Systems Theory

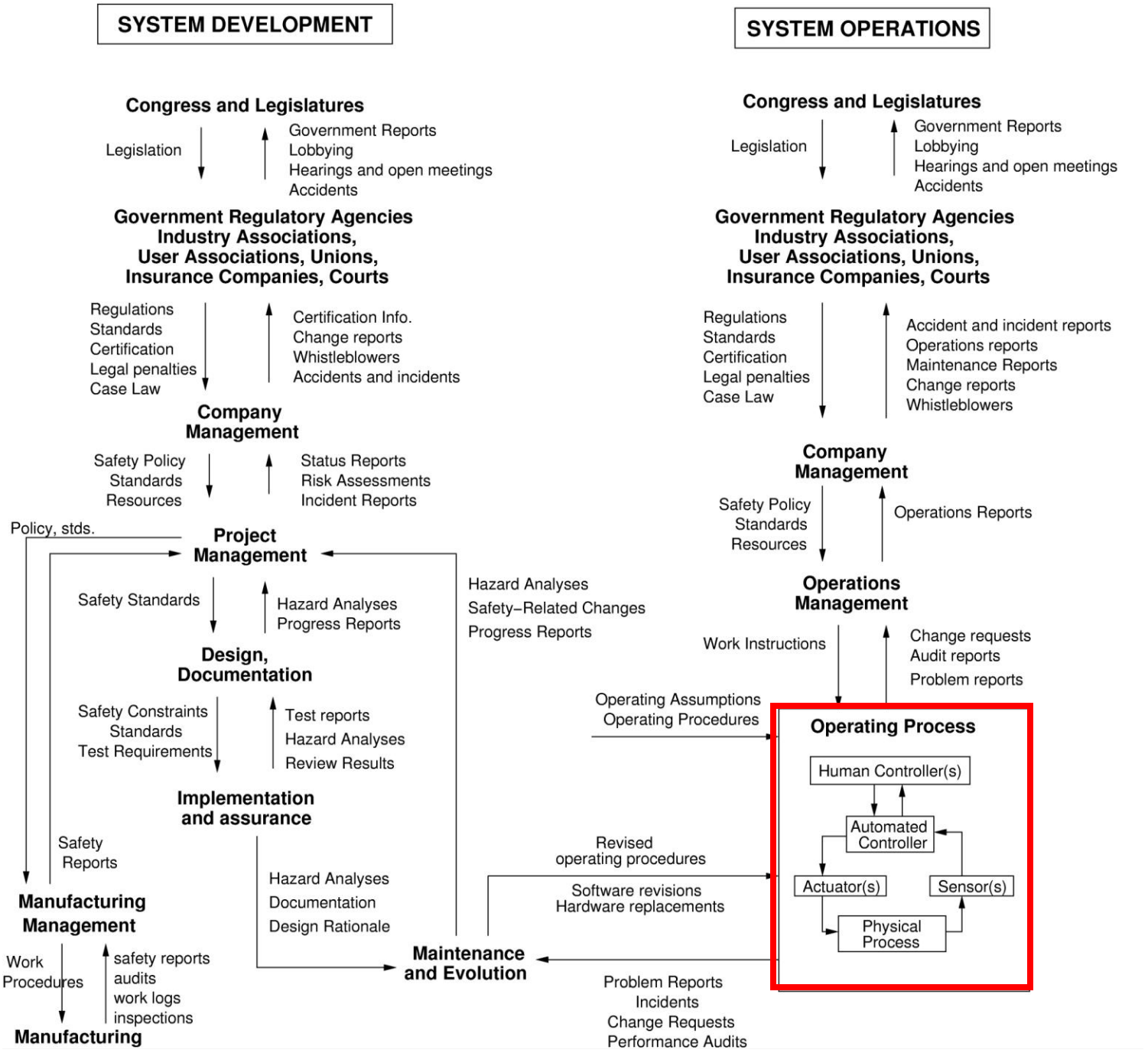
- Developed for biology (von Bertalanffy) and engineering (Norbert Wiener)
- Basis of system engineering and system safety (ICBMs of 1950s)
- Focuses on systems taken as a whole, not on parts taken separate
  - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects
  - These properties derive from relationships among the parts of the system

    How they interact and fit together

Hierarchy and Emergence

- Complex systems can be modeled as a hierarchy of organizational levels
  - Each level more complex than one below
  - Levels characterized by emergent properties
    - Irreducible
    - Represent constraints on the degree of freedom of components at lower level
- Safety is an emergent system property
  - It is NOT a component property
  - It can only be analyzed in the context of the whole

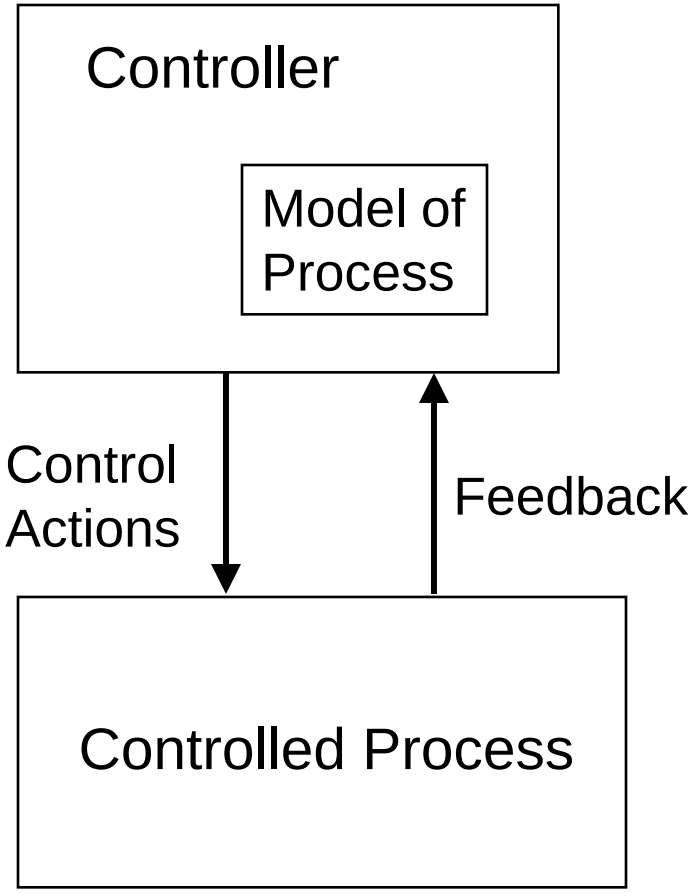
Example Safety Control Structure



Communication and Control

- Hierarchies characterized by control processes working at the interfaces between levels
- A control action imposes constraints upon the activity at a lower level of the hierarchy
- Systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback loops of information and control
- Control in open systems implies need for communication

Control processes operate between levels of control



Process models must contain:
- Required relationship among process variables
- Current state (values of process variables
- The ways the process can change state

Relationship Between Safety and Process Models

- Accidents occur when models do not match process and
  - Required control commands are not given
  - Incorrect (unsafe) ones are given
  - Correct commands given at wrong time (too early, too late)
  - Control stops too soon

(Note the relationship to component interaction accidents)

Explains software errors, human errors, component interaction accidents …

System's Theoretic View of Safety

- Safety is an emergent system property
  - Accidents arise from interactions among system components (human, physical, social)
  - That violate the constraints on safe component behavior and interactions
- Losses are the result of complex processes, not simply chains of failure events
- Most major accidents arise from a slow migration of the entire system toward a state of high-risk
- Based on systems theory rather than reliability theory

STAMP

- Treat safety as a dynamic control problem rather than a component failure problem.
  - O-ring did not control propellant gas release by sealing gap in field joint of Challenger Space Shuttle
  - Software did not adequately control descent speed of Mars Polar Lander
  - Temperature in batch reactor not adequately controlled in system design
  - Public health system did not adequately control contamination of the milk supply with melamine
  - Financial system did not adequately control the use of financial instruments
- Events are the result of the inadequate control
  - Result from lack of enforcement of safety constraints in system design and operations

STAMP (3)

- A change in emphasis:

~~"prevent failures"~~

↓

"enforce safety constraints on system behavior"

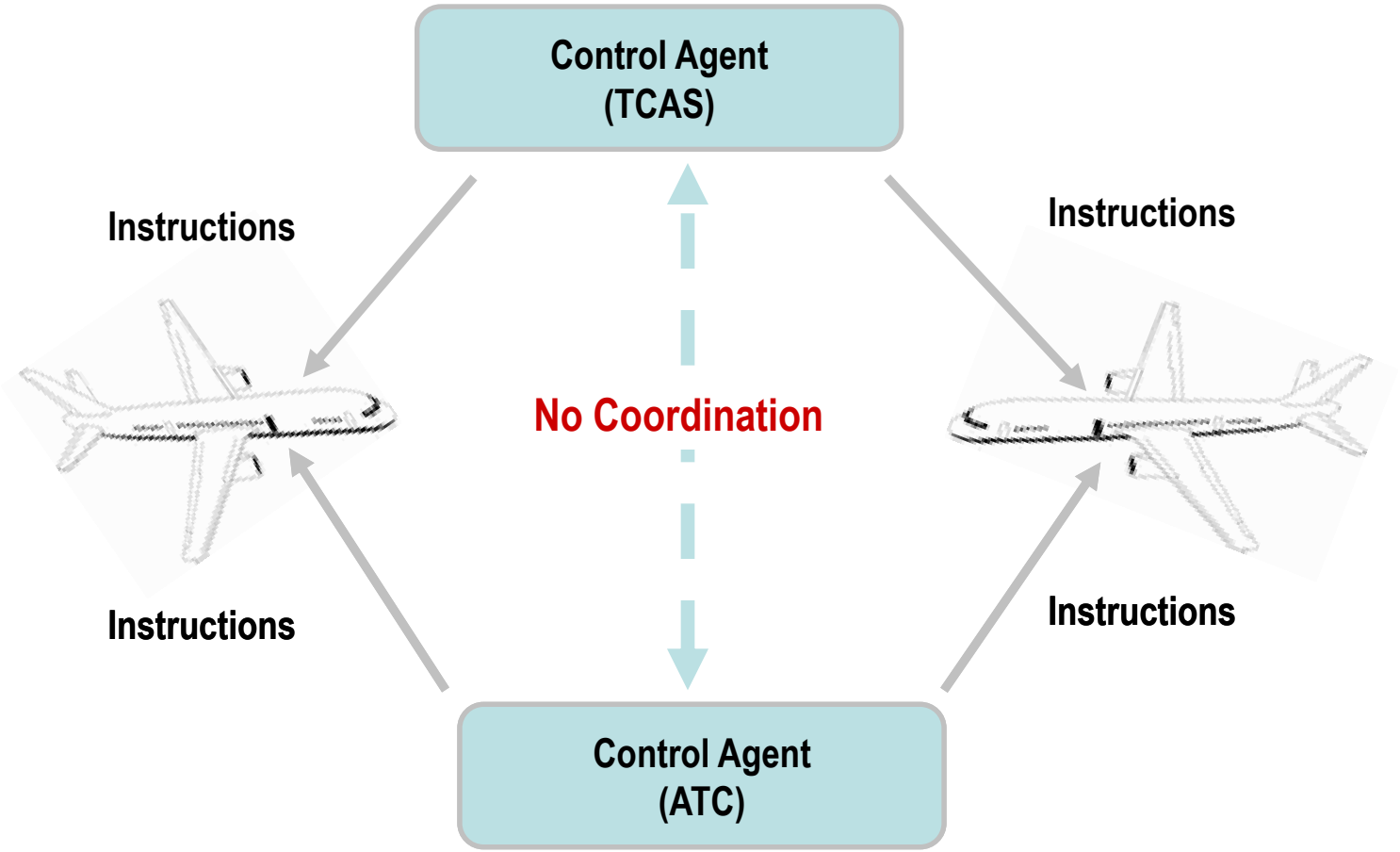
- Losses are the result of complex dynamic processes, not simply chains of failure events
- Most major accidents arise from a slow migration of the entire system toward a state of high-risk
  - Need to control and detect this migration

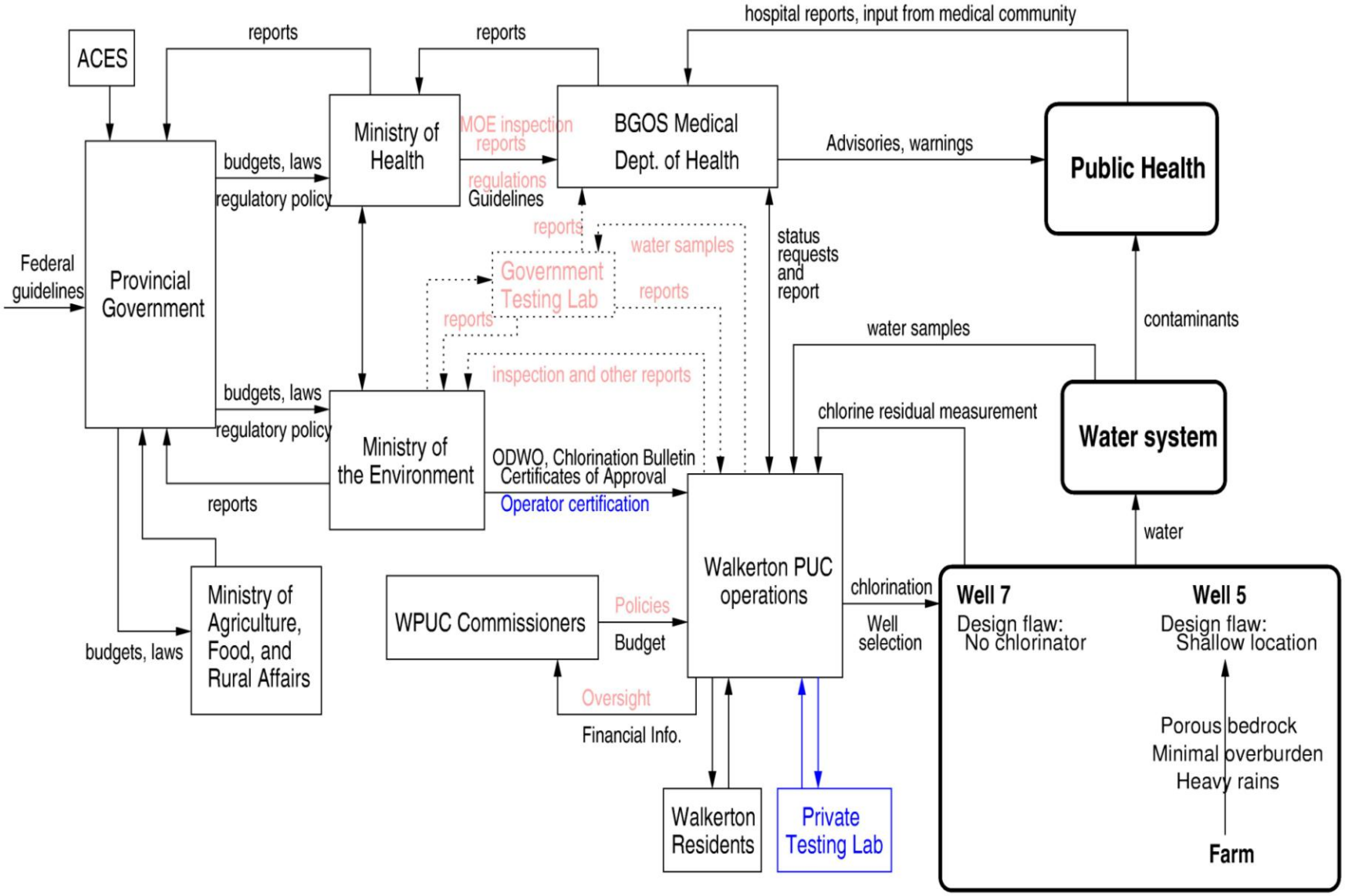
Summary: Accident Causality

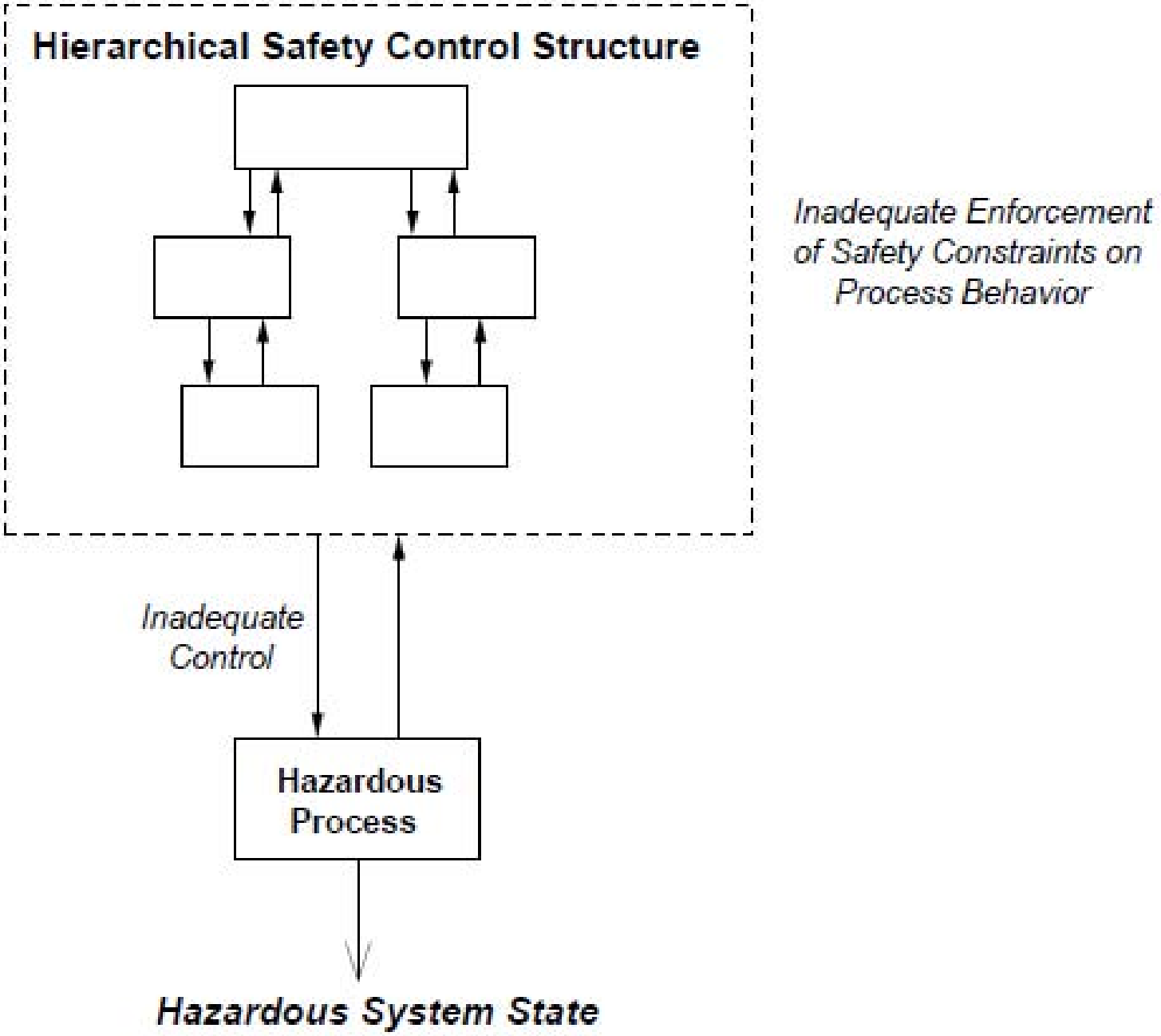
- Accidents occur when
  - Control structure or control actions do not enforce safety constraints
    - Unhandled environmental disturbances or conditions
    - Unhandled or uncontrolled component failures
    - Dysfunctional (unsafe) interactions among components
  - Control actions inadequately coordinated among multiple controllers
  - Control structure degrades over time (asynchronous evolution)

Uncoordinated “Control Agents”

“UNSAFE STATE”
BOTH TCAS and ATC provide uncoordinated & independent instructions




ACES
reports
reports
hospital reports, input from medical community
Ministry of Health
MOE inspection reports
BGOS Medical Dept. of Health
Advisories, warnings
Public Health
budgets, laws
regulatory policy
regulations
Guidelines
Federal guidelines
Provincial Government
reports
water samples
Government Testing Lab
reports
reports
status requests and report
contaminants
water samples
inspection and other reports
budgets, laws
regulatory policy
Ministry of the Environment
chlorine residual measurement
Water system
ODWO, Chlorination Bulletin
Certificates of Approval
Operator certification
reports
water
Ministry of Agriculture, Food, and Rural Affairs
budgets, laws
WPUC Commissioners
Policies
Budget
Walkerton PUC operations
chlorination
Well selection
Well 7
Design flaw:
No chlorinator
Well 5
Design flaw:
Shallow location
Oversight
Financial Info.
Porous bedrock
Minimal overburden
Heavy rains
Farm
Walkerton Residents
Private Testing Lab


Hierarchical Safety Control Structure
Inadequate Enforcement of Safety Constraints on Process Behavior
Inadequate Control
Hazardous Process
Hazardous System State

Uses for STAMP

- More comprehensive accident/incident investigation and root cause analysis
- Basis for new, more powerful hazard analysis techniques (STPA)
- Safety-driven design (physical, operational, organizational))
  - Can integrate safety into the system engineering process
  - Assists in design of human-system interaction and interfaces
- Organizational and cultural risk analysis
  - Identifying physical and project risks
  - Defining safety metrics and performance audits
  - Designing and evaluating potential policy and structural improvements
  - Identifying leading indicators of increasing risk (“canary in the coal mine”)

Does it work? Is it practical?

Technical

- Safety analysis of new missile defense system (MDA)
- Safety-driven design of new JPL outer planets explorer
- Safety analysis of the JAXA HTV (unmanned cargo spacecraft to ISS)
- Incorporating risk into early trade studies (NASA Constellation)
- Orion (Space Shuttle replacement)
- Safety of maglev trains (Japan Central Railway)
- NextGen (for NASA, just starting)
- Accident/incident analysis (aircraft, petrochemical plants, air traffic control, railway accident, …)

Does it work? Is it practical?

Social and Managerial

- Analysis of the management structure of the space shuttle program (post-Columbia)
- Risk management in the development of NASA's new manned space program (Constellation)
- NASA Mission control ─ re-planning and changing mission control procedures safely
- Food safety
- Safety in pharmaceutical drug development
- Risk analysis of outpatient GI surgery at Beth Israel Deaconess Hospital
- Analysis and prevention of corporate fraud

16.863J / ESD.863J System Safety

Spring 2011