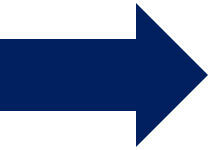
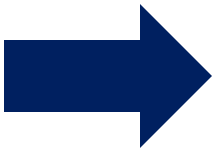
CAST Analysis

CAST Process



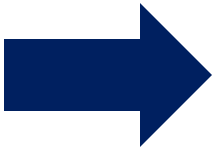
- Identify the Accident (Loss)
- Identify the Hazards
- Identify the Safety Constraints
- Identify the Proximal Events
- Draw the Safety Control Structure
- Analyze each component

CAST Process



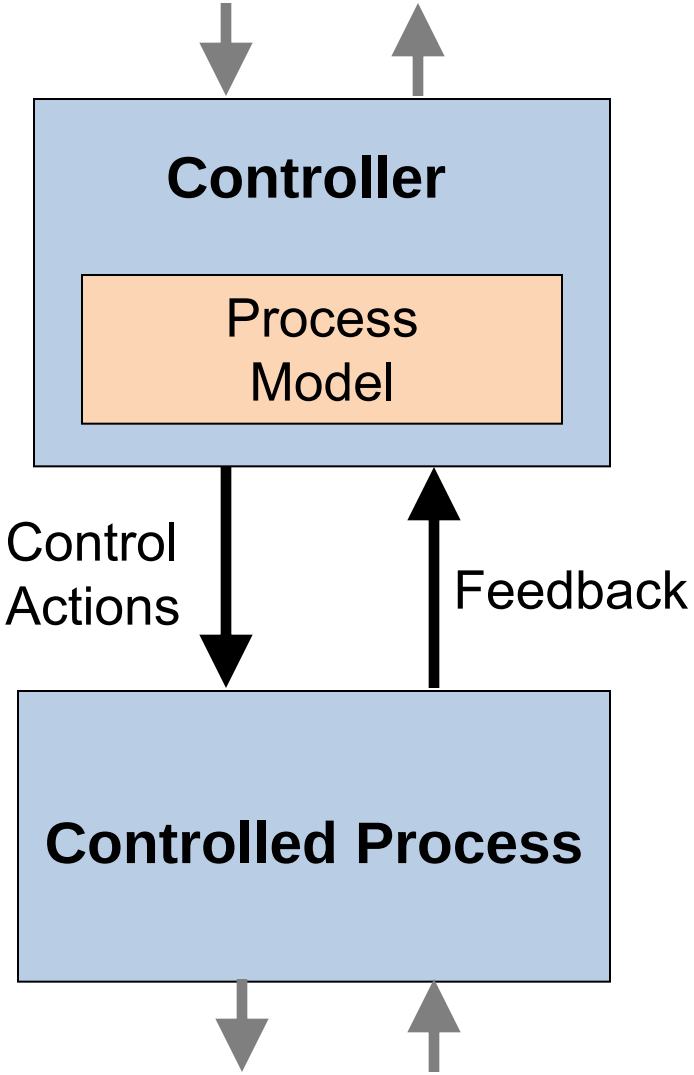
- Identify the Accident (Loss)
- Identify the Hazards
- Identify the Safety Constraints
- Identify the Proximal Events
- Draw the Safety Control Structure
- Analyze each component

CAST Process

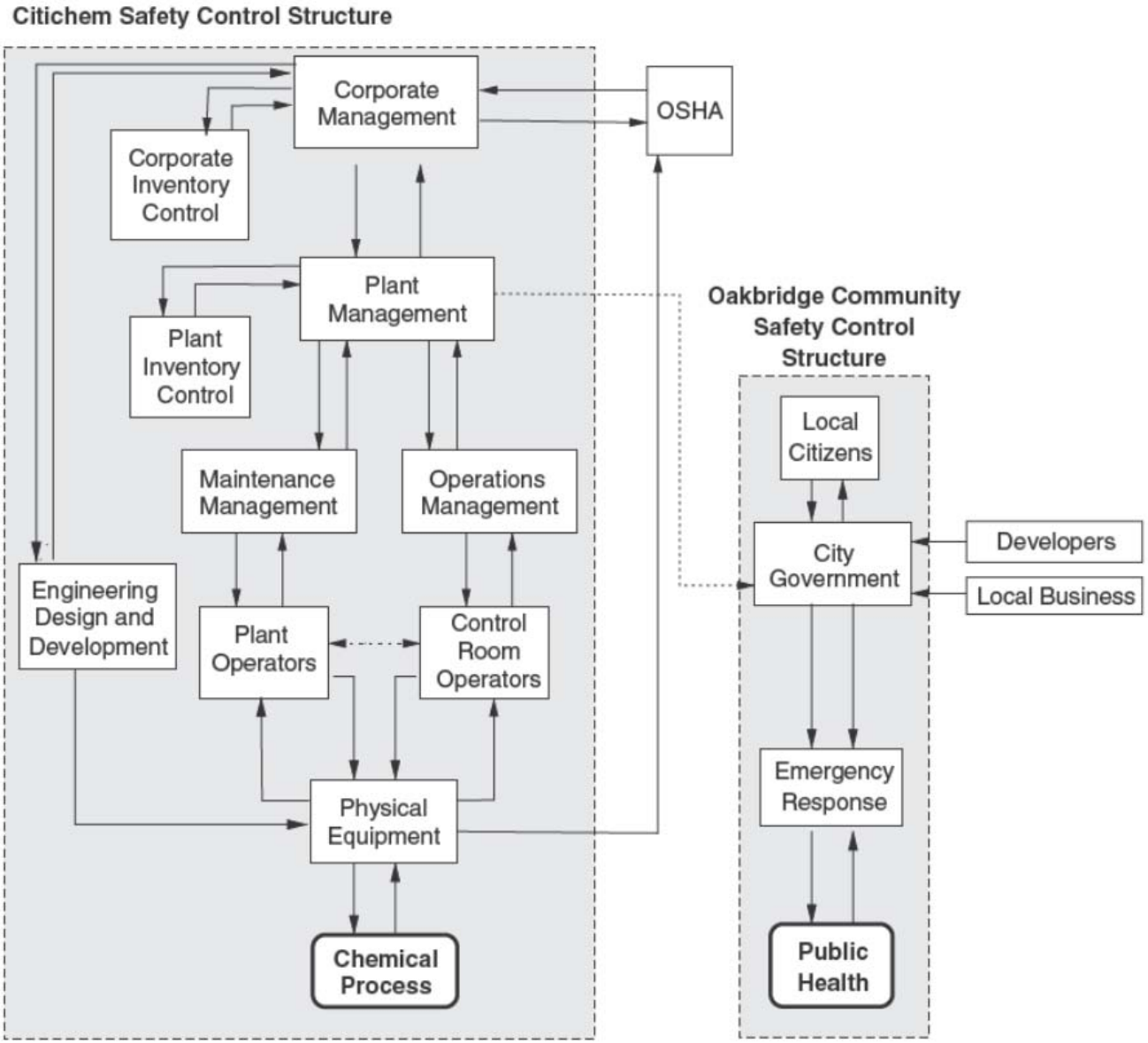


- Identify the Accident (Loss)
- Identify the Hazards
- Identify the Safety Constraints
- Identify the Proximal Events
- Draw the Safety Control Structure
- Analyze each component

Basic Control Loop

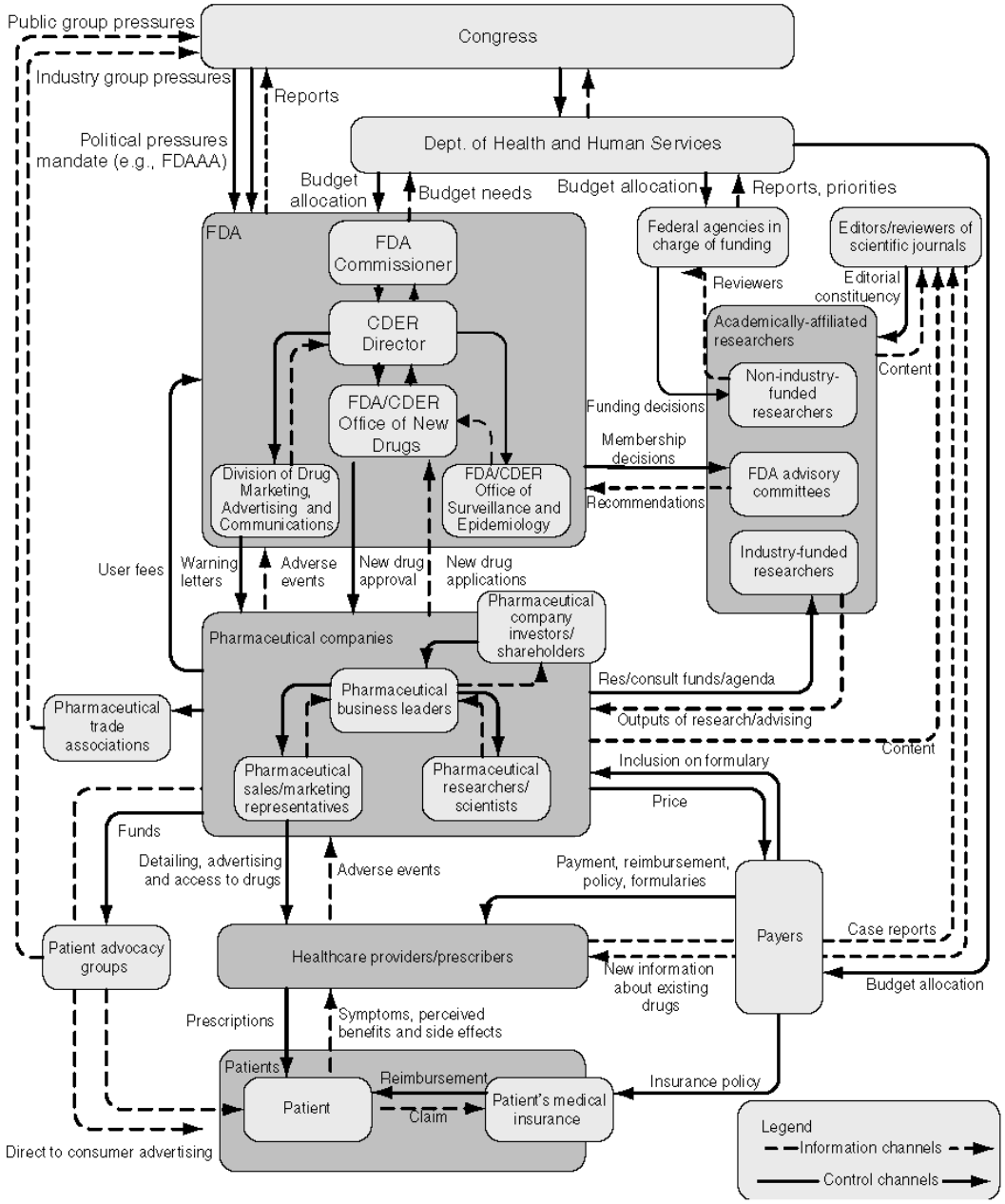


Safety Control Structure



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

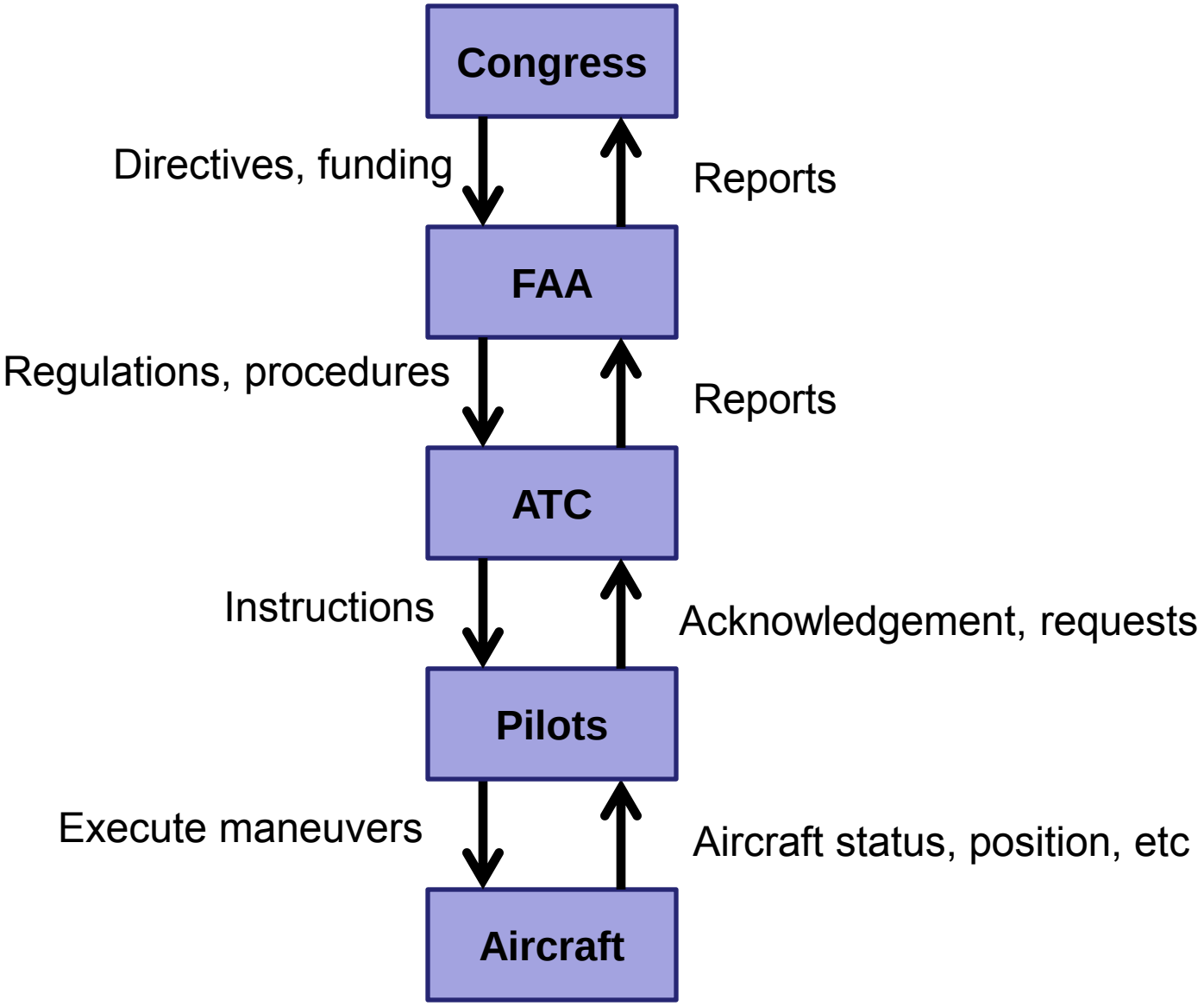
ESW p354



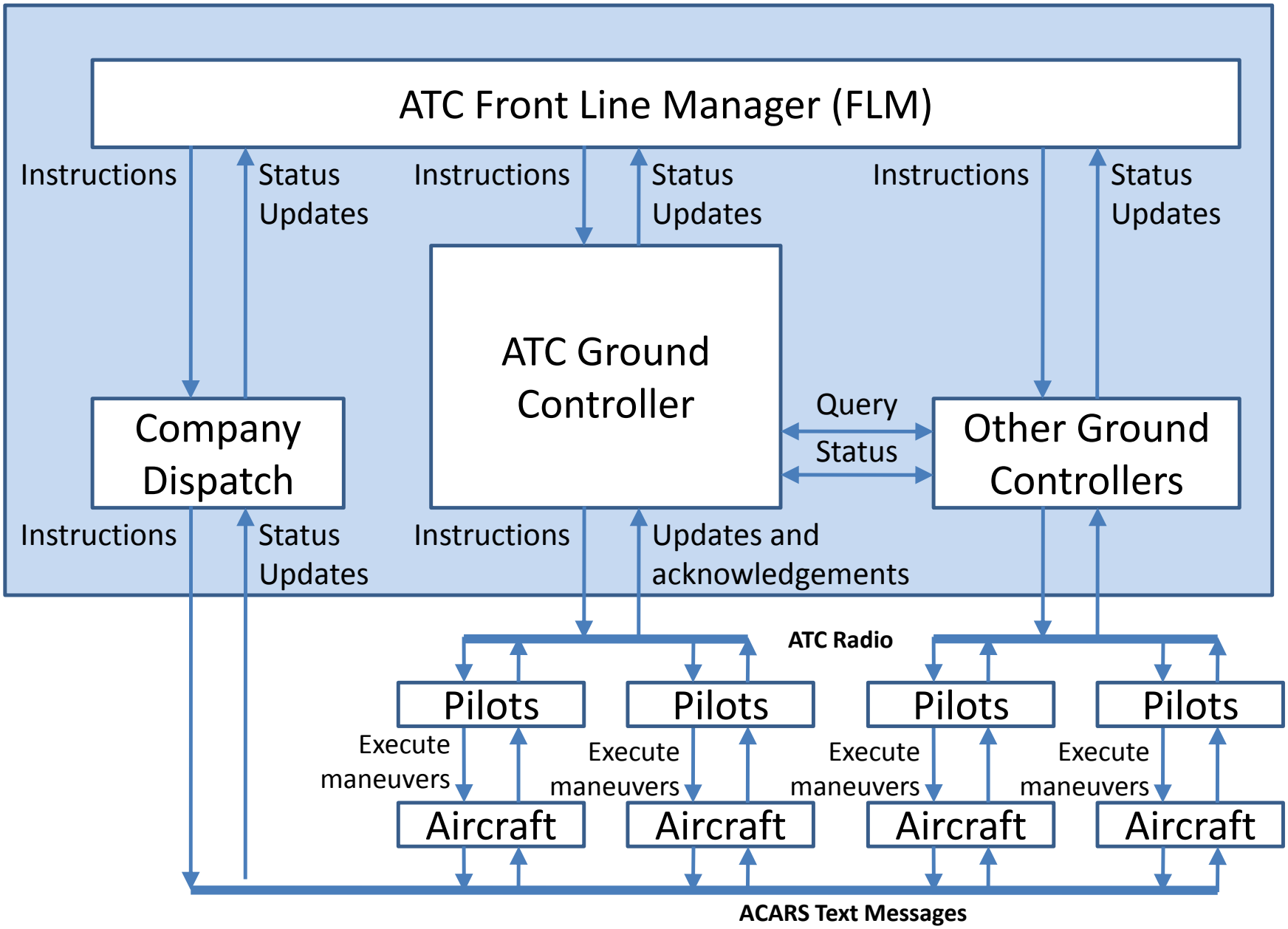
From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

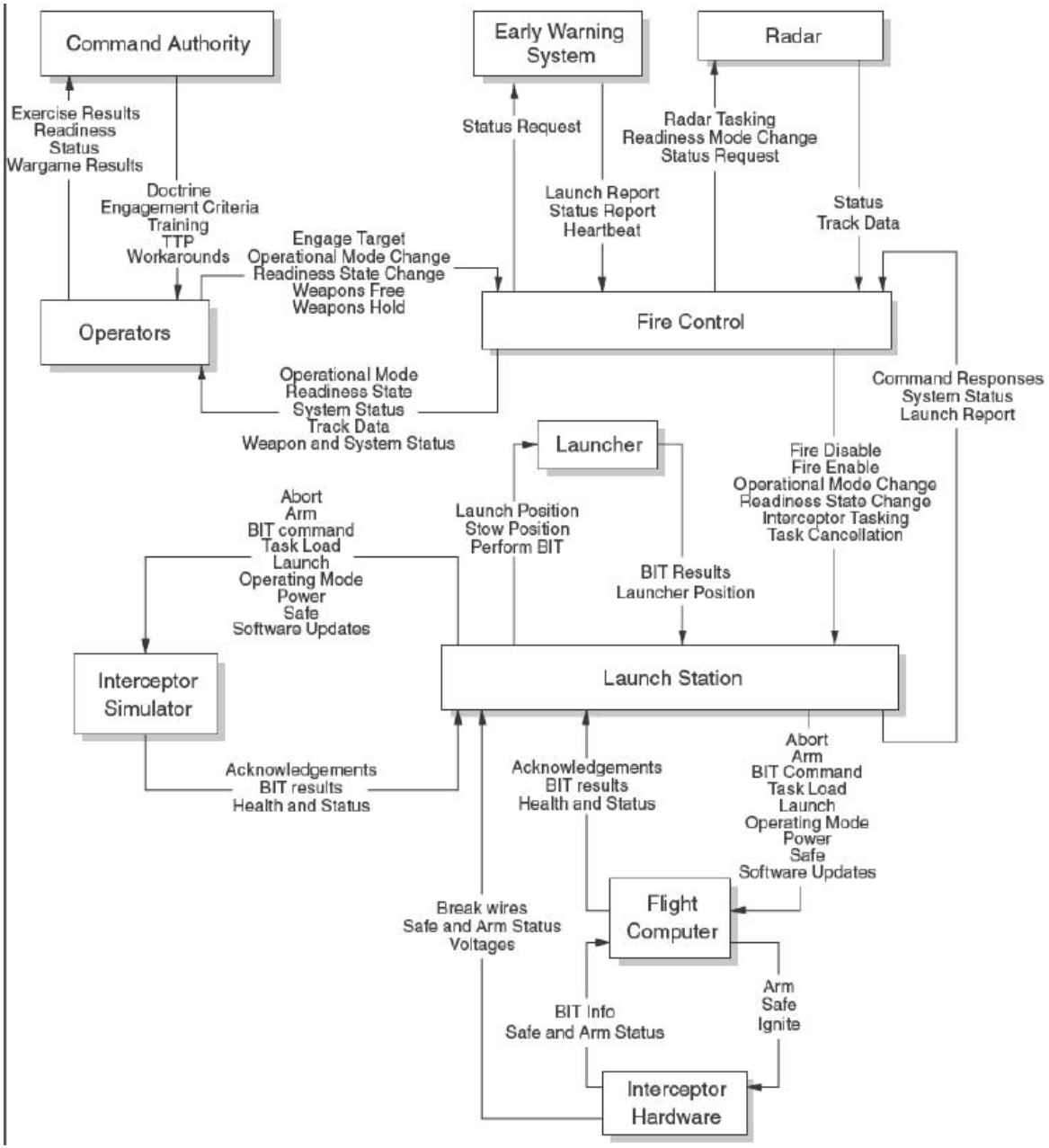
ESW p206: U.S. pharmaceutical safety control structure

Example High-level control structure



Air Traffic Control (ATC)



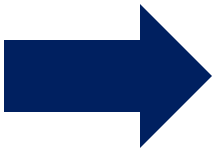


From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

ESW p216: Ballistic Missile Defense System

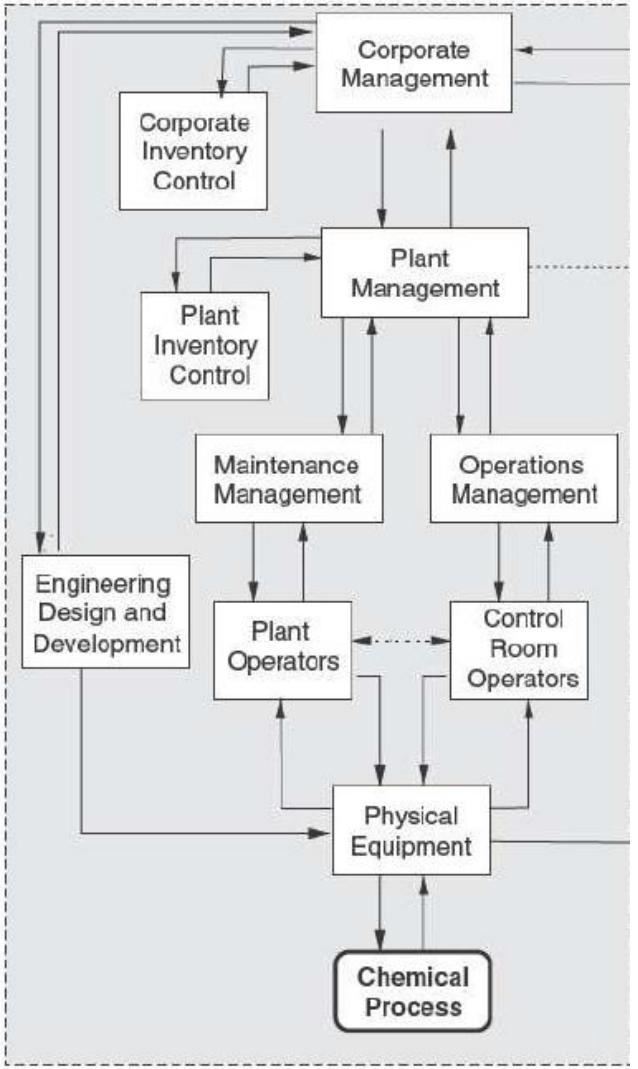
CAST Process

- Identify the Accident (Loss)
- Identify the Hazards
- Identify the Safety Constraints
- Identify the Proximal Events
- Draw the Safety Control Structure
- Analyze each component
  - Physical System
  - Controllers



Analyze physical system

- Responsibilities (safety constraints)
  - ?
- Emergency and Safety Equipment (controls)
  - ?
- Failures and inadequate controls
  - ?
- Contextual Factors
  - ?



Physical System

From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Analyze physical system

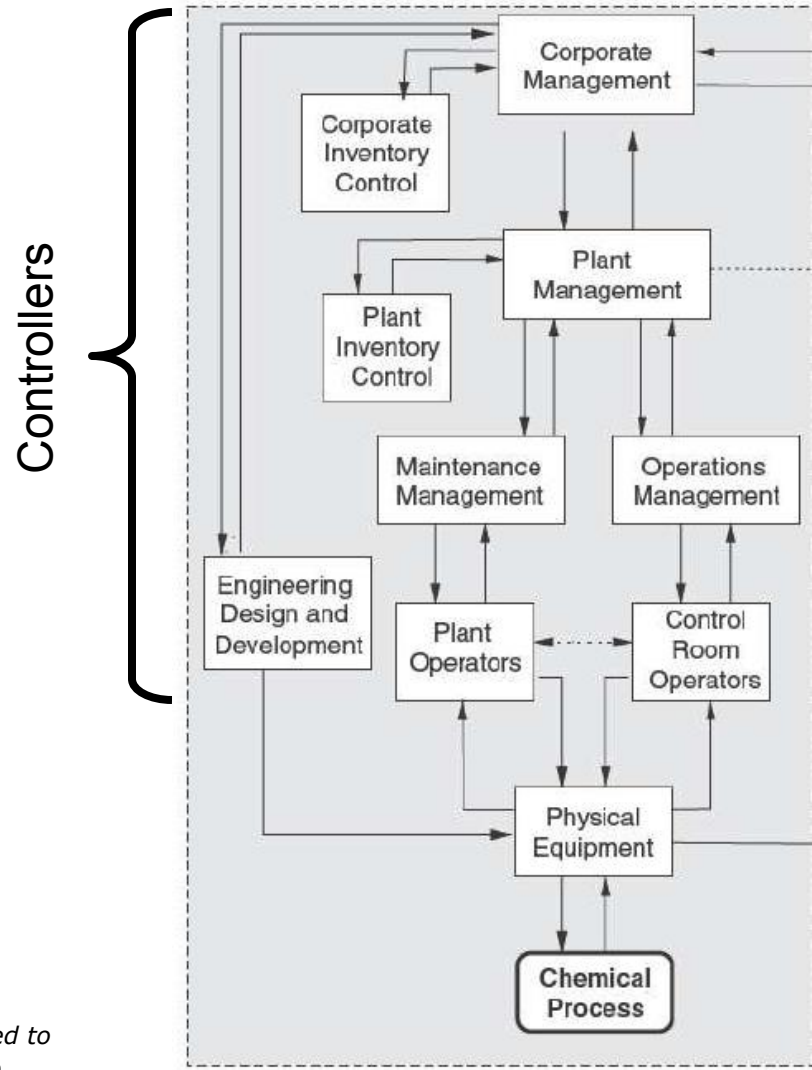
- Responsibilities (safety constraints)
  - Prevent runaway reactions
  - Prevent inadvertent release of toxic chemicals or explosion
  - Convert released chemicals into a nonhazardous of less hazardous form
  - Provide indicators (alarms) of the existence of hazardous conditions
- Emergency and Safety Equipment (controls)
  - Air monitors
  - Windsock
  - Pressure relief system
  - Process sensors, gauges and indicators
  - Spare tank

Analyze physical system (cont)

- Failures and Inadequate Controls
  - Inadequate protection against water getting into tanks
  - Inadequate monitoring of chemical process: Gauges were missing or inoperable
  - Inadequate emergency relief system (jammed, valves too small, lines too small)
- Contextual Factors
  - The plant was built in a remote location 30 years ago so it would have a buffer area around it,
  - but the city grew closer over the years
  - Approximately 24 different chemical products are manufactured at Oakbridge, most of which are toxic to humans and some very toxic
  - At the time of the start of the accident proximal events, Unit 7 was shut down and was not being used. It was restarted to provide extra K34
  - The plant already was operating at capacity before the decision to increase production of K34

Analyze controllers

- Operations Manager
- Software systems
- Maintenance Manager/Worker
- Plant Manager
- Corporate Management
- Etc.



From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Analyze Controller: Operations Manager

- Safety-related responsibilities
  - ?
- Unsafe Decisions and Control actions
  - ?
- Process model flaws
  - ?
- Context
  - ?

Analyze Controller: Operations Manager

- Safety-related responsibilities
  - Develop operating procedures that adequately control hazards
  - Provide operator training on plant hazards and safe operating procedures. Audit to ensure training is effective
  - Oversee operations to ensure that policies and procedures are being followed
- Unsafe Decisions and Control actions
  - Decides to take level gauge from tank 702 and put it on 701; runs unit 7 without a level gauge on 702. Ignores concerns by operators about operating a tank with no gauge
  - Agrees to or makes changes without thoroughly analyzing hazards involved
  - Agrees to start unit 7 in ten days knowing he does not have the personnel to do a thorough inspection and adequate startup activities

Analyze Controller: Operations Manager (cont)

- Process model flaws
  - Thinks tank 702 is empty. Does not know that water was found by maintenance in tank 701.
  - Inaccurate assessment of likelihood of having to use Tank 702
  - Like the others, most likely does not understand the limitations of the design of the safety equipment
- Context
  - Under same performance pressures as everyone else
  - No organization responsible for safety analyses and risk assessments
  - Understaffed

A note about
Unsafe Control Actions vs. Hazards

- Hazards
  - Generally should not name a specific component
  - Should describe general behavior of the system (aircraft, train, space vehicle, chemical plant, etc.)
- Unsafe Control Actions (UCAs)
  - Describe behavior of a specific component (pilot, manager, software automation, etc.)
  - Cause system-level hazards

16.63J / ESD.03J System Safety
Fall 2012