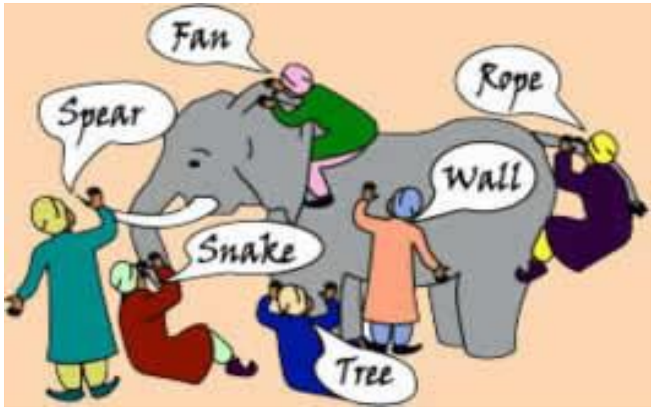


Hints on Using CAST for Accident Analysis

Nancy Leveson

Thoughts

- CAST should be used for accident analysis, STPA is not appropriate
  - Only want what happened, not everything that <u>could</u> happen
  - Social parts of system are critical in accident analysis
    - Most difficult to identify and thus most often omitted in accident reports
    - CAST is designed to help you analyze these parts
  - Need to consider both operations and development processes and their controls

Conclusions

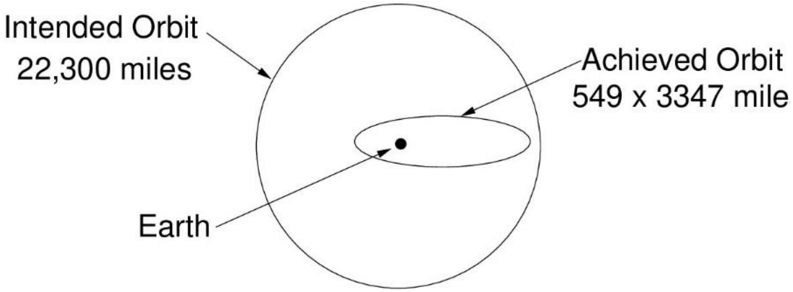
- CAST helps you collect the information you need
- To prevent accidents, analyze social parts of system (SMS) use a different type of analysis than STPA (see my SMS tutorial)

Example: What Happened?

- April 30, 1999, Titan IV B-32 booster equipped with Centaur TC-14 upper stage launched from Cape Canaveral.
- Mission was to place a Milstar-3 satellite into geosynchronous orbit.
- Milstar satellite placed in an unusable low elliptical orbit and had to be destroyed
- One of most costly unmanned losses at Cape Canaveral to that date.
- Loss was $1.3 billion

Chain of Events

- Roll rate filter constant incorrectly entered manually (typo) into load tape (-0.1992476 instead of -1.992476)
- Incorrect roll rate filter constant zeroed any roll rate data
- Resulted in loss of roll axis control
- Which then caused loss of yaw and pitch control
- Led to excessive firings of Reaction Control System
- Leading to hydrazine depletion
- Erratic vehicle flight during Centaur main engine burns caused an orbit apogee and perigee much lower then desired
- Resulted in Milstar separating in a useless low final orbit



1. **Root cause?**
2. **Recommendations?**
3. **Questions raised?**

Events are Not Enough

- Lots of questions raised:
  - Why was human typo not caught by LM review and testing process?
  - Problem was evident on launch pad, why did nobody question behavior before launch?
  - Why were the controls created to prevent this type of accident ineffective in this case?
    - Need to identify these first

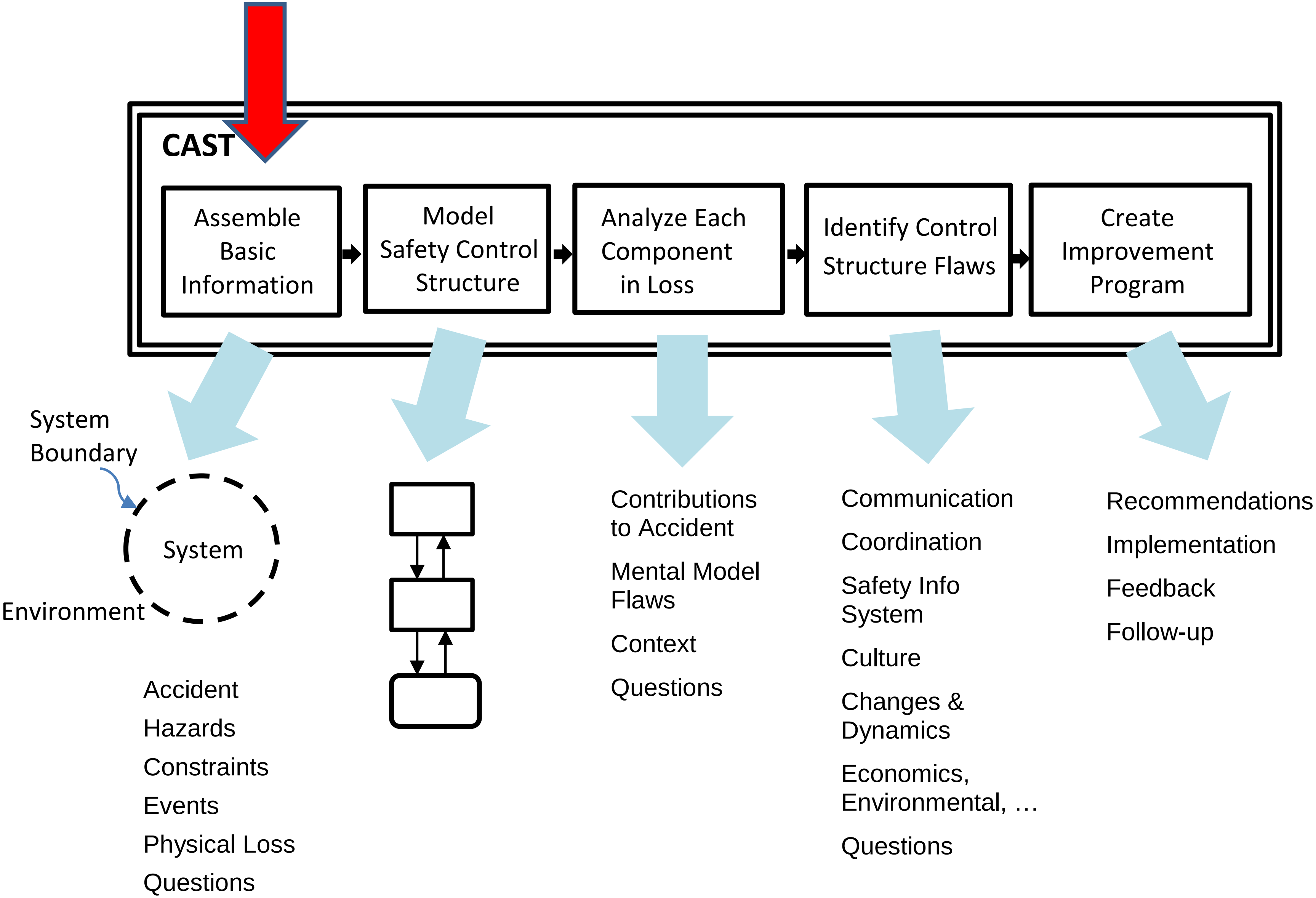
Controls to Ensure Correct Load Tape Constants

1. Multiple checks on load tape constants during development
2. Testing and oversight at the Cape

None of these was successful in this case

To understand why, need to look at individual behavior, operation of structural controls, and safety control structure design (SMS)

- Everyone involved had incorrect process models
- Lots of missing feedback paths
- Controls and control structure as designed were not effective



CAST

Assemble Basic Information

Model Safety Control Structure

Analyze Each Component in Loss

Identify Control Structure Flaws

Create Improvement Program

System Boundary

System

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, Environmental, …

Questions

Recommendations

Implementation

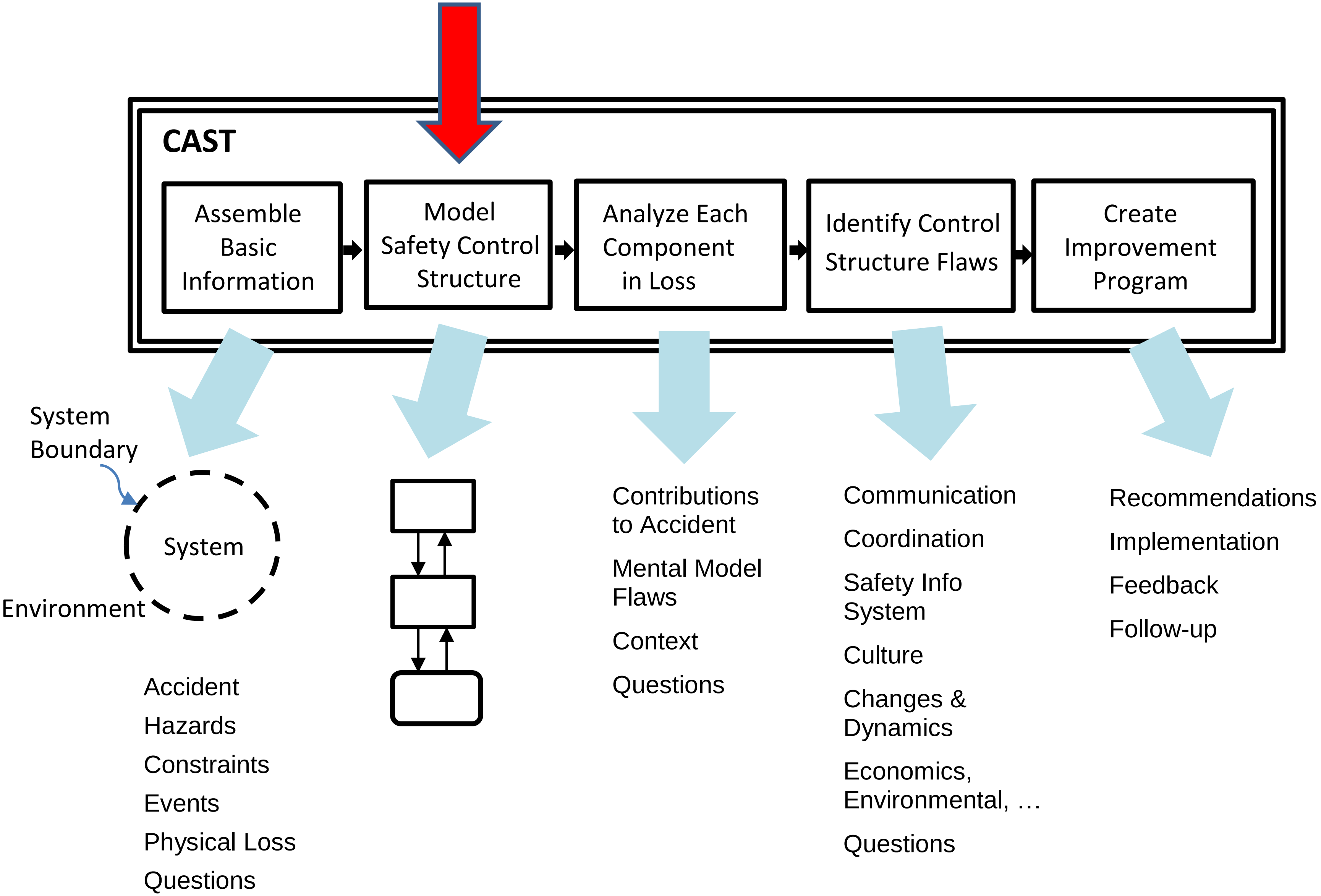
Feedback

Follow-up

Starting Information

- **Loss Event**: Loss of satellite and its intended function
- **Hazard**: Satellite does not reach a useful geosynchronous orbit

Goal is to determine why the controls in place were not effective and how to improve them for the future



CAST

Assemble Basic Information

Model Safety Control Structure

Analyze Each Component in Loss

Identify Control Structure Flaws

Create Improvement Program

System Boundary

System

Environment

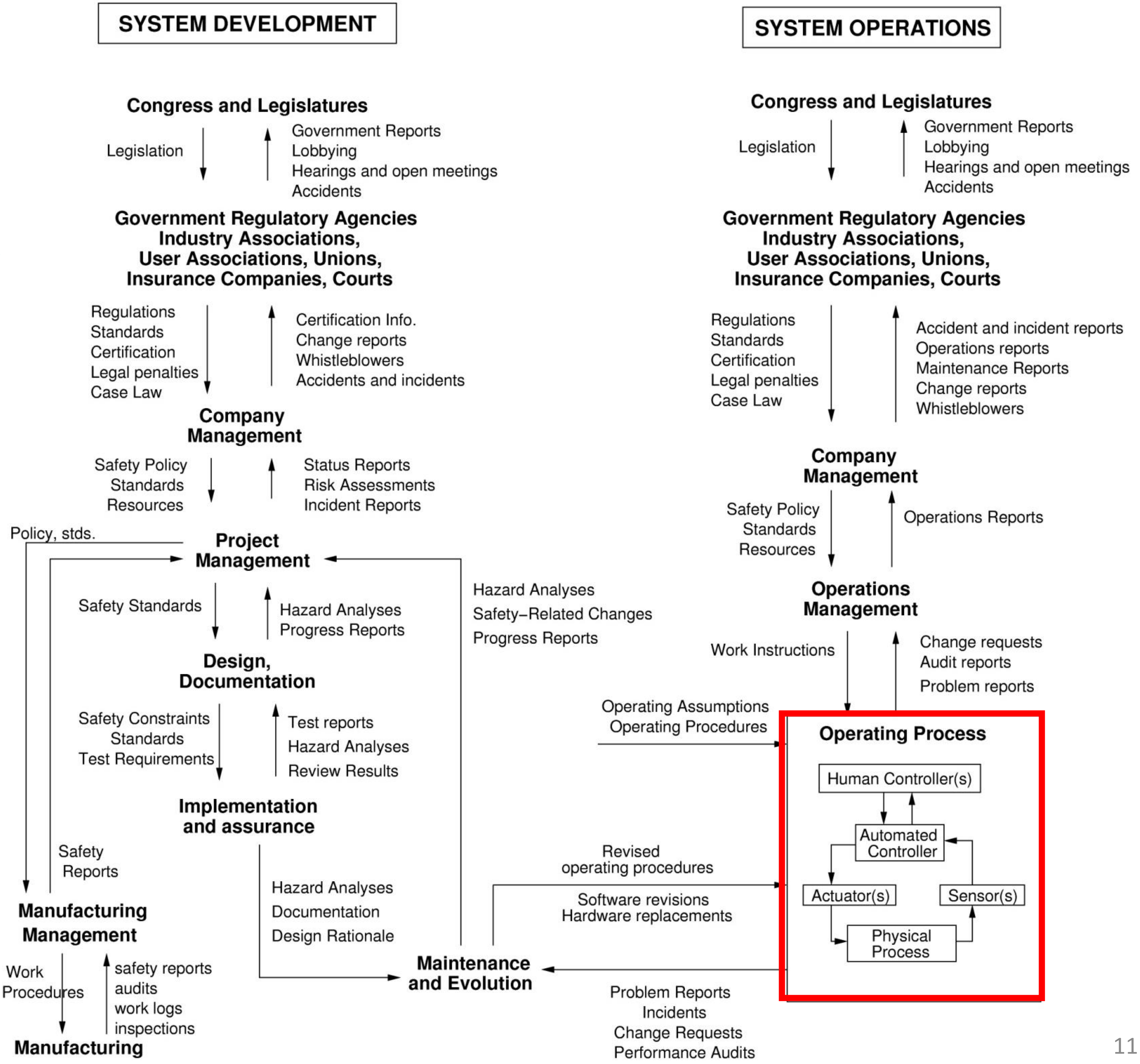
Accident
Hazards
Constraints
Events
Physical Loss
Questions

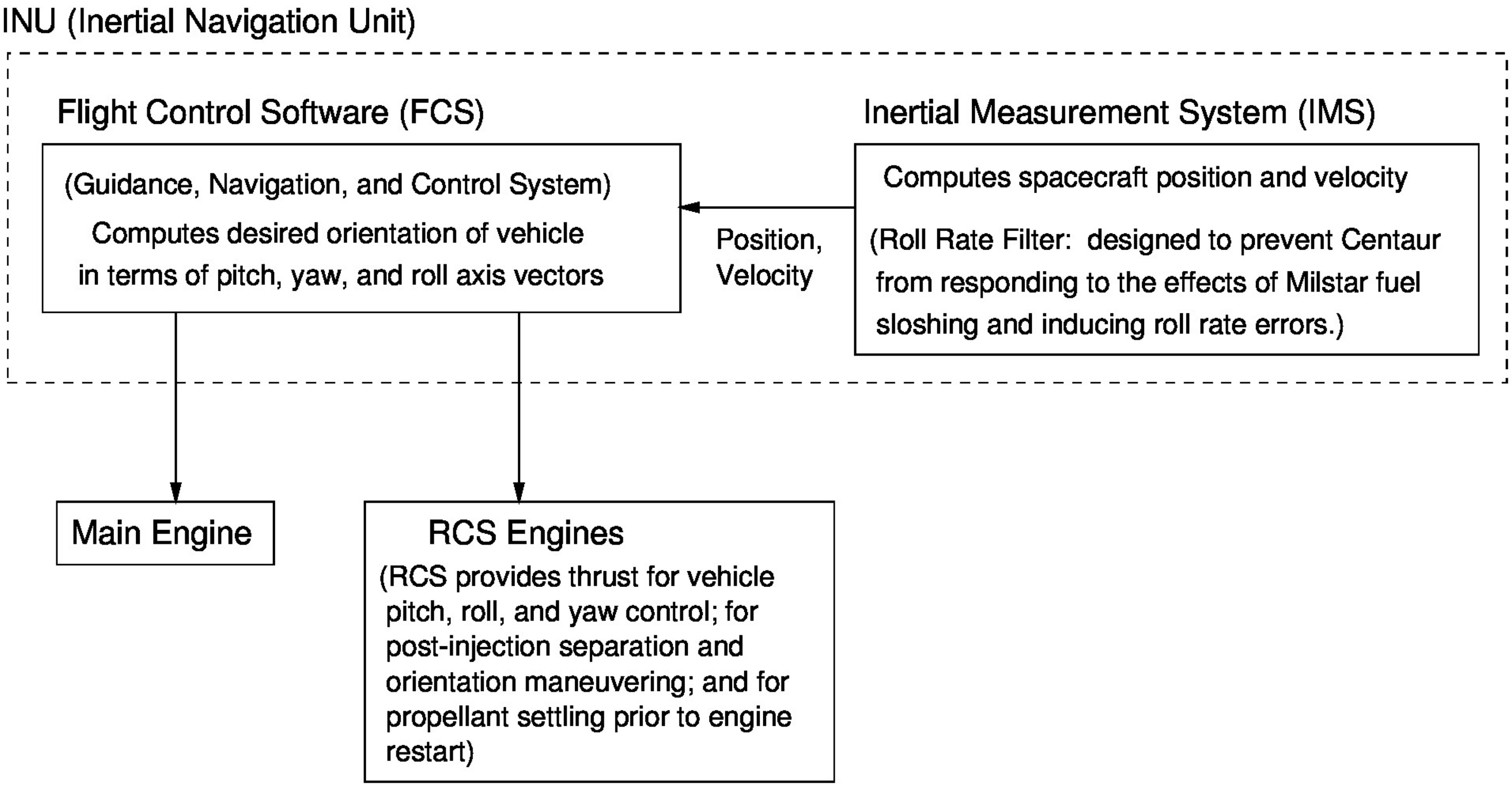
Contributions to Accident
Mental Model Flaws
Context
Questions

Communication
Coordination
Safety Info System
Culture
Changes & Dynamics
Economics, Environmental, …
Questions

Recommendations
Implementation
Feedback
Follow-up

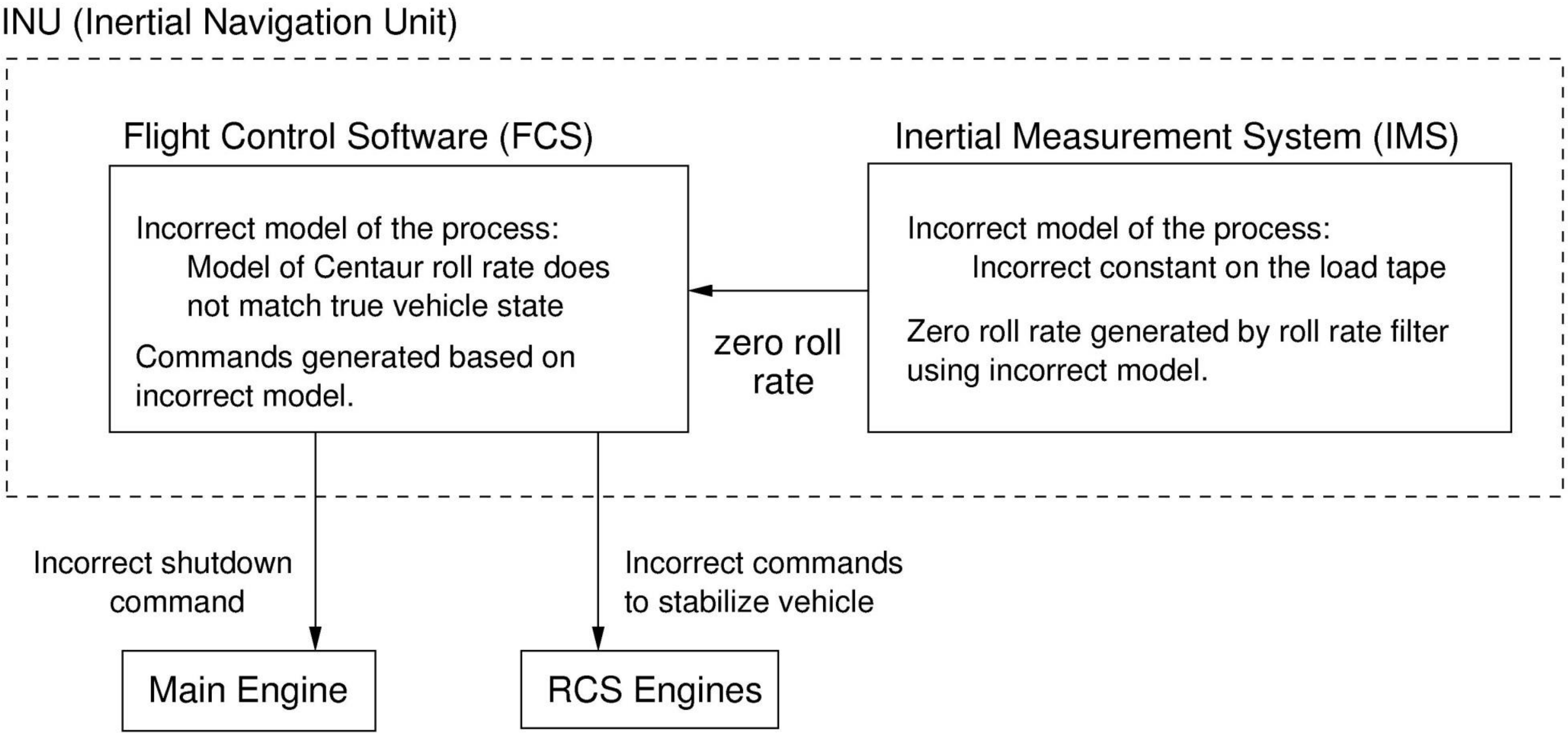
Example Safety Control Structure (SMS)




INU (Inertial Navigation Unit)
Flight Control Software (FCS)
(Guidance, Navigation, and Control System)
Computes desired orientation of vehicle in terms of pitch, yaw, and roll axis vectors
Inertial Measurement System (IMS)
Computes spacecraft position and velocity
(Roll Rate Filter: designed to prevent Centaur from responding to the effects of Milstar fuel sloshing and inducing roll rate errors.)
Position, Velocity
Main Engine
RCS Engines
(RCS provides thrust for vehicle pitch, roll, and yaw control; for post-injection separation and orientation maneuvering; and for propellant settling prior to engine restart)

Safety constraint on FCS violated: The FCS must provide the attitude control, separation, and orientation commands to the main engines and RCS to attain geosynchronous orbit

Safety constraint on IMS violated: (1) Position and velocity values provided to FCS must not lead to an FCS hazardous control action (2) Roll rate filter must prevent Centaur from responding to the effects of fuel sloshing and induce roll rate errors.



INU (Inertial Navigation Unit)

Flight Control Software (FCS)

Incorrect model of the process:
Model of Centaur roll rate does not match true vehicle state

Commands generated based on incorrect model.

Inertial Measurement System (IMS)

Incorrect model of the process:
Incorrect constant on the load tape

Zero roll rate generated by roll rate filter using incorrect model.

zero roll rate

Incorrect shutdown command

Incorrect commands to stabilize vehicle

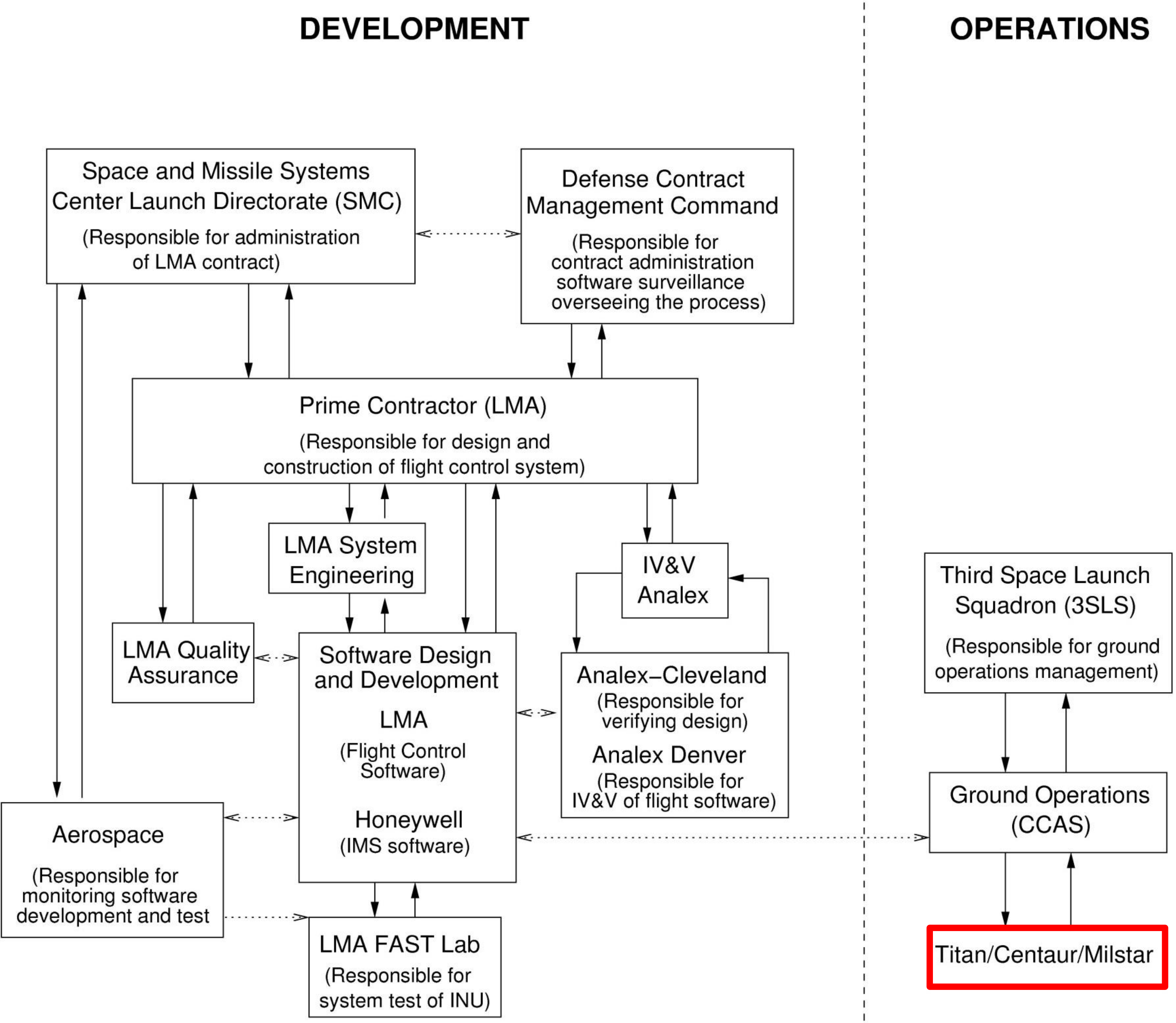
Main Engine

RCS Engines

Some Basic Questions

- Why was an erroneous load tape type created? Why were the controls not effective in preventing or discovering this during development and the extensive verification and validation process?
- Why was the roll rate error not detected during launch operations?
- How did the error get past the quality assurance process?
- What role, if any, did program management play in this?

1. **Recommendations?**
2. **More questions raised?**



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

Analex−Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

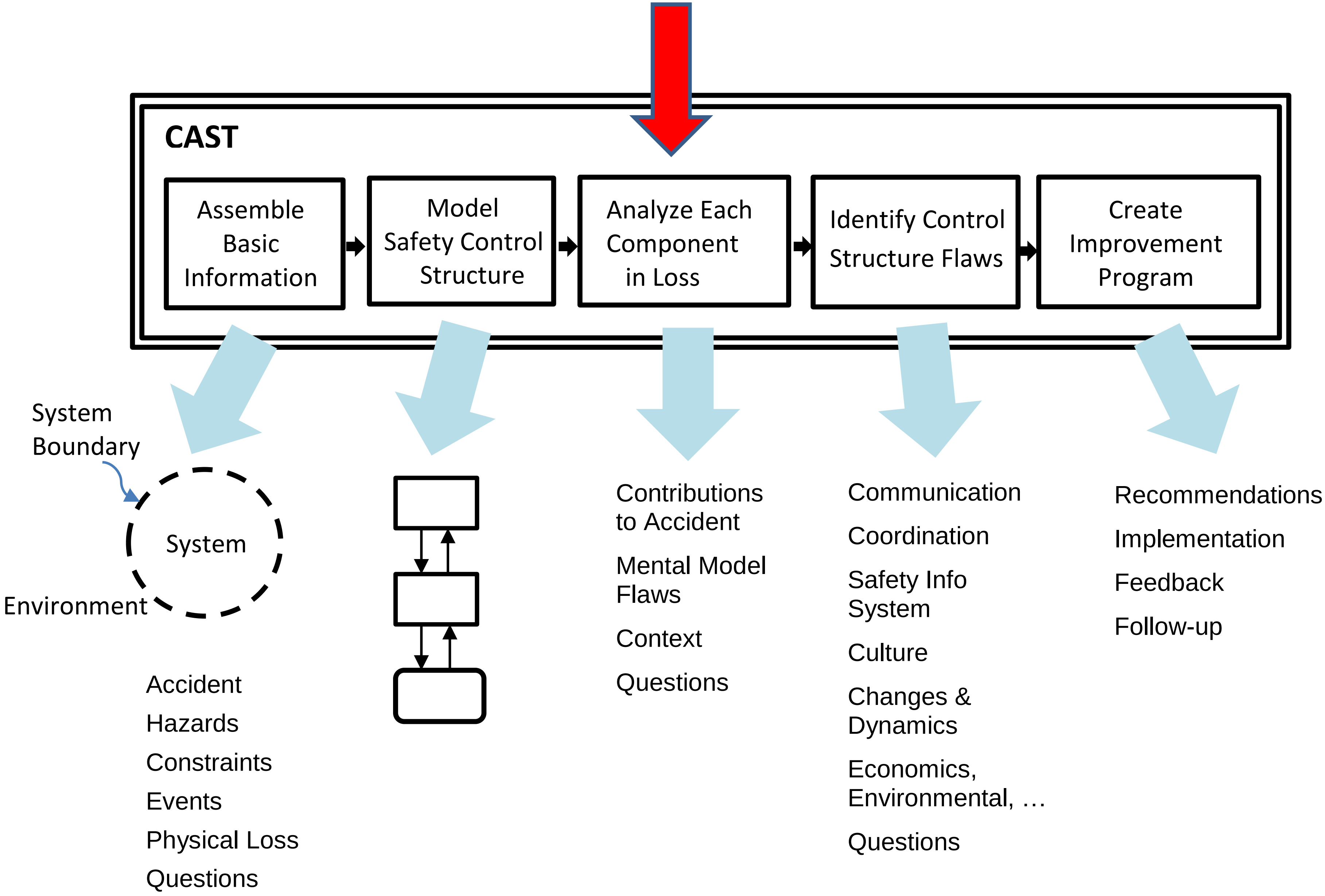
(Responsible for system test of INU)

Third Space Launch Squadron (3SLS)

(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar



CAST

Assemble Basic Information → Model Safety Control Structure → Analyze Each Component in Loss → Identify Control Structure Flaws → Create Improvement Program

System Boundary

System

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, Environmental, …

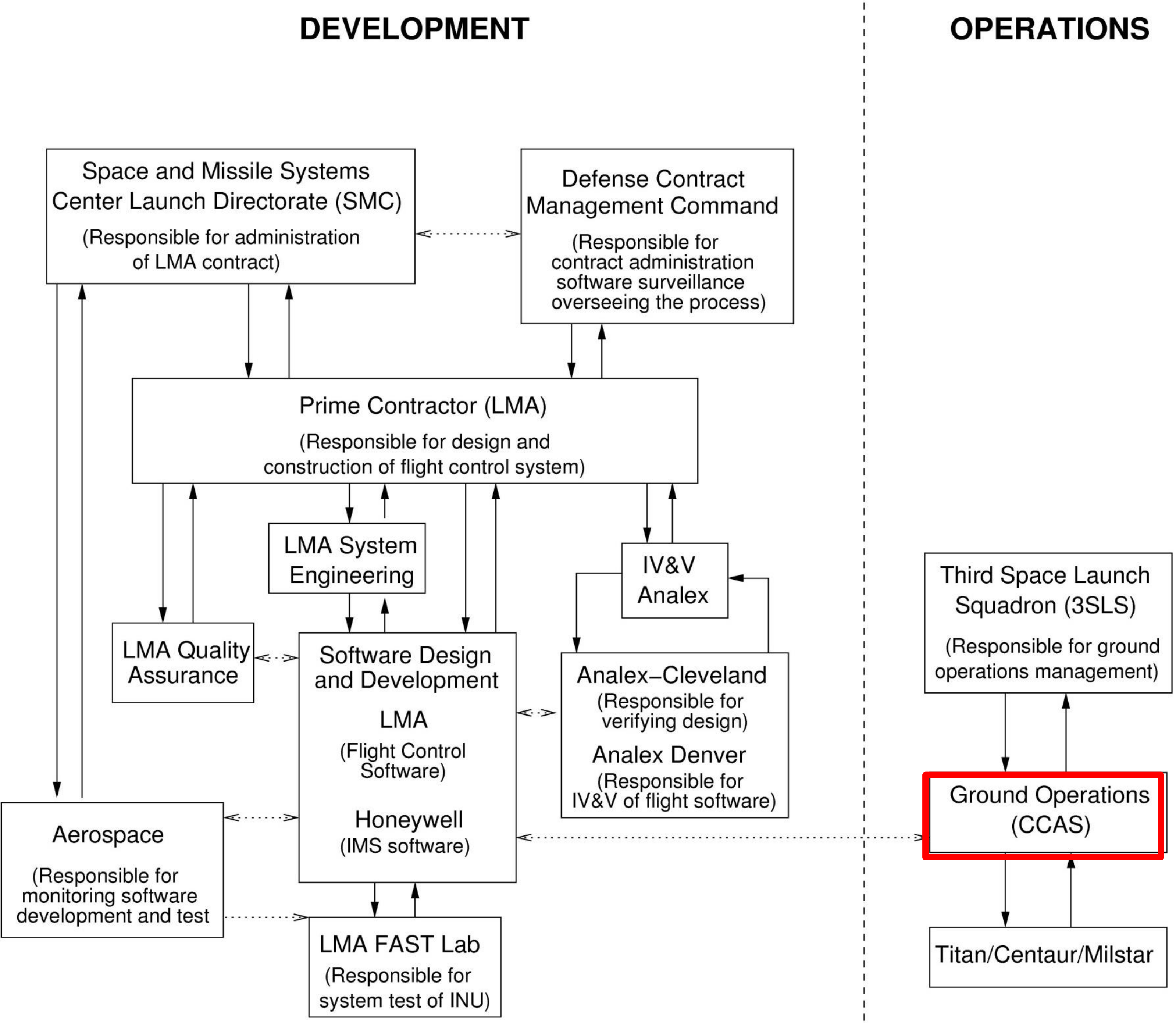
Questions

Recommendations

Implementation

Feedback

Follow-up



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

Analex–Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

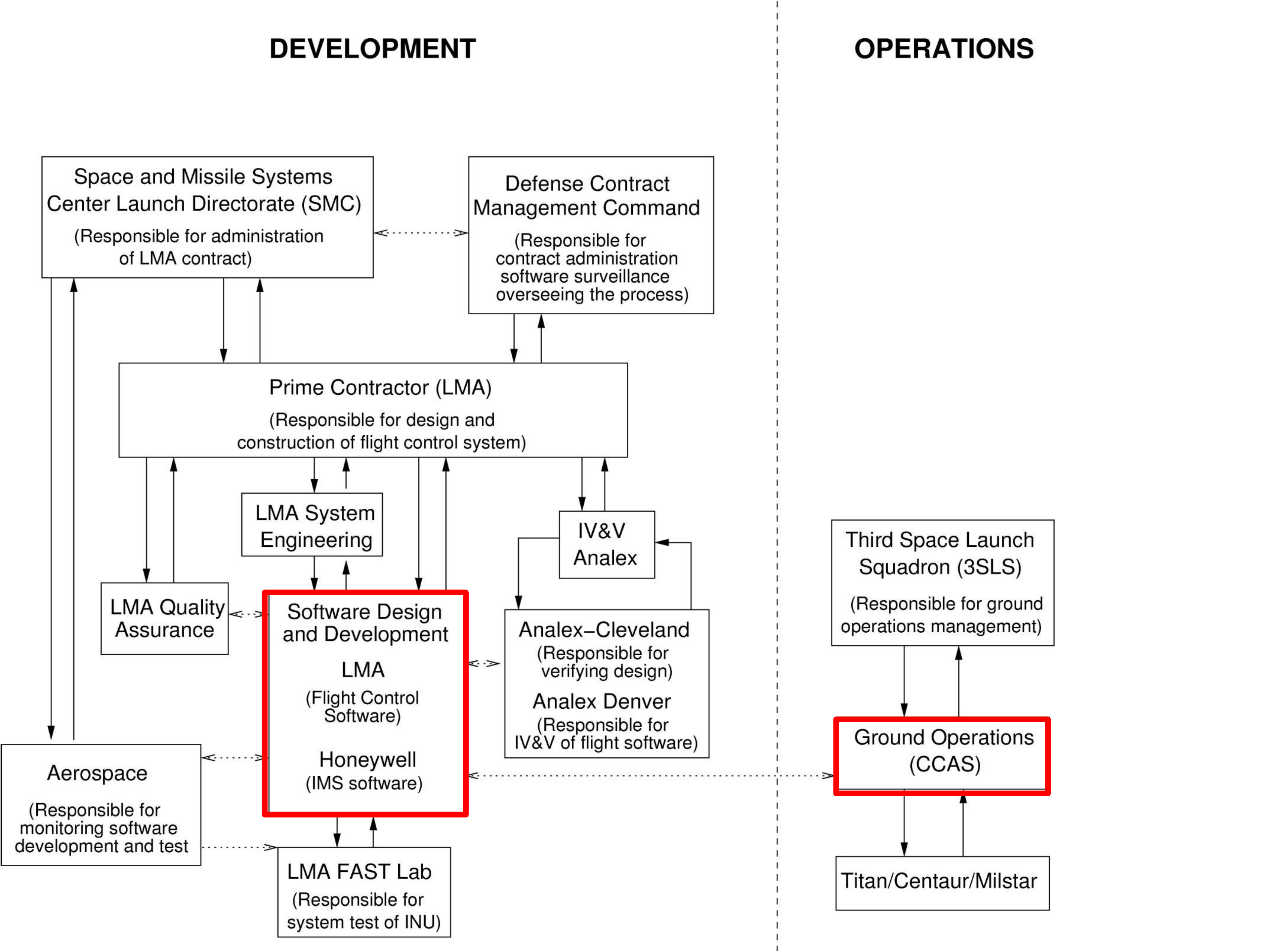
(Responsible for system test of INU)

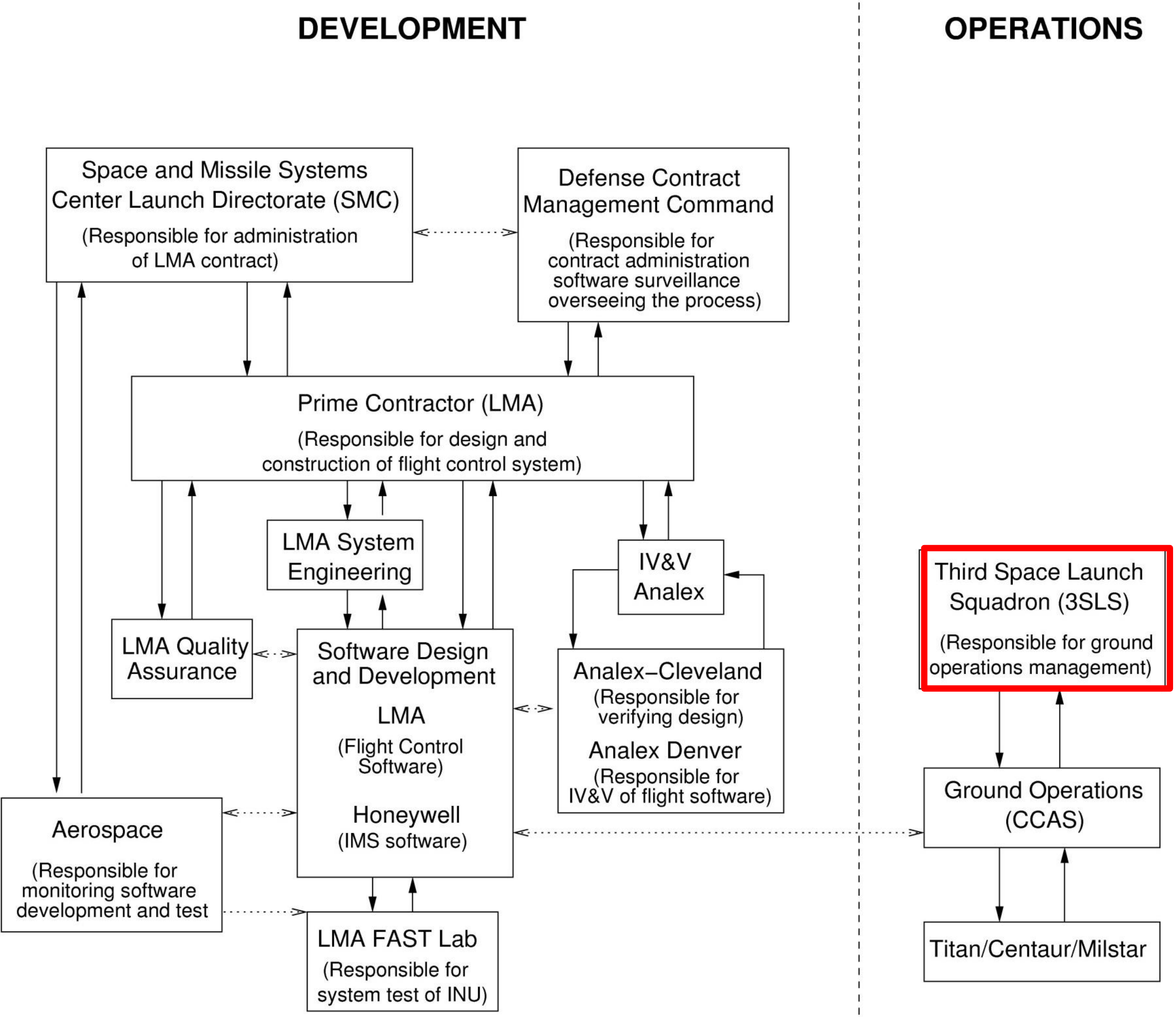
Third Space Launch Squadron (3SLS)

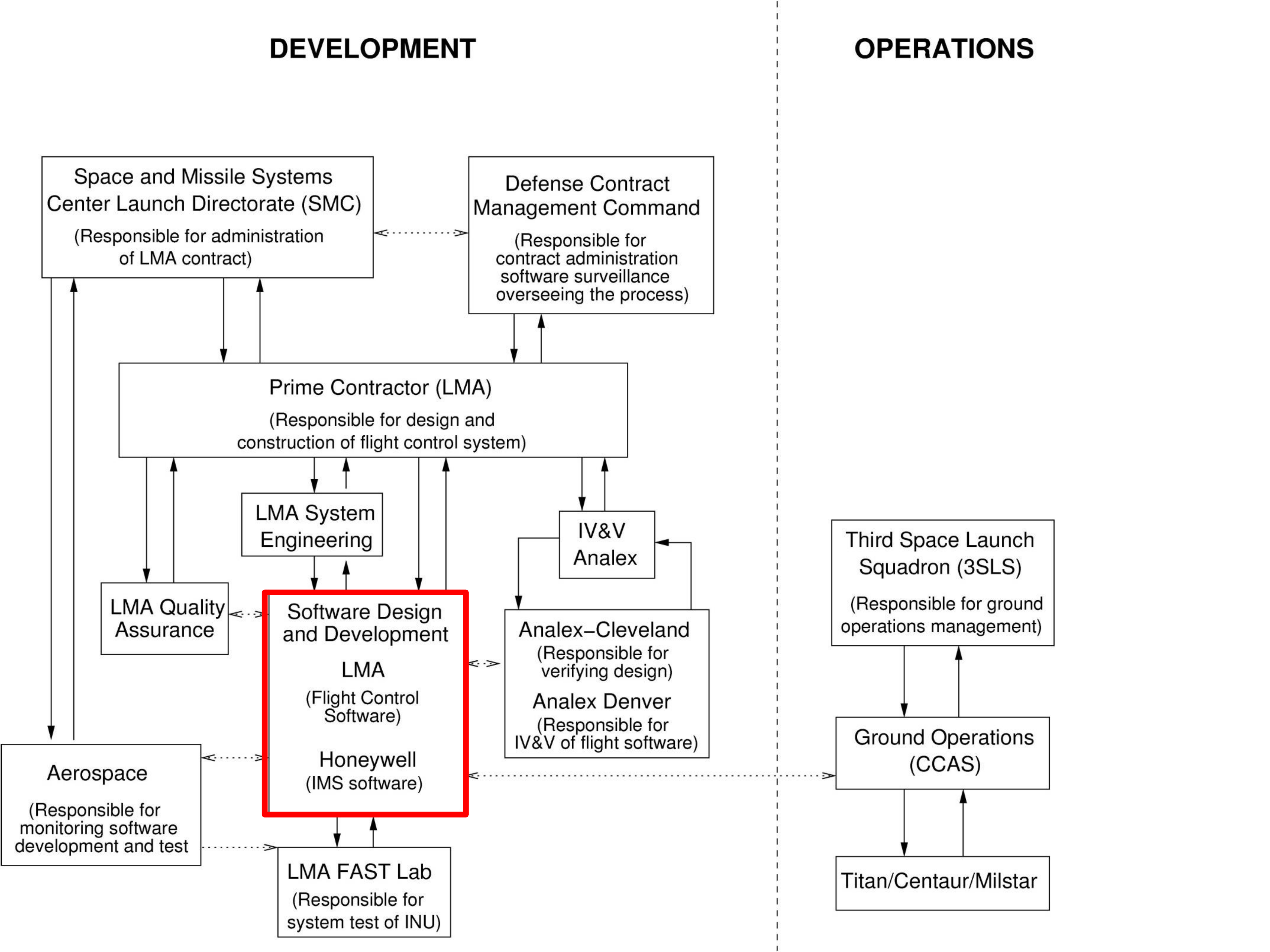
(Responsible for ground operations management)

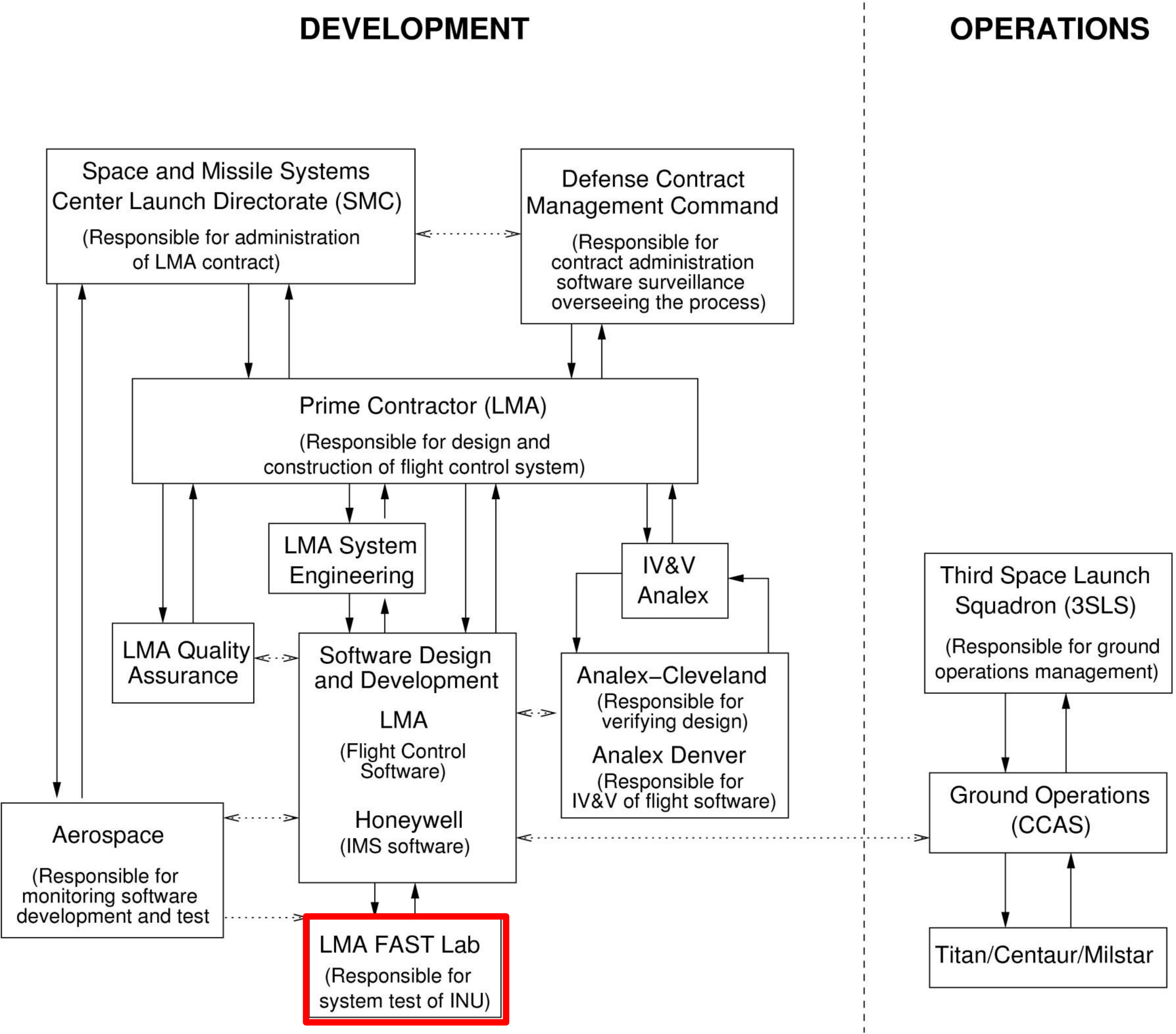
Ground Operations (CCAS)

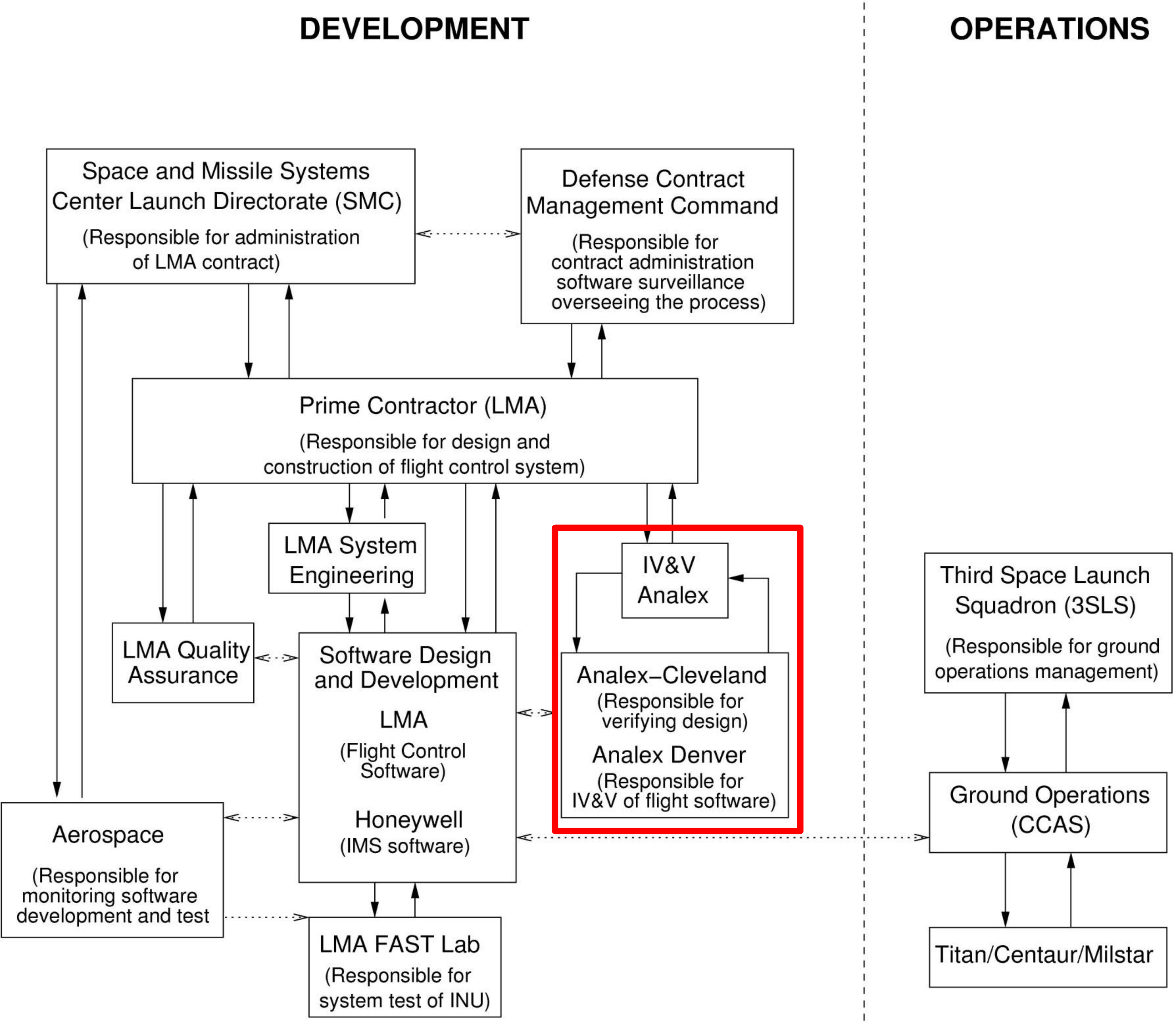
Titan/Centaur/Milstar


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex−Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Titan/Centaur/Milstar


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex−Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Titan/Centaur/Milstar


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex–Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Titan/Centaur/Milstar


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex–Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Titan/Centaur/Milstar



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

IV&V Analex

Analex−Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

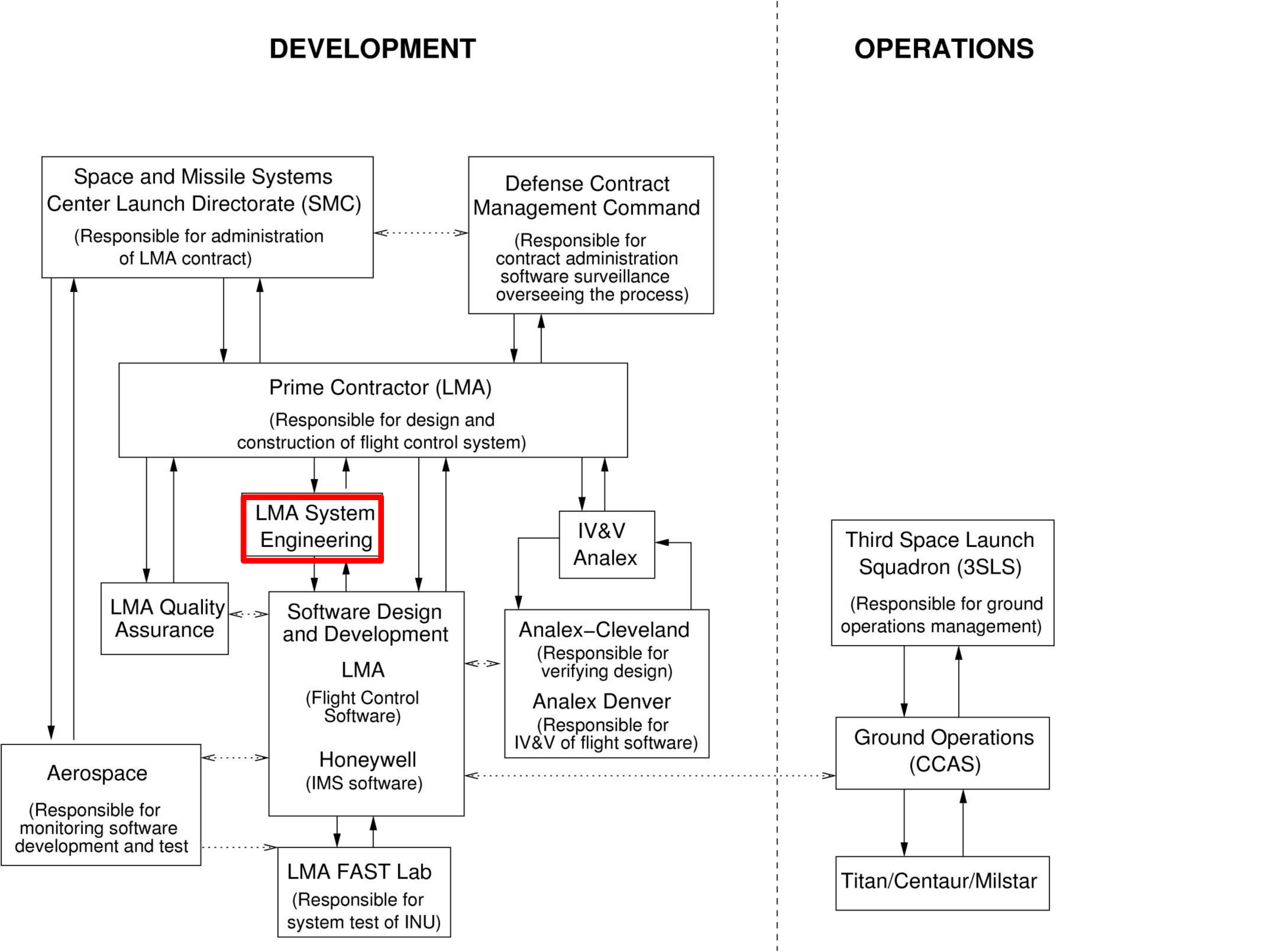
(Responsible for system test of INU)

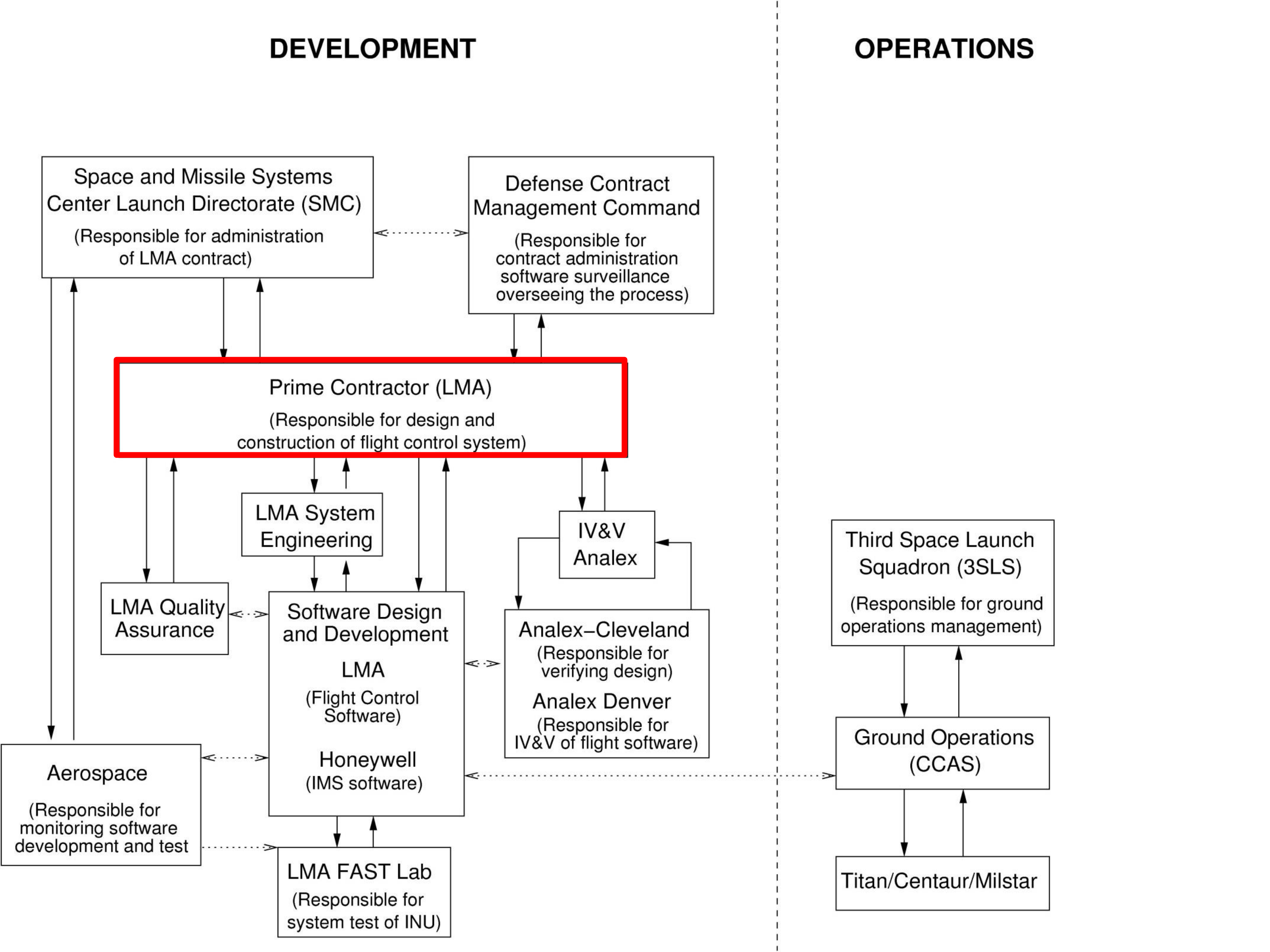
Third Space Launch Squadron (3SLS)

(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex−Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Titan/Centaur/Milstar



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)

Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)
(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)

Analex−Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)

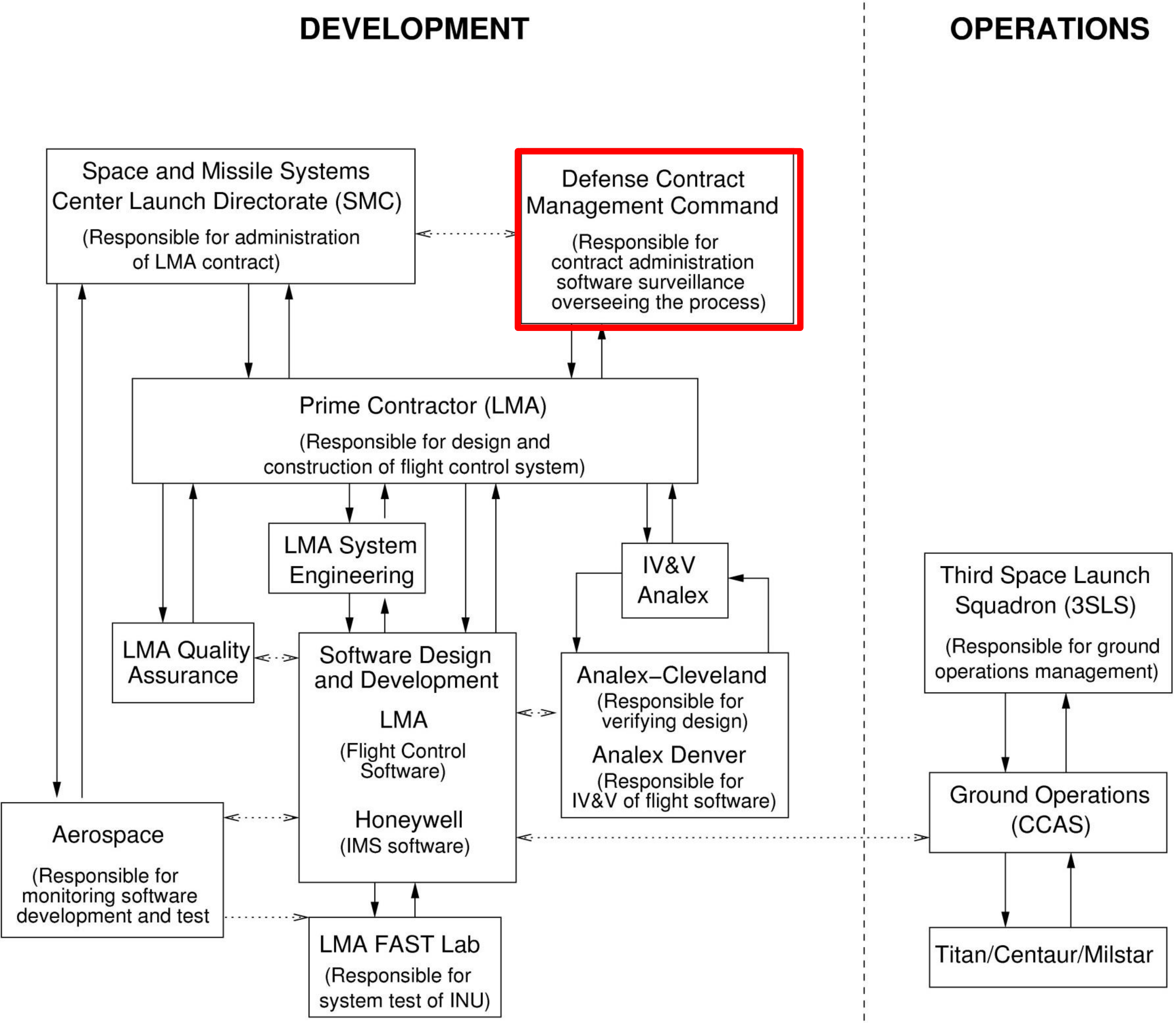
Aerospace
(Responsible for monitoring software development and test

LMA FAST Lab
(Responsible for system test of INU)

Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

Analex–Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

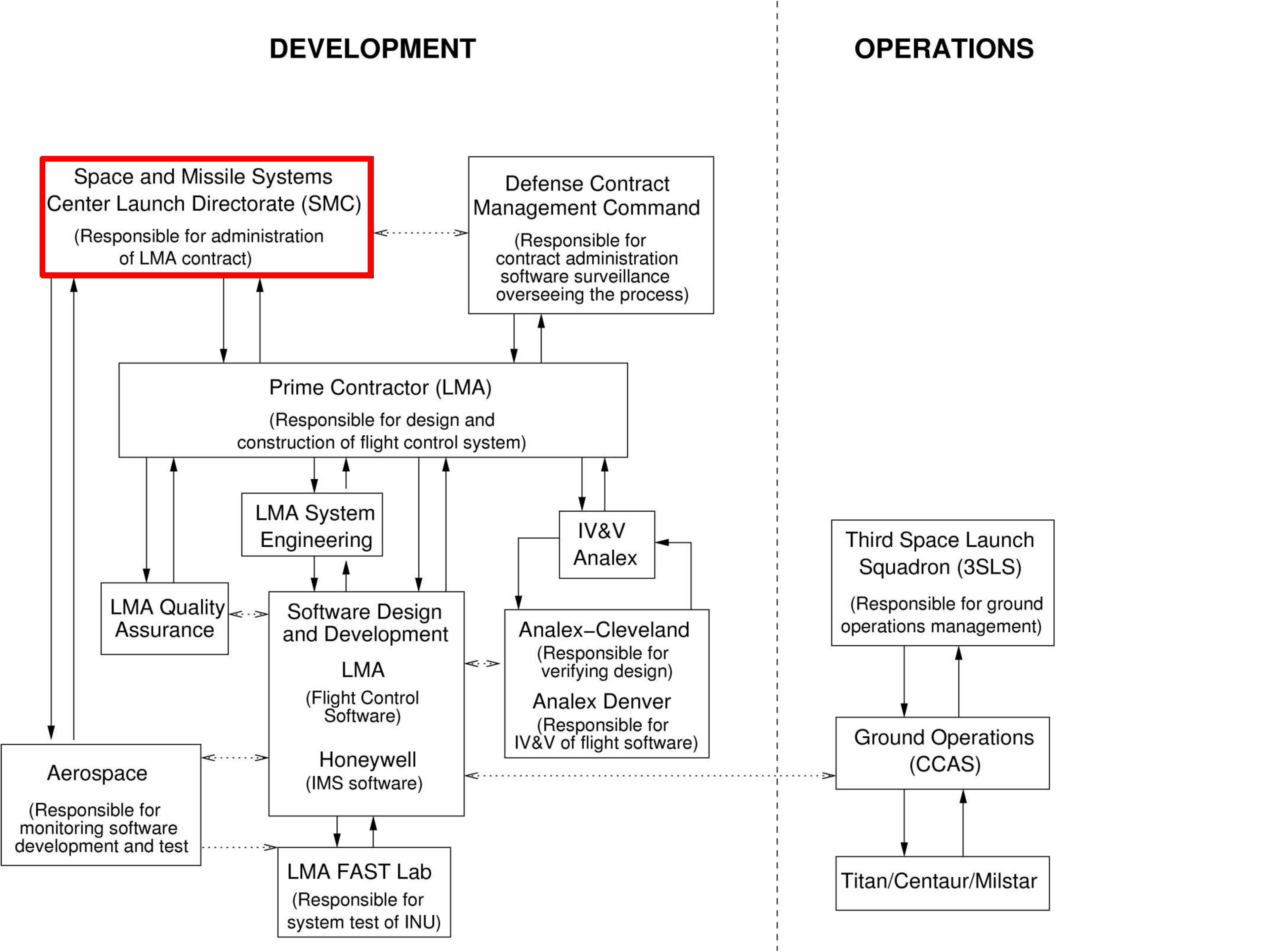
(Responsible for system test of INU)

Third Space Launch Squadron (3SLS)

(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

Analex–Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

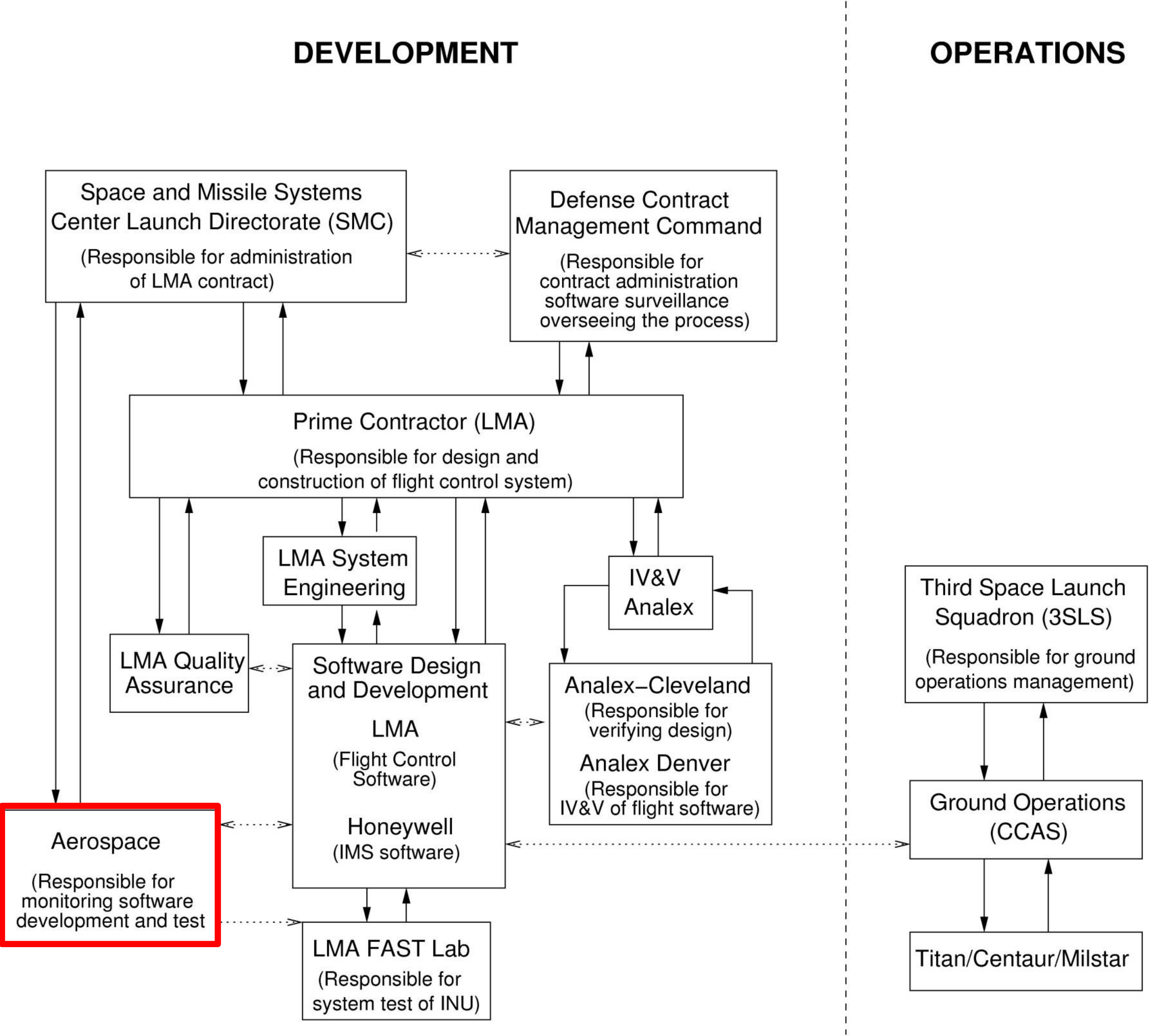
(Responsible for system test of INU)

Third Space Launch Squadron (3SLS)

(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar



DEVELOPMENT

OPERATIONS

Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

(Responsible for contract administration software surveillance overseeing the process)

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA

(Flight Control Software)

Honeywell

(IMS software)

Analex–Cleveland

(Responsible for verifying design)

Analex Denver

(Responsible for IV&V of flight software)

Aerospace

(Responsible for monitoring software development and test

LMA FAST Lab

(Responsible for system test of INU)

Third Space Launch Squadron (3SLS)

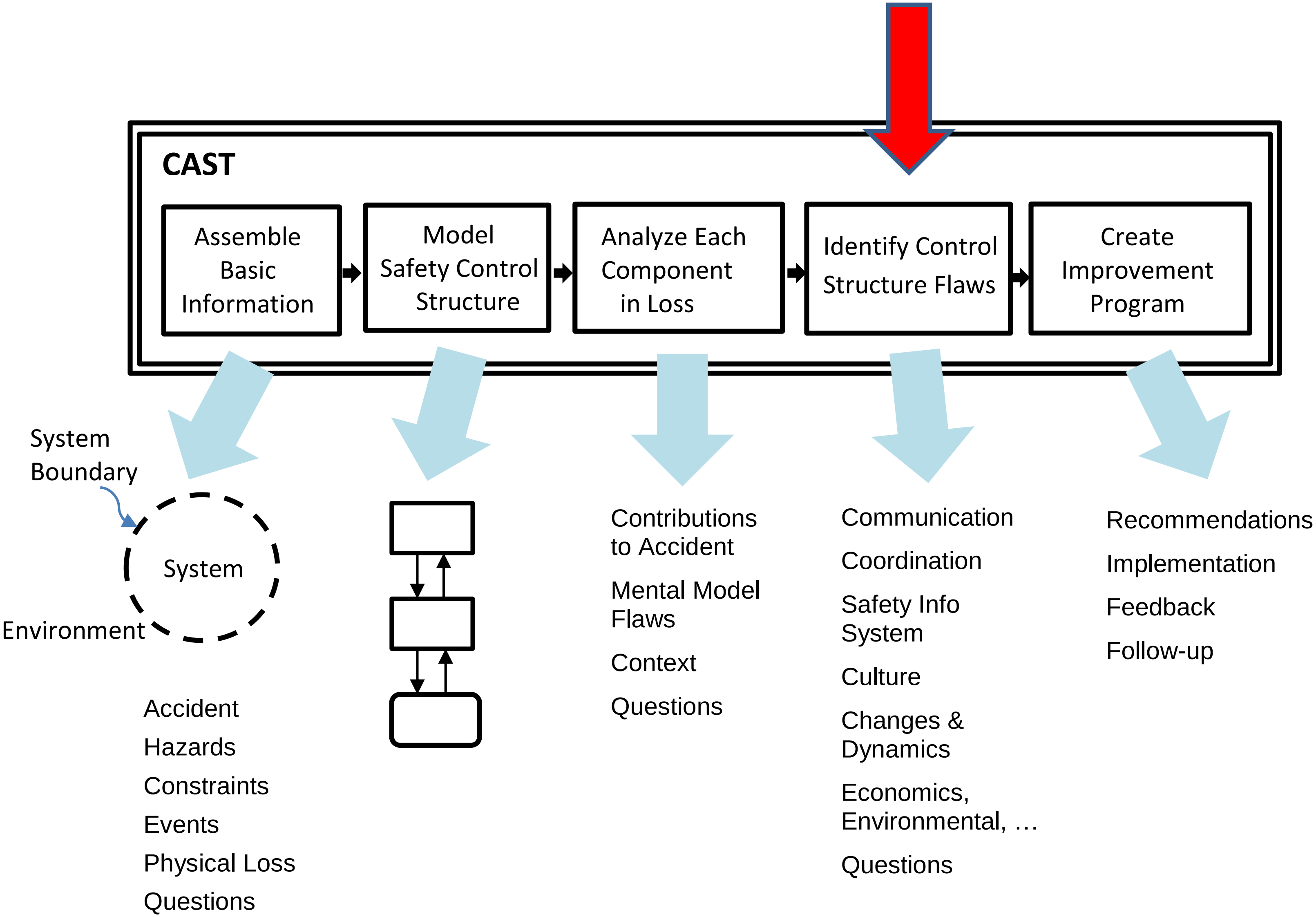
(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar

Overall

- Understanding why loss occurred and fixing the problems involves more than just identifying proximate cause (human error in transcribing long strings of digits). Known and should have been controls established throughout process to detect and fix it. Either missing or inadequately designed and implemented.



CAST

Assemble Basic Information → Model Safety Control Structure → Analyze Each Component in Loss → Identify Control Structure Flaws → Create Improvement Program

Accident
Hazards
Constraints
Events
Physical Loss
Questions

Contributions to Accident

Mental Model Flaws

Context

Questions

Communication

Coordination

Safety Info System

Culture

Changes & Dynamics

Economics, Environmental, …

Questions

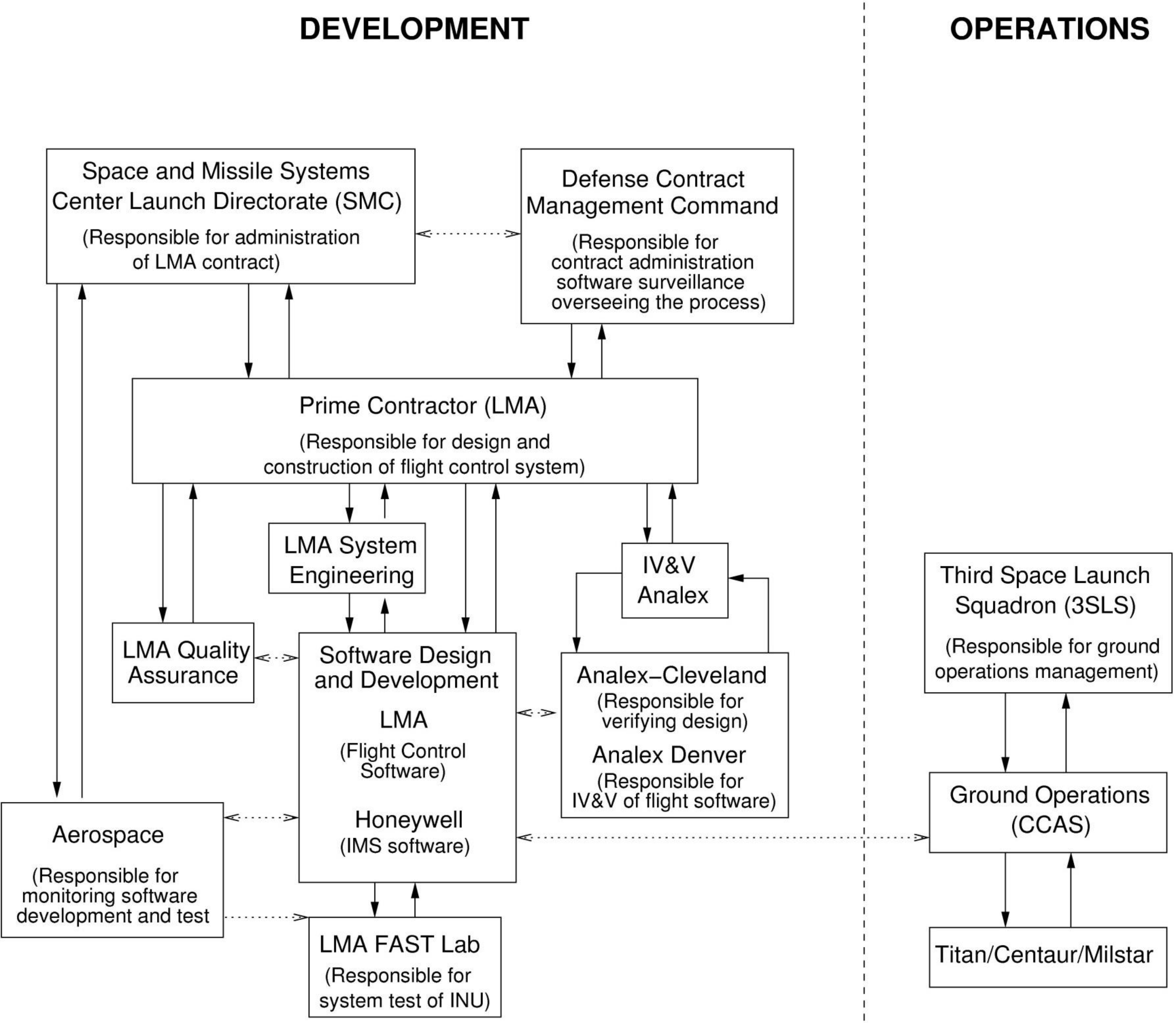
Recommendations

Implementation

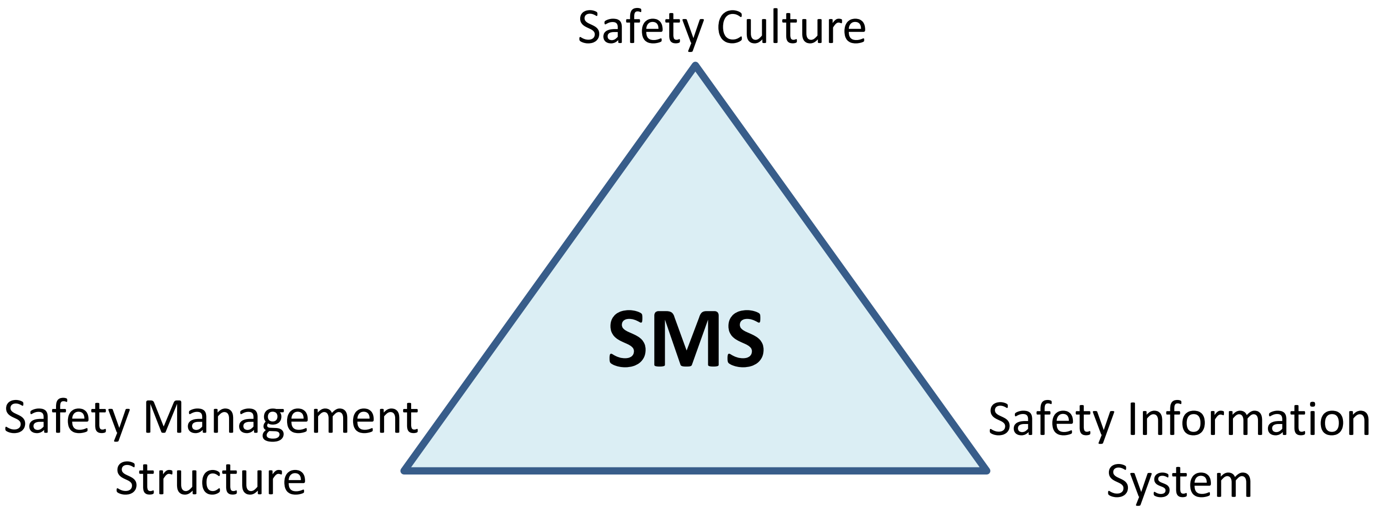
Feedback

Follow-up

- Each component worked correctly. But together did not enforce the safety constraints.
- So next need to look at flaws in the Safety Management System as a whole
- No checklists, these lead to accidents (both in hazard analysis and in accident analysis)


DEVELOPMENT
OPERATIONS
Space and Missile Systems Center Launch Directorate (SMC)
(Responsible for administration of LMA contract)
Defense Contract Management Command
(Responsible for contract administration software surveillance overseeing the process)
Prime Contractor (LMA)
(Responsible for design and construction of flight control system)
LMA System Engineering
IV&V Analex
LMA Quality Assurance
Software Design and Development
LMA
(Flight Control Software)
Honeywell
(IMS software)
Analex−Cleveland
(Responsible for verifying design)
Analex Denver
(Responsible for IV&V of flight software)
Aerospace
(Responsible for monitoring software development and test
LMA FAST Lab
(Responsible for system test of INU)
Third Space Launch Squadron (3SLS)
(Responsible for ground operations management)
Ground Operations (CCAS)
Titan/Centaur/Milstar

Three Parts to an SMS



- Culture defines desirable and effective behavior
- Safety management structure determines how cultural goals will be implemented
- Safety Information System provides information to make management structure successful

Flaws in Interactions Among Components and Overall Safety Control Structure

- Safety Information System
  - Formal anomaly reporting system did not exist or was not used. Why? A “concern” and not a “deviation.”

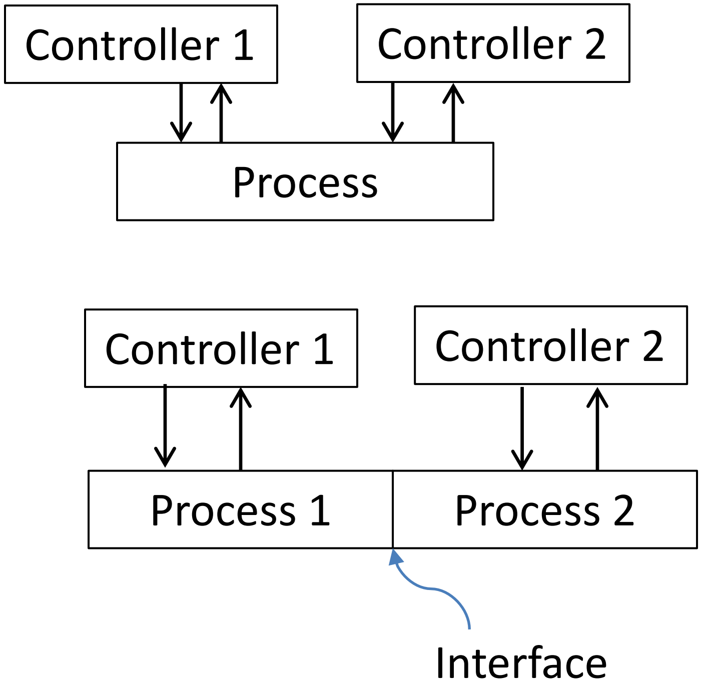
- Safety Culture
  - Considered a mature program so did not need extensive safety program? (MIL-STD-882, where was it?, does it continue into operations?)

Overall Control Structure

- Communication and Coordination (including communication channels and feedback)
  - Lack of effective feedback channel from launch site to LMA (developers)
  - LMA engineers in Denver did not speak directly with CCAS engineers
  - Accidents often in interfaces between departments
  - What coordination between SMC, DCMC, and Aerospace Corp? (not in accident report)

- Communication and coordination (continued)
  - Responsibility diffused among various partners, complete coverage. In the end, nobody tested the load tape and everyone thought someone else was doing it.
  - Fragmented and stovepiped software development process
  - No comprehensive and defined system and software engineering processes among all the partners
    - IMS software developed by Honeywell. Focus of all the LMA engineers and AF Program Office personnel focused on flight control software and had little knowledge of IMS software.
    - Honeywell delivered IMS software to LMA and assumed would be tested properly in system test.

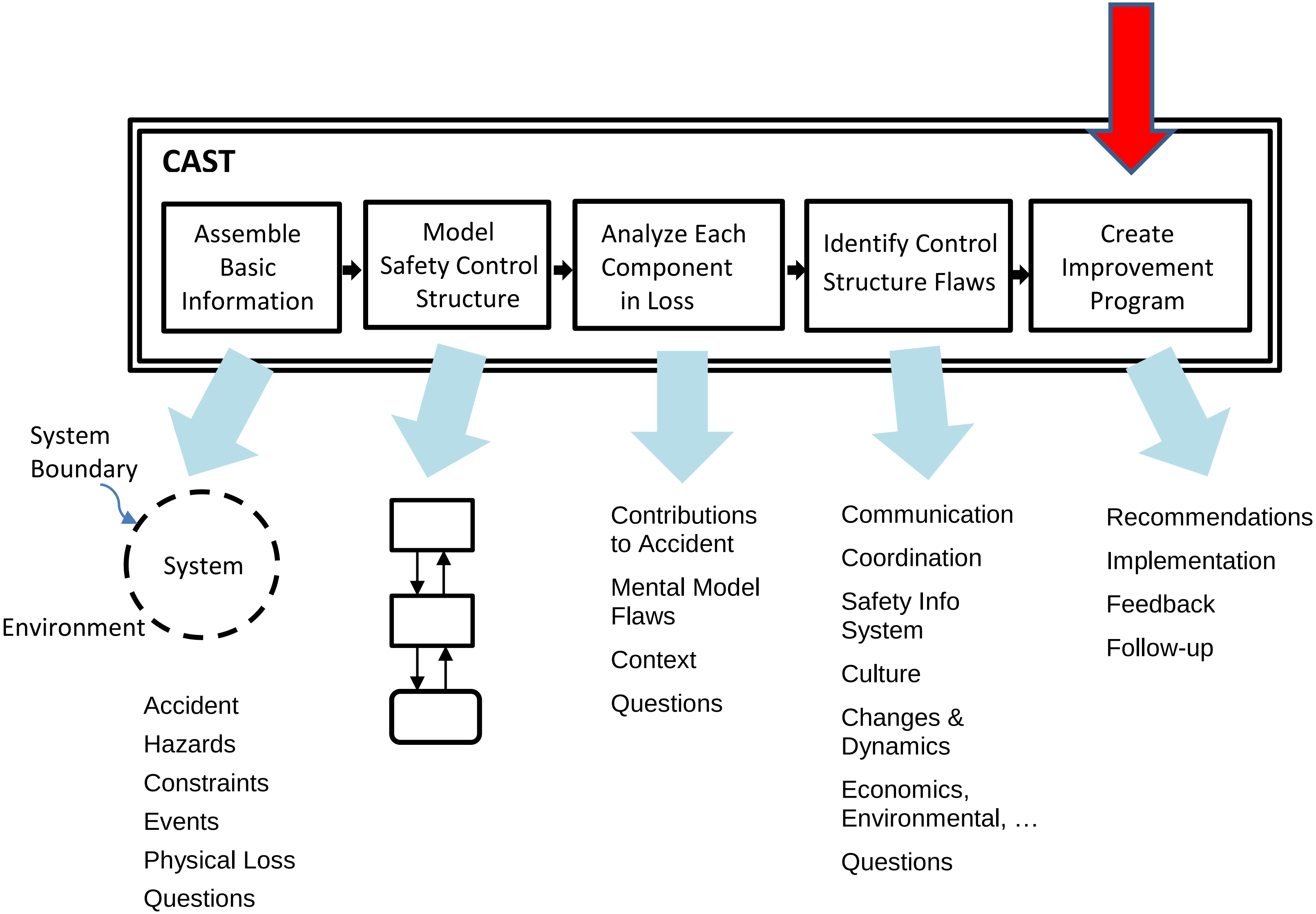
Common Coordination Problems



- Everyone assumes someone else taking care of it
- At boundary and nobody thinks it is their responsibility

- Confusion about responsibilities
  - Nobody assigned responsibility for monitoring software behavior after loaded in INU. Lack of coordination of responsibilities (lack of understanding of each other’s responsibilities between LMA Denver and LMA launch personnel at CCAS.
  - Lots of “holes” or “gaps” in responsibilities

- Dynamics and Changes over Time
  - Centaur software process developed early n program. Many of individuals who designed it were no longer involved in it due to corporate mergers and restructuring and maturation of Titan IV program. Much of system and process history and design rationale was lost with their departure.
  - Software filter used was not needed and should have been left out. Kept in for “consistency.”
  - Originally FAST lab constructed with capability to exercise actual flight values for the roll rate filter constants, but not widely known by current FAST software engineers. Knowledge of capability had been lost in corporate consolidation and evolution process. So used a default set of constants.



CAST

Assemble Basic Information

Model Safety Control Structure

Analyze Each Component in Loss

Identify Control Structure Flaws

Create Improvement Program

System Boundary

System

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, Environmental, …

Questions

Recommendations

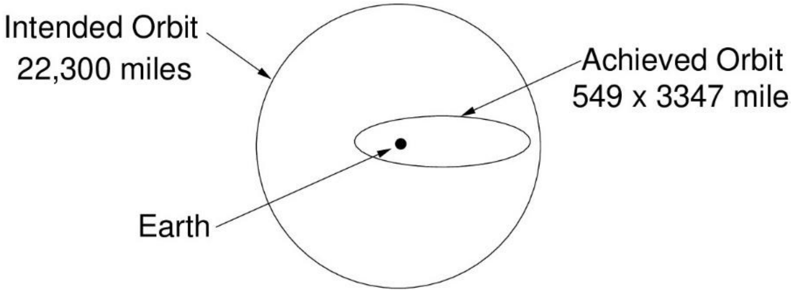
Implementation

Feedback

Follow-up

Chain of Events

- Roll rate filter constant incorrectly entered manually (typo) into load tape (-0.1992476 instead of -1.992476)
- Incorrect roll rate filter constant zeroed any roll rate data
- Resulted in loss of roll axis control
- Which then caused loss of yaw and pitch control
- Led to excessive firings of Reaction Control System
- Leading to hydrazine depletion
- Erratic vehicle flight during Centaur main engine burns caused an orbit apogee and perigee much lower then desired
- Resulted in Milstar separating in a useless low final orbit



1. **Root cause?**
2. **Recommendations?**
3. **Questions raised?**