Analyzing Accidents

Agenda

- Discuss assignment 1
  - Citichem video
- Design for safety and hindsight bias
- Introduction to CAST accident analysis
- Assignment 2

Citichem Video

Design for Safety

- Eliminate or control scenarios (causal factors) identified by hazard analysis
- Fault Tolerance
  - Failures will occur
  - Need to make sure they don't result in an accident
- Design to prevent operator error
  - Human errors will occur
  - Need to make sure they don't result in an accident
  - Design so that don't induce human error

AF 447 Video

- http://www.youtube.com/watch?v=8IBUf4HbIa8

AF 447

- In modern aviation, large commercial jets almost fly themselves. Voss said that on any given flight, pilots are manually flying the plane for only three minutes -- one minute and 30 seconds each for take-off and landing.
- "The fact is there aren't many opportunities for a pilot to hand fly the aircraft anymore," he said. "The truth is it's only a few minutes during each flight, maybe until they climb up to altitude. Many airlines don't even allow the hand flying for that long."
- At the heart of the heated debate over so-called "automation addiction," which is when pilots are overly dependent on computers to fly their planes, is the question of whether pilots are actually learning how to properly fly large commercial aircraft.

AF 447 (2)

- "Because of this sophistication and the ability of airplane to fly themselves, they don't have as many chances to actually fly the airplane, to actually exercise their stick and rudder capabilities," Bill Bozin, the vice president of safety and technical affairs at Airbus, told "Nightline" in June.
- In the wake of the Air France crash, Voss said "many airlines" were retraining their pilots on flying manually, but that much more needs to be done to overhaul pilot training programs around the world.

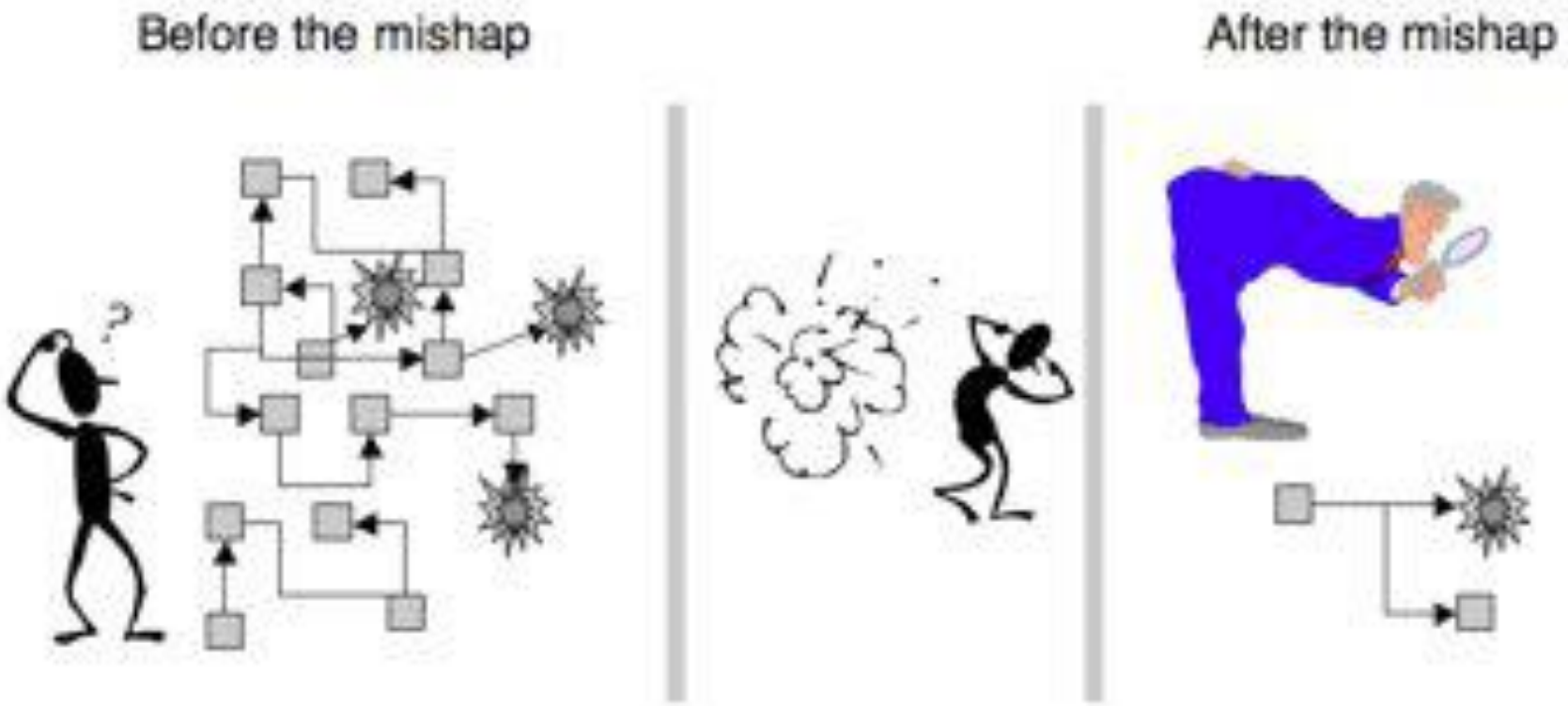
Lots of Issues with Humans and Automation

- Who has the final authority: humans or automation?
- Overreliance, lose skills
- Complacency, loss of attention

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
- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome

"Could have", "Should have", "If would have"



Sidney Dekker, 2009

Overcoming Hindsight Bias

- Need to consider why it made sense for people to do what they did
- Some factors that affect behavior
  - Goals person pursuing at time and whether may have conflicted with each other (e.g., safety vs. efficiency, production vs. protection)
  - Unwritten rules or norms
  - Information availability vs. information observability
  - Attentional demands
  - Organizational context

Hindsight Bias Examples

- Data availability vs. data observability
  - "The available evidence should have been sufficient to give the Board Operator a clear indication that Tank 731 was indeed filling and required immediate attention."

Board Control Valve Position: closed	Flow Meter: *shows no flow*
Bypass Valve: *closed*	SO_2 alarm: *off*
Level in tank: 7.2 feet	High level alarm: *off*

  - "Operators could have trended the data" on the control board

"Coulda, woulda, shoulda"

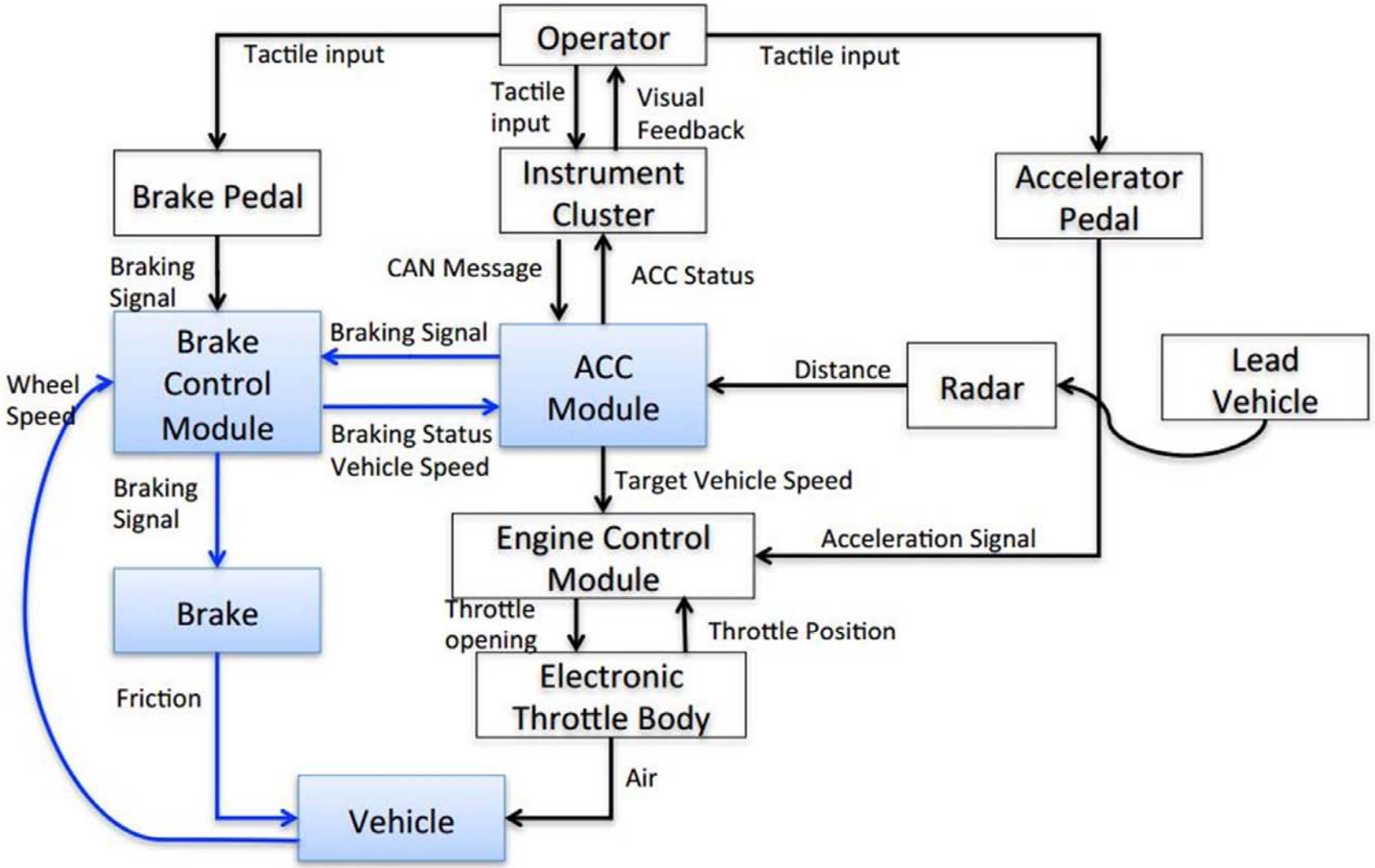
Hindsight Bias Examples

- Another example
  - "Interviews with operations personnel did not produce a clear reason why the response to the SO_2 alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation."

Safety Control Structure

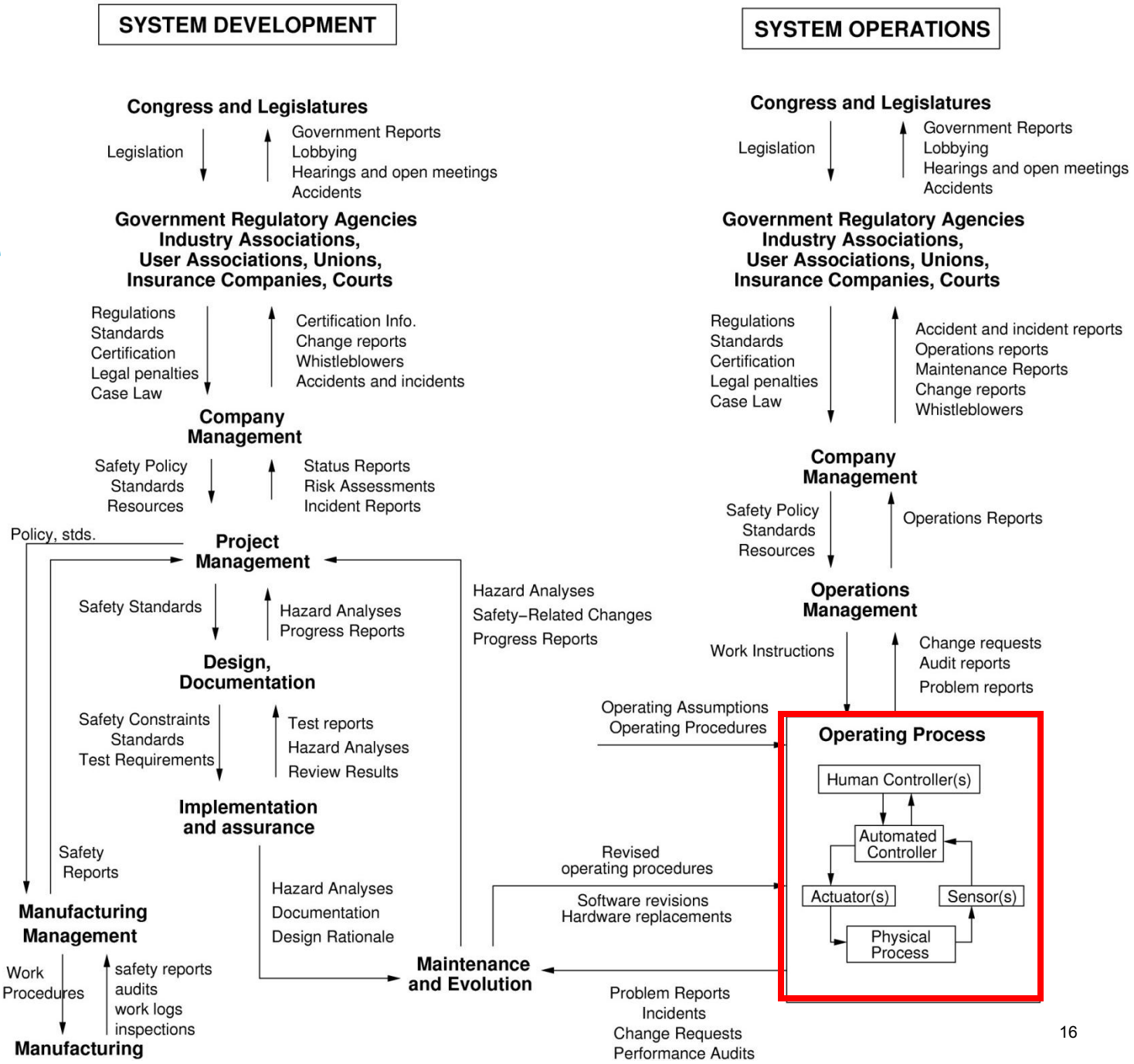
- Safety needs to be managed
- Hierarchical safety control structure used to maintain safety constraints.

Example: ACC – BCM Control Loop



Courtesy of Qi D. Van Eikema Hommes. Used with permission.

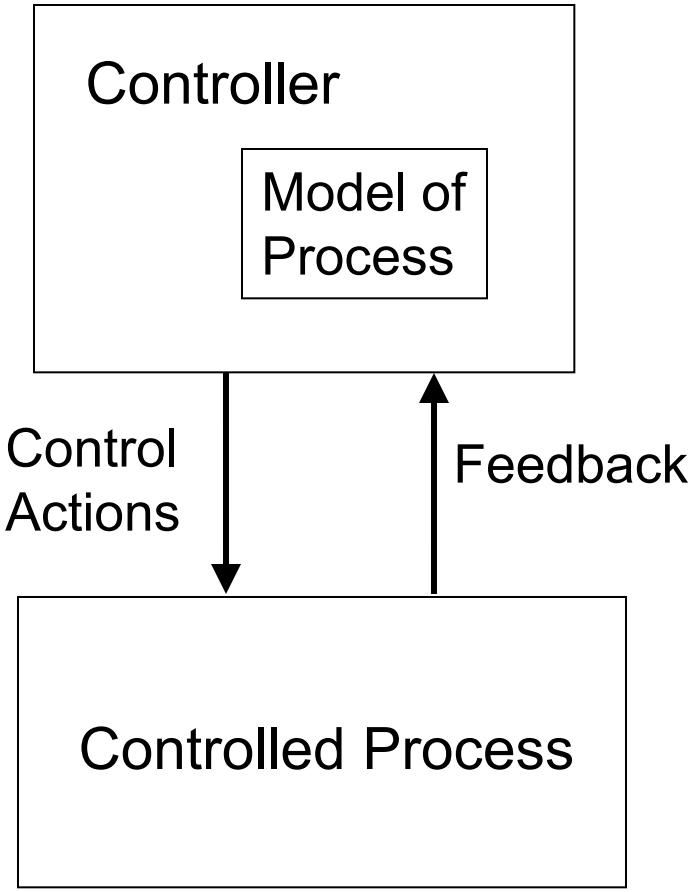
Example Safety Control Structure



Safety Constraints

- Each component in the control structure has
  - Assigned responsibilities, authority, accountability
  - Controls that can be used to enforce safety constraints
- Each component's behavior is influenced by
  - Context (environment) in which operating
  - Knowledge about current state of controlled process

Every Controller Contains a Process Model



Accidents occur when model of process is inconsistent with real state of process and controller provides inadequate control actions

Feedback channels are critical
-- Design
-- Operation

Citichem
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 (Next class)

Definitions

- Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

Accident	Hazard
Satellite becomes lost or unrecoverable	Satellite maneuvers out of orbit
People are exposed to toxic chemicals	Toxic chemicals are released into the atmosphere
People are irradiated	Nuclear power plant experiences nuclear meltdown
People die from food poisoning	Food products containing pathogens are sold

Definitions from ESW

Identify Accident, Hazards, Safety Constraints

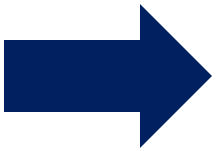
- Accident (Loss)
  - ?
- Hazard
  - ?
- Safety constraint
  - ?

Identify Accident, Hazards, Safety Constraints

- Accident (Loss)
  - Death, illness, or injury due to exposure to toxic chemicals.
- Hazard
  - Uncontrolled release of toxic chemicals
- Safety constraints
  - Chemicals must be under positive control at all times
  - Measures must be taken to reduce exposure if inadvertent release occurs
  - Means must be available to treat exposed individuals inside the plant

Additional hazards / constraints can be found in ESW p355

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 (Next class)

Proximal Events

- ?

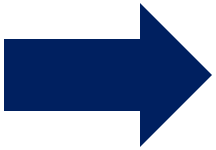
Proximal Events

1. **Rain gets into tank 701** (and presumably 702), both of which are in Unit 7 of the Citichem Oakbridge plant. Unit 7 was shut down at the time due to lowered demand for K34.
2. **Unit 7 is restarted** when a large order for K34 is received.
3. **A small amount of water is found** in tank 701 and an order is issued to make sure the tank is dry before startup.
4. T34 transfer is started at unit 7.
5. The **level** gauge transmitter in the 701 storage tank **shows more than it shou**ld.
6. **A request is sent to maintenance** to put in a new level transmitter.
7. The level transmitter from tank 702 is moved to tank 701. (Tank 702 is used as a spare tank for overflow from tank 701 in case there is a problem.)
8. **Pressure in Unit 7 reads as too high**.
9. The backup cooling compressor is activated.
10. Tank 701 temperature exceeds 12 degrees Celsius.
11. A sample is run, an operator is sent to check tank pressure, and the **plant manager is called.**
12. **Vibration is detected** in tank 701.
13. The temperature and pressure in tank 701 continue to increase.

Proximal Events

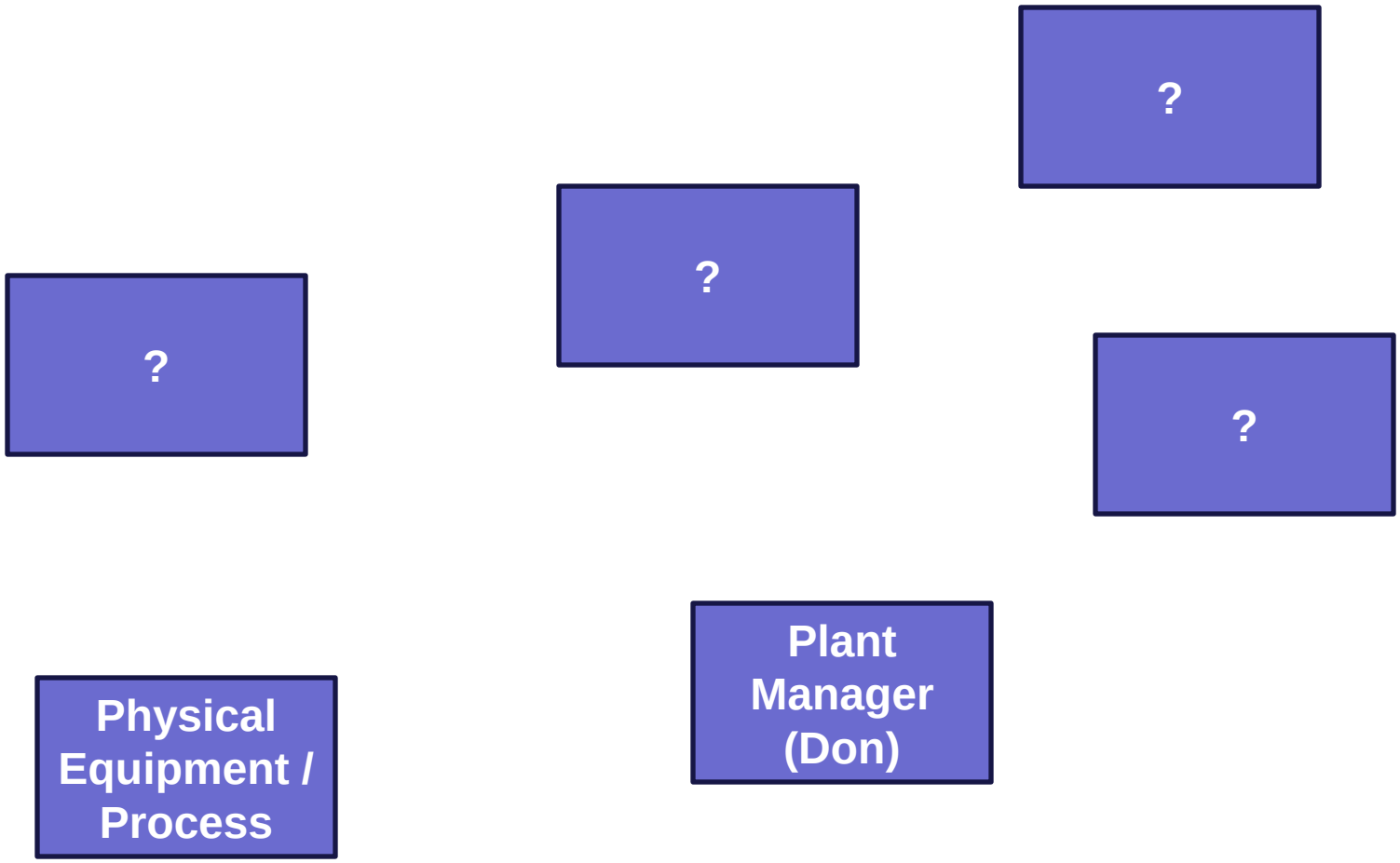
14. **Water is found** in the sample that was taken (see event 11).
15. Tank 701 is dumped into the spare tank 702
16. A **runaway reaction** occurs in tank 702.
17. The **emergency relief valve jams** and runoff is not diverted into the backup scrubber.
18. An **uncontrolled gas release** occurs.
19. An alarm sounds in the plant.
20. Nonessential personnel are ordered into units 2 and 3, which have positive pressure and filtered air.
21. People faint outside the plant fence.
22. Police evacuate a nearby school.
23. The engineering manager calls the local hospital, gives them the chemical name and a hotline phone number to learn more about the chemical.
24. The public road becomes jammed and emergency crews cannot get into the surrounding community.
25. Hospital personnel cannot keep up with steady stream of victims.
26. Emergency medical teams are airlifted in.

CAST Process

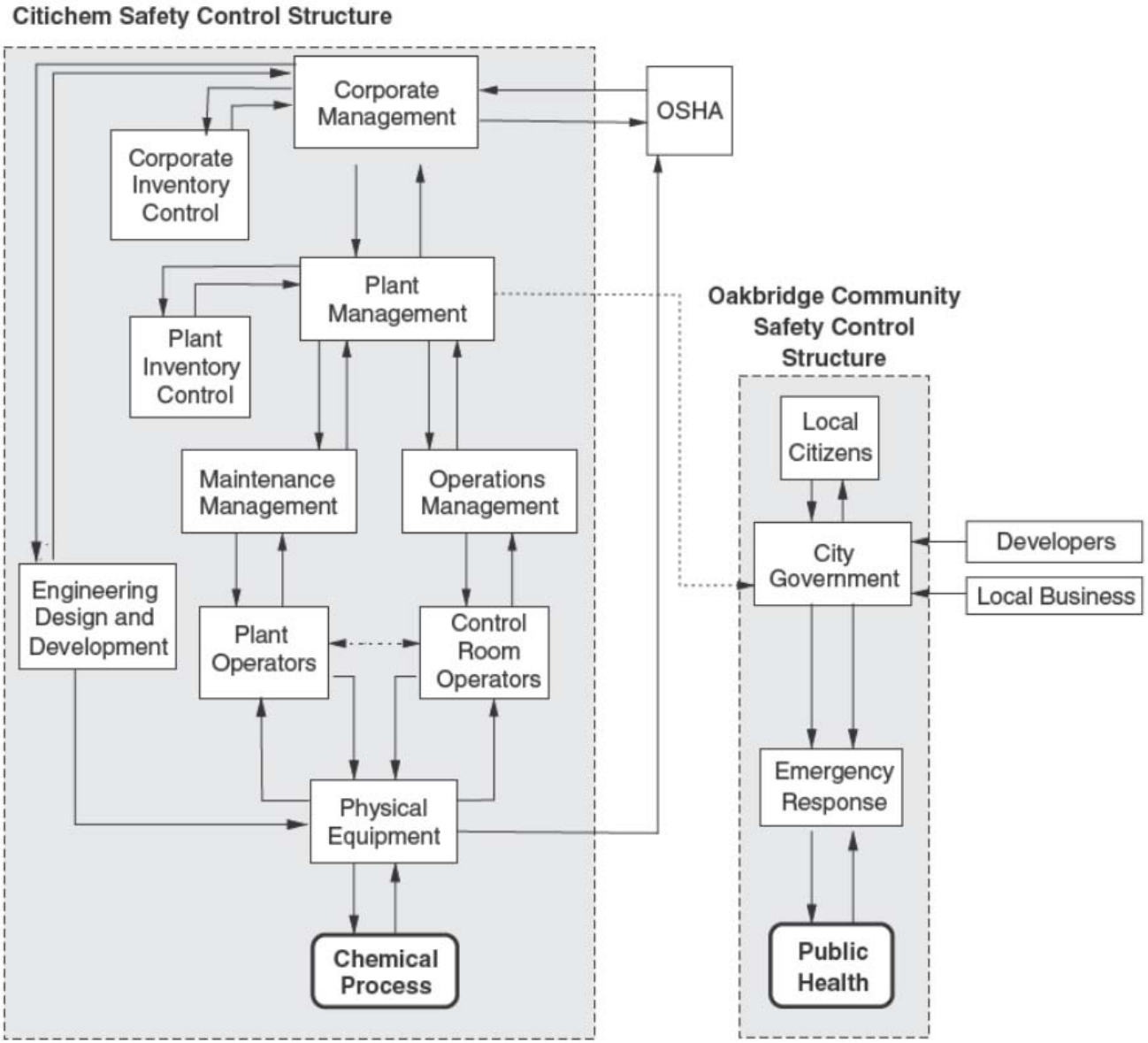


- Identify the Accident (Loss)
- Identify the Hazards
- Identify the Safety Constraints
- Identify the Proximal Events
- Draw the Safety Control Structure
- Analyze each component (Next class)

Safety Control Structure



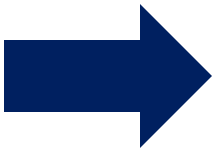
Safety Control Structure



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

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 (Next class)



16.63J / ESD.03J System Safety
Fall 2012