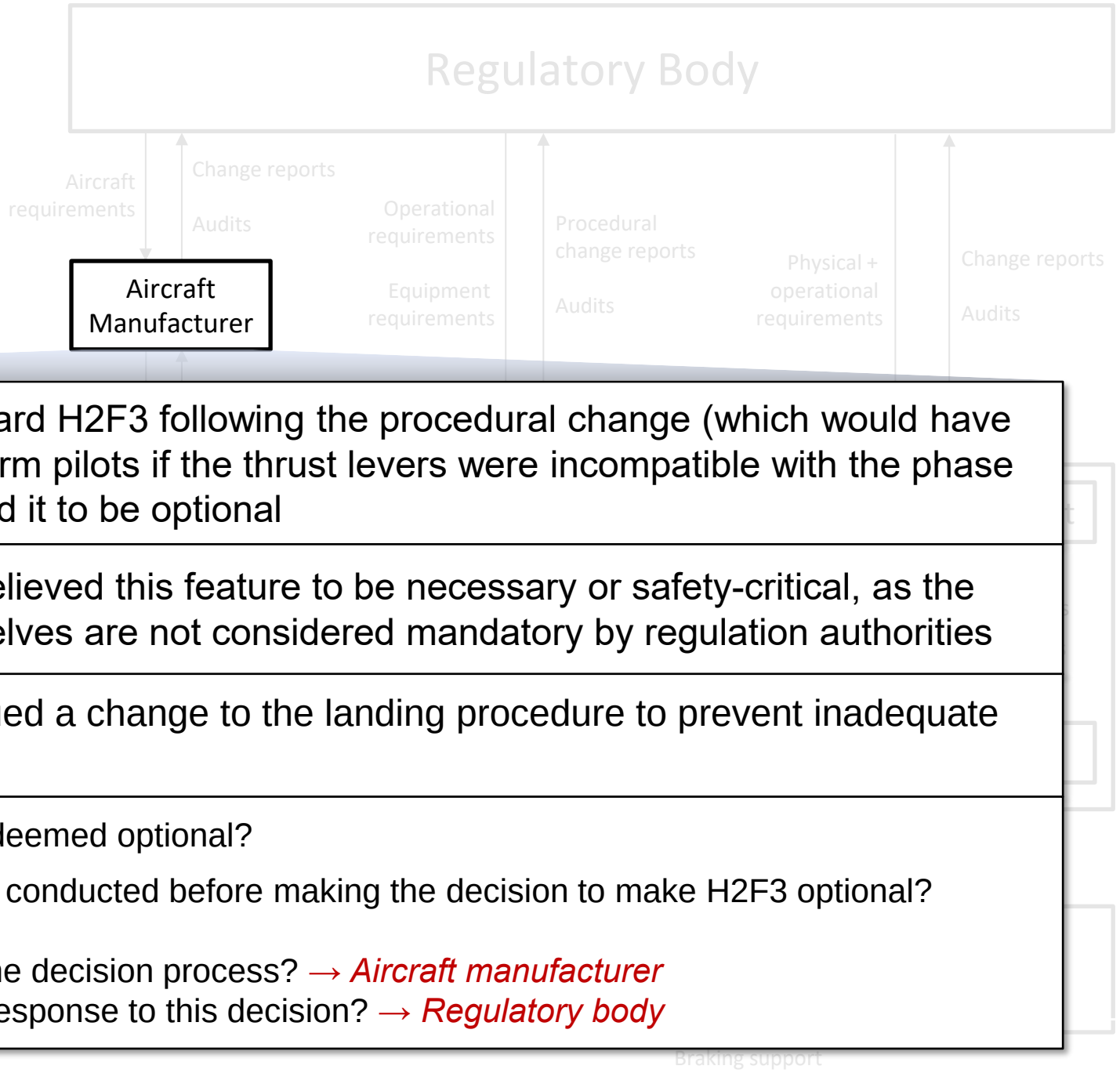
- What kind of analysis was conducted before making the decision to not directly inform pilots of this change? → ***Airline management***
- Had airline management observed similar instances involving use of outdated procedures? → ***Airline management***
- What were the challenges to obtaining more safety-accredited personnel at the airline? → ***Airline management***
- Why was the safety management system at the airline not providing follow-ups to reports? → ***Airline management***
- Were the reports being investigated without the submitter being informed, or were they not investigated at all? → ***Airline management***

- What kind of information had the airline received regarding the safety-criticality of this procedural change? → ***Aircraft manufacturer***

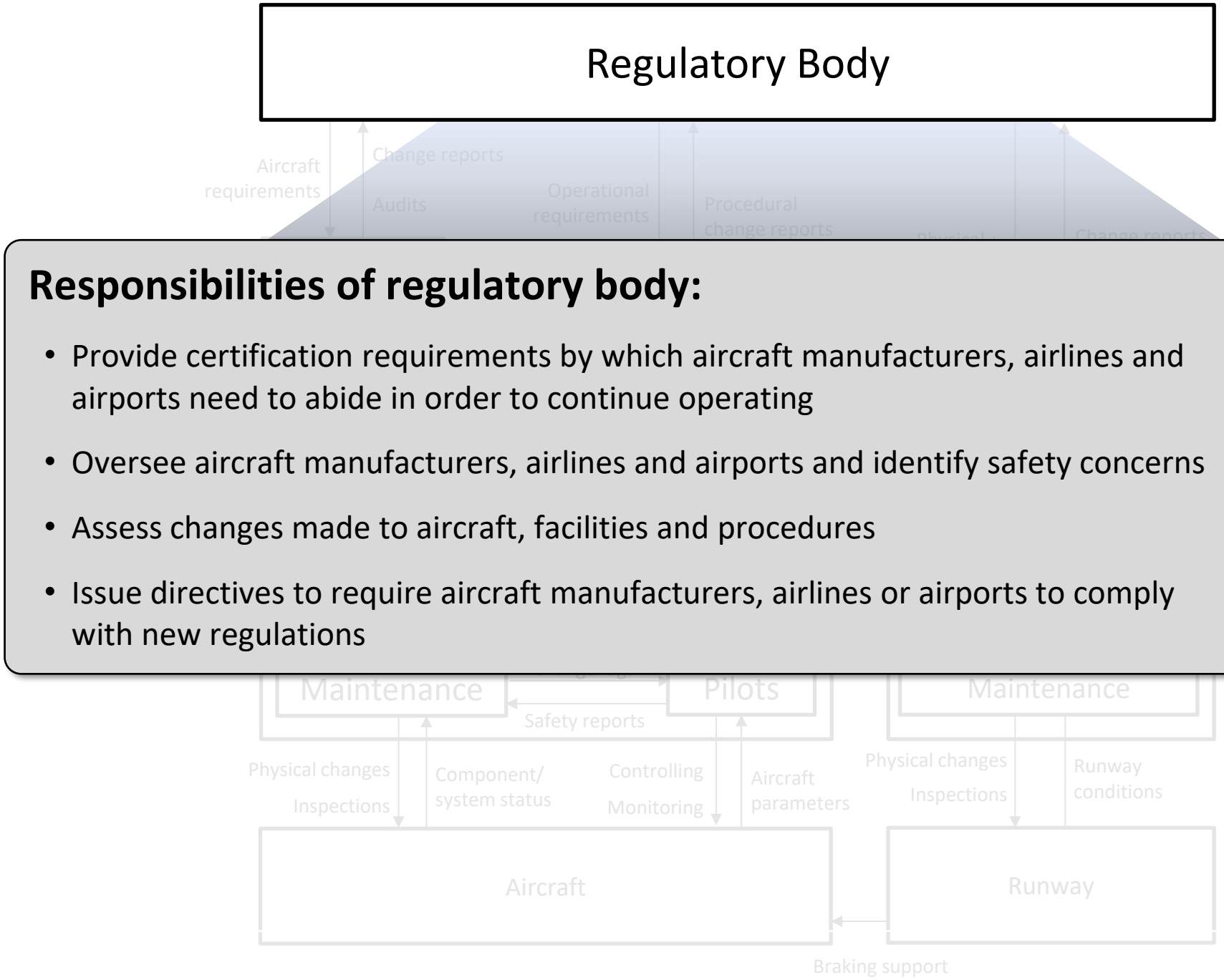


Responsibilities of aircraft manufacturer:

- Design and manufacture aircraft according to certification requirements imposed by regulatory bodies
- Communicate with aircraft operators regarding changes to aircraft or procedures
- Document, manage and act upon reports of safety-related incidents

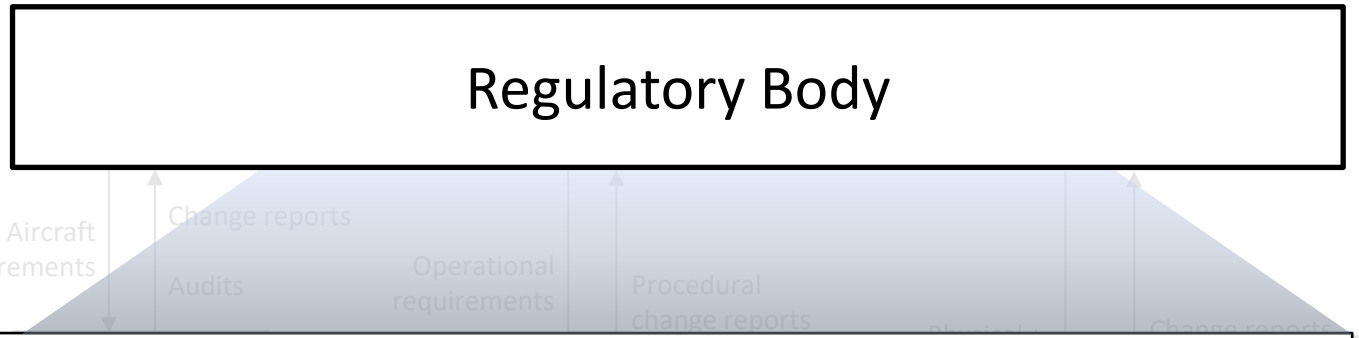


Contribution		Airbus published standard H2F3 following the procedural change (which would have installed an alert to inform pilots if the thrust levers were incompatible with the phase of flight) and determined it to be optional
Why?	**Process Model Flaws**	Airbus may not have believed this feature to be necessary or safety-critical, as the thrust reversers themselves are not considered mandatory by regulation authorities
	Contextual Factors	Airbus had already issued a change to the landing procedure to prevent inadequate thrust lever positioning
Questions		Why was standard H2F3 deemed optional? What kind of analysis was conducted before making the decision to make H2F3 optional? → *Aircraft manufacturer* Were pilots consulted in the decision process? → *Aircraft manufacturer* What was the regulatory response to this decision? → *Regulatory body*



Responsibilities of regulatory body:

- Provide certification requirements by which aircraft manufacturers, airlines and airports need to abide in order to continue operating
- Oversee aircraft manufacturers, airlines and airports and identify safety concerns
- Assess changes made to aircraft, facilities and procedures
- Issue directives to require aircraft manufacturers, airlines or airports to comply with new regulations



Contribution		Deemed procedural change sufficient in preventing thrust lever mispositioning on landing and allowed standard H2F3 to remain optional
Why?	**Process Model Flaws**	Because the regulatory bodies themselves did not consider thrust reversers mandatory for certification, thrust reverser related issues may have been viewed as non-safety critical beyond accidental deployment in flight
	Contextual Factors	Airbus had already drafted and analyzed the new procedure, therefore the relevant regulatory agencies may have accepted it without further validation
Questions		Why was standard H2F3 allowed to remain optional? What kind of analysis was conducted before signing off on Airbus' decision to make H2F3 optional? → *Regulatory body*



Most of the components have contributed to the accident in some way or did not operate exactly as planned

When looking only at what the operators did or did not do, it appears that they were the primary contributors to the loss

Usually, the actions of the operators will be found to be **understandable** when the reason for their behavior is examined



Identify flaws in the control structure **as a whole** by investigating the general **systemic factors** that contributed to the loss

For example: (but not limited to)



- Autobrake only informs pilots when it *is* decelerating at the desired rate
- Ground spoilers do not inform pilots of the reason for non-deployment
- No reporting of procedural deviations to airline management and no follow-up on reports

(missing feedback)

- No communication of reasons for procedural changes
- False process model update through cessation of alarms

(inappropriate feedback)

- …

For example: (but not limited to)

Communication and Coordination

Safety Culture

Safety Information/ Management Systems

Economic and Environmental Factors

Changes and Dynamics over Time

- Decentralized safety information system at airline (information stemming from safety analyses conducted by flight crews never reached maintenance team)
- Scarcity of safety-qualified professionals at airline, spread out over more than 30 bases of operation the airline held around the world (only 6 had training in safety investigation, only 3 were qualified to process Air Safety Reports (ASR) and only 1 was a psychologist specializing in human factors)
- Common practice within the airline was for senior crewmembers to directly approach company management with major issues that needed to be resolved

For example: (but not limited to)

Communication and Coordination

Safety Culture

Safety Information/ Management Systems

Economic and Environmental Factors

Changes and Dynamics over Time

- No direct communication about procedural changes and their reasons
- No documentation of compliance with procedural change)over the last 28 landings that PR-MBK conducted with the disabled reverser, five different procedures were used)
- Runway allowed to resume full operations without proper grooving
- …

Id
sy

For example: (but not limited to)

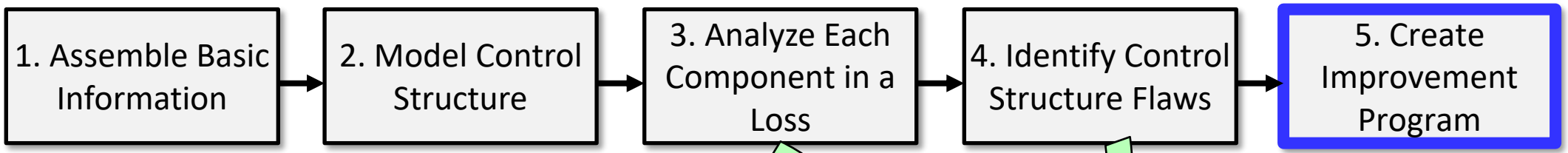
Communication and Coordination

Safety Culture

Safety Information/ Management Systems

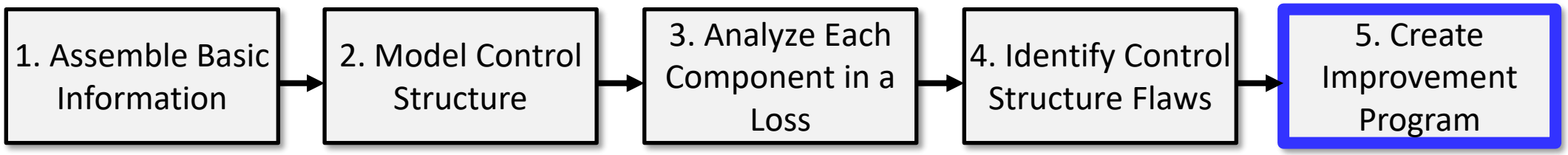
Economic and Environmental Factors

Changes and Dynamics over Time

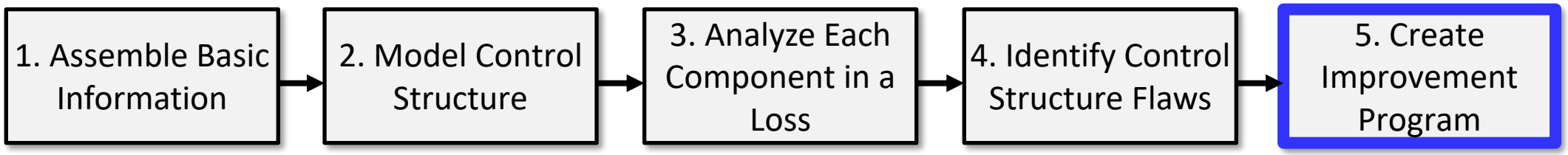


Recommendations can be generated from:

- Roles of components (identified in step 3)
- Systemic factors (identified in step 4)

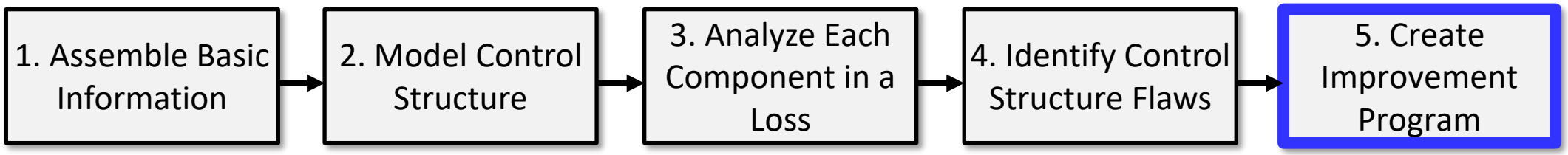


Component: Auto Brake Controller	
Role(s)	**Recommendations**
Did not issue braking commands because autobrake is activated by the ground spoiler deployment command, which never happened.	Auto brake logic needs to be reexamined to determine whether the benefits of tying its activation to ground spoiler deployment outweigh the risks in case of non-activation
Did not inform pilots that it wasn't issuing brake commands, other than *not* lighting up the "DECEL" light which activates when 80% of the desired deceleration rate is achieved	Auto brake controller needs to inform pilots through visual and auditory cues when it is *not* decelerating appropriately, as opposed to only notifying them if it *is* decelerating



Component: Airline Management	
Role(s)	**Recommendations**
Did not directly inform flight crews or train them on the change to the procedure in the MMEL for landing with one thrust reverser deactivated	Safety information system and management of change procedures must be redesigned to ensure that safety critical information about physical and procedural changes reaches pilots before they need to use that information
Chose to forgo standard which would have added alarms for inadequate thrust lever position at landing and would immediately have notified the pilots of JJ3054 of the inappropriate settings	Decision-making processes regarding adoption of optional standards must be reexamined to ensure flight crew input is considered

...



Three requirements for **successful implementation of recommendations**:

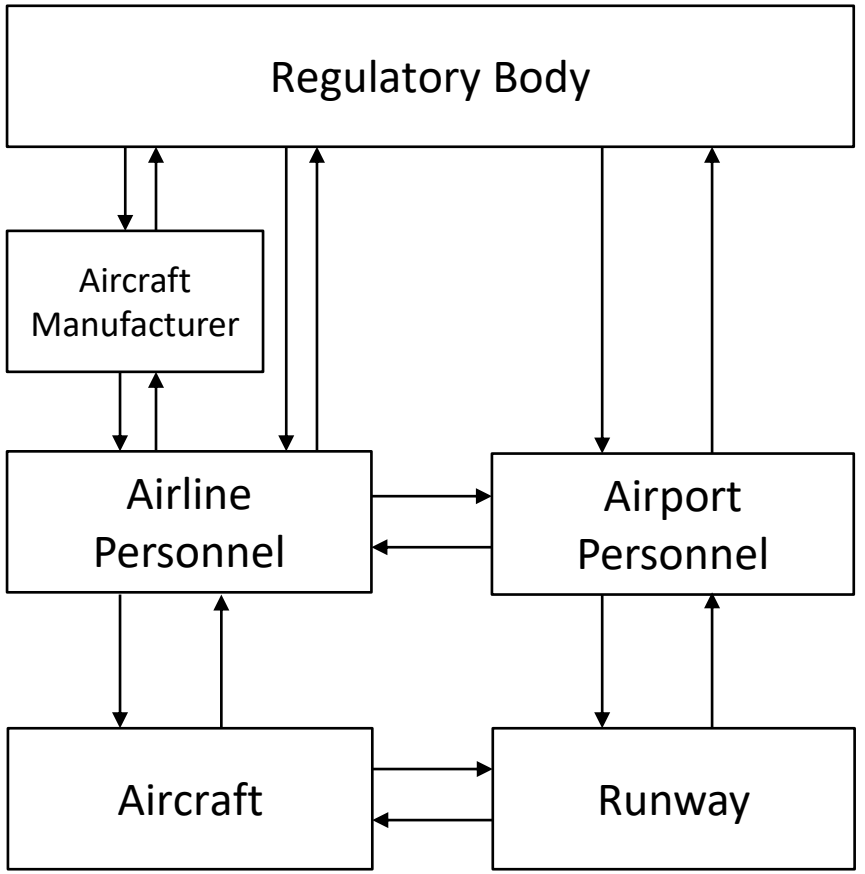
1. Assigning responsibility for implementing the recommendations
2. Checking that they have been implemented
3. Establishing a feedback system to determine whether they were effective in strengthening the controls

1. Assemble Basic Information → 2. Model Control Structure → 3. Analyze Each Component in a Loss → 4. Identify Control Structure Flaws → 5. Create Improvement Program

Accident: Loss of TAM Linhas Aéreas Flight JJ3054



CAST Handbook



http://sunnyday.mit.edu/CAST-Handbook.pdf

Rodrigo Lopes Rose

rlrose@mit.edu