Intro to Systems Theory and STAMP

Why do we need something different?

- Fast pace of technological change
- Reduced ability to learn from experience
- Changing nature of accidents
- New types of hazards
- Increasing complexity and coupling
- Decreasing tolerance for single accidents
- Difficulty in selecting priorities and making tradeoffs
- More complex relationships between humans and automation
- Changing regulatory and public views of safety

STAMP
(System-Theoretic Accident Model and Processes)

- A new, more powerful accident causation model
- Based on systems theory, not reliability theory
- Treats accidents as a dynamic control problem (vs. a failure problem)
- Includes
  - Entire socio-technical system (not just technical part)
  - Component interaction accidents
  - Software and system design errors
  - Human errors

Introduction to Systems Theory

Ways to cope with complexity

1. Analytic Reduction
2. Statistics

[Recommended reading: Peter Checkland, "Systems Thinking, Systems Practice," John Wiley, 1981]

Analytic Reduction

- Divide system into distinct parts for analysis

  Physical aspects → Separate physical components

  Behavior → Events over time

- Examine parts separately

- Assumes such separation possible:

  1. The division into parts will not distort the phenomenon
     - Each component or subsystem operates independently
     - Analysis results not distorted when consider components separately

Analytic Reduction (2)

2. Components act the same when examined singly as when playing their part in the whole
   - Components or events not subject to feedback loops and non-linear interactions

3. Principles governing the assembling of components into the whole are themselves straightforward
   - Interactions among subsystems simple enough that can be considered separate from behavior of subsystems themselves
   - Precise nature of interactions is known
   - Interactions can be examined pairwise

Called **Organized Simplicity**

Statistics

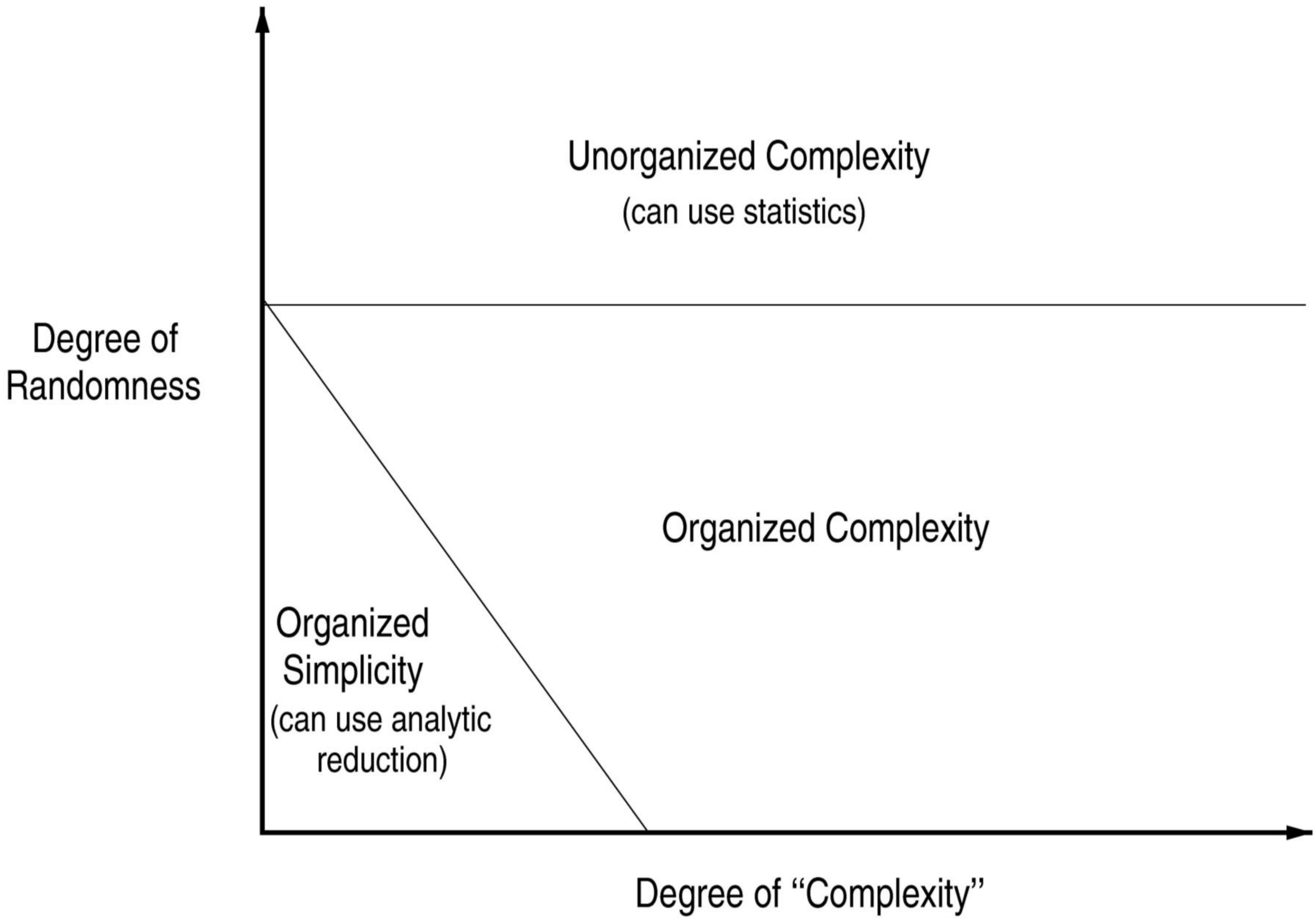
- Treat system as a structureless mass with interchangeable parts
- Use Law of Large Numbers to describe behavior in terms of averages
- Assumes components are sufficiently regular and random in their behavior that they can be studied statistically

Called **Unorganized Complexity**

Complex, Software-Intensive Systems

- Too complex for complete analysis
  - Separation into (interacting) subsystems distorts the results
  - The most important properties are emergent
- Too organized for statistics
  - Too much underlying structure that distorts the statistics

Called **Organized Complexity**


Unorganized Complexity
(can use statistics)
Degree of Randomness
Organized Complexity
Organized Simplicity
(can use analytic reduction)
Degree of "Complexity"

Systems Theory

- Developed for biology (von Bertalanffly) and engineering (Norbert Weiner)
- Basis of system engineering and system safety
  – ICBM systems of the 1950s
  – Developed to handle systems with "organized complexity"

Systems Theory (2)

- Focuses on systems taken as a whole, not on parts taken separately
  - 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

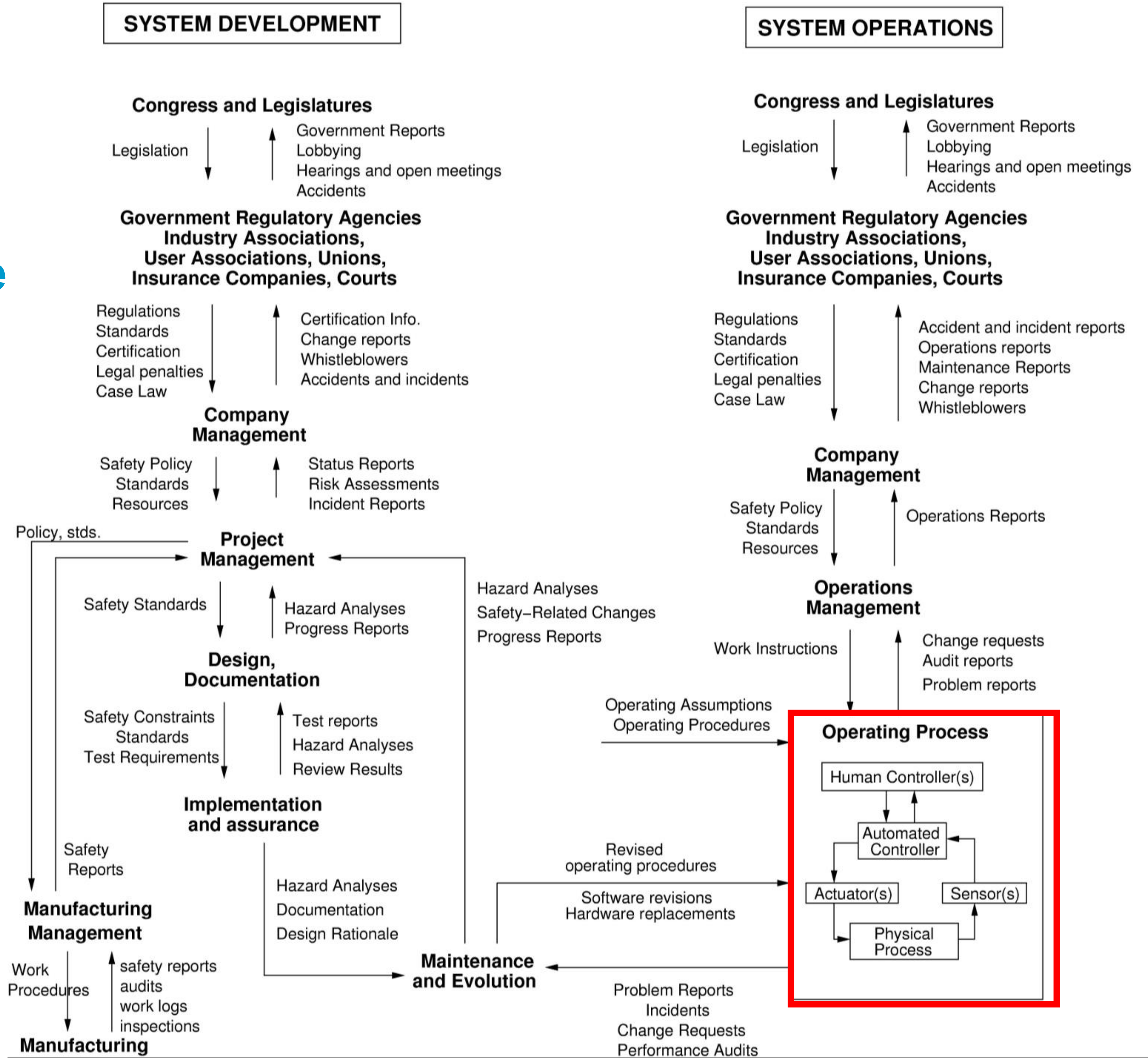
- Two pairs of ideas

1. Hierarchy and emergence
2. Communication and control

Hierarchy and Emergence

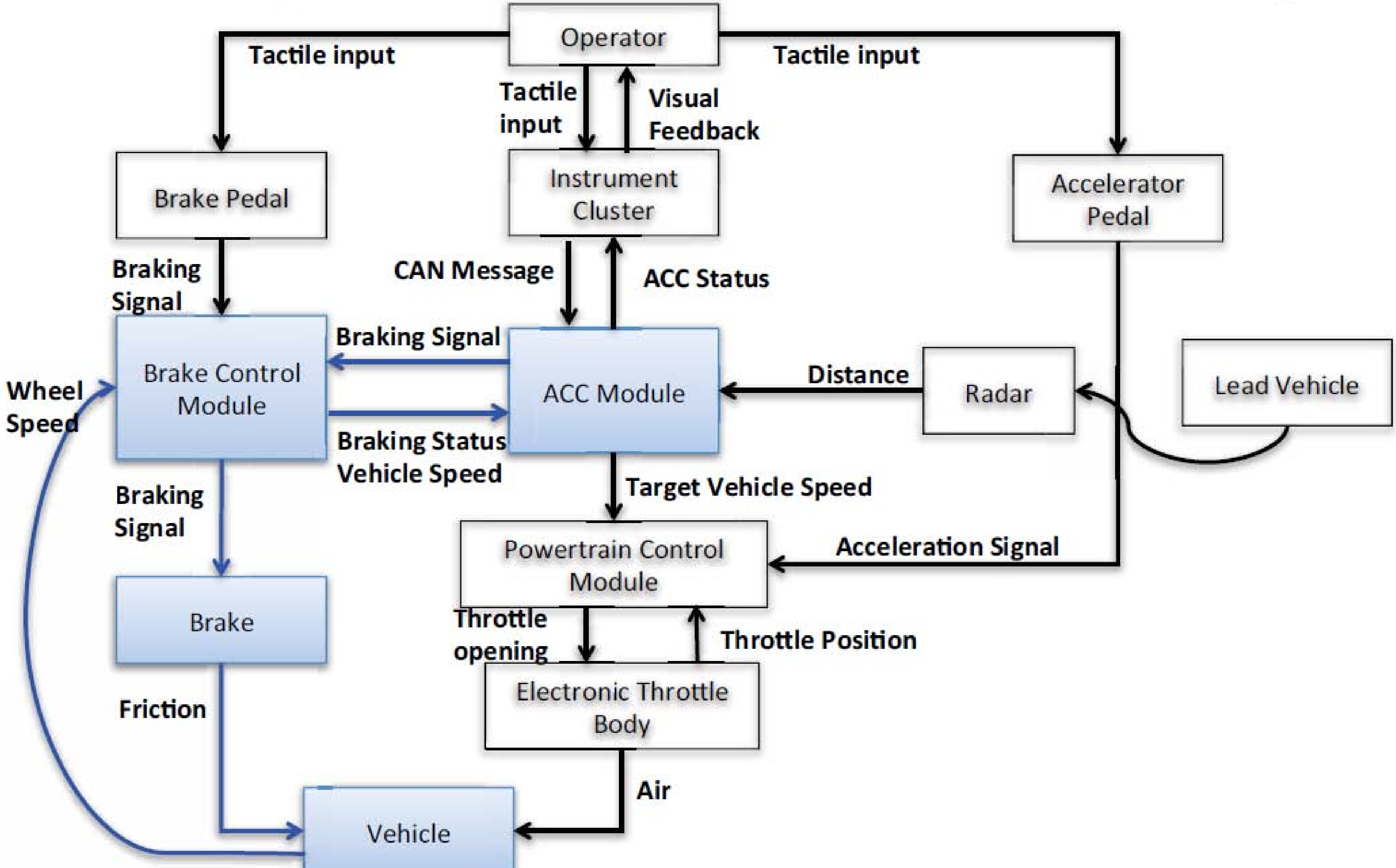
- Complex systems can be modeled as a hierarchy of organizational levels
  - Each level more complex than one below
  - Levels characterized by emergent properties
    - Irreducible
    - Represent constraints on the degree of freedom of components at lower level
- Safety is an emergent system property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

Example Safety Control Structure



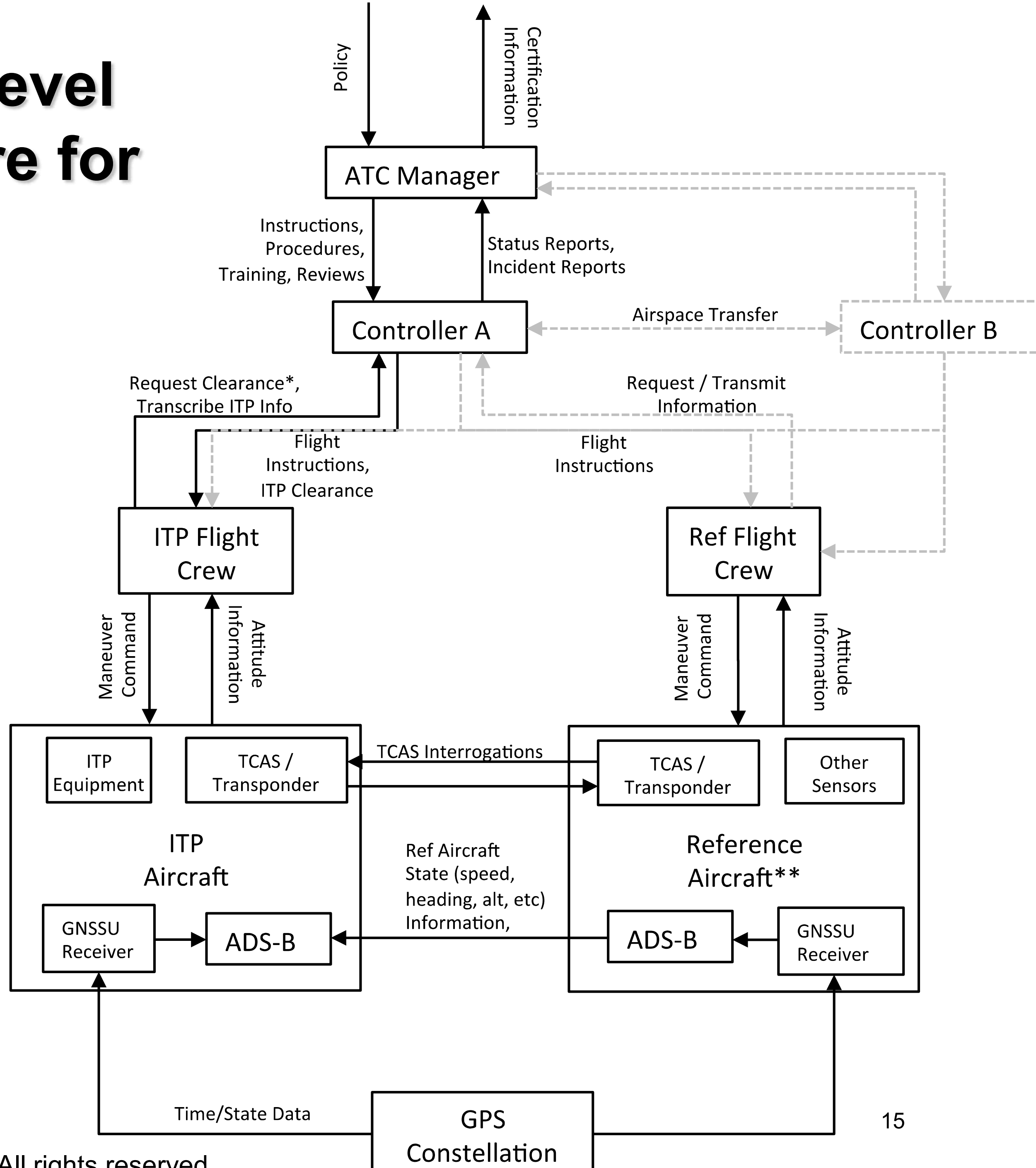
From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Example: ACC – BCM Control Loop



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

Example High-Level Control Structure for ITP



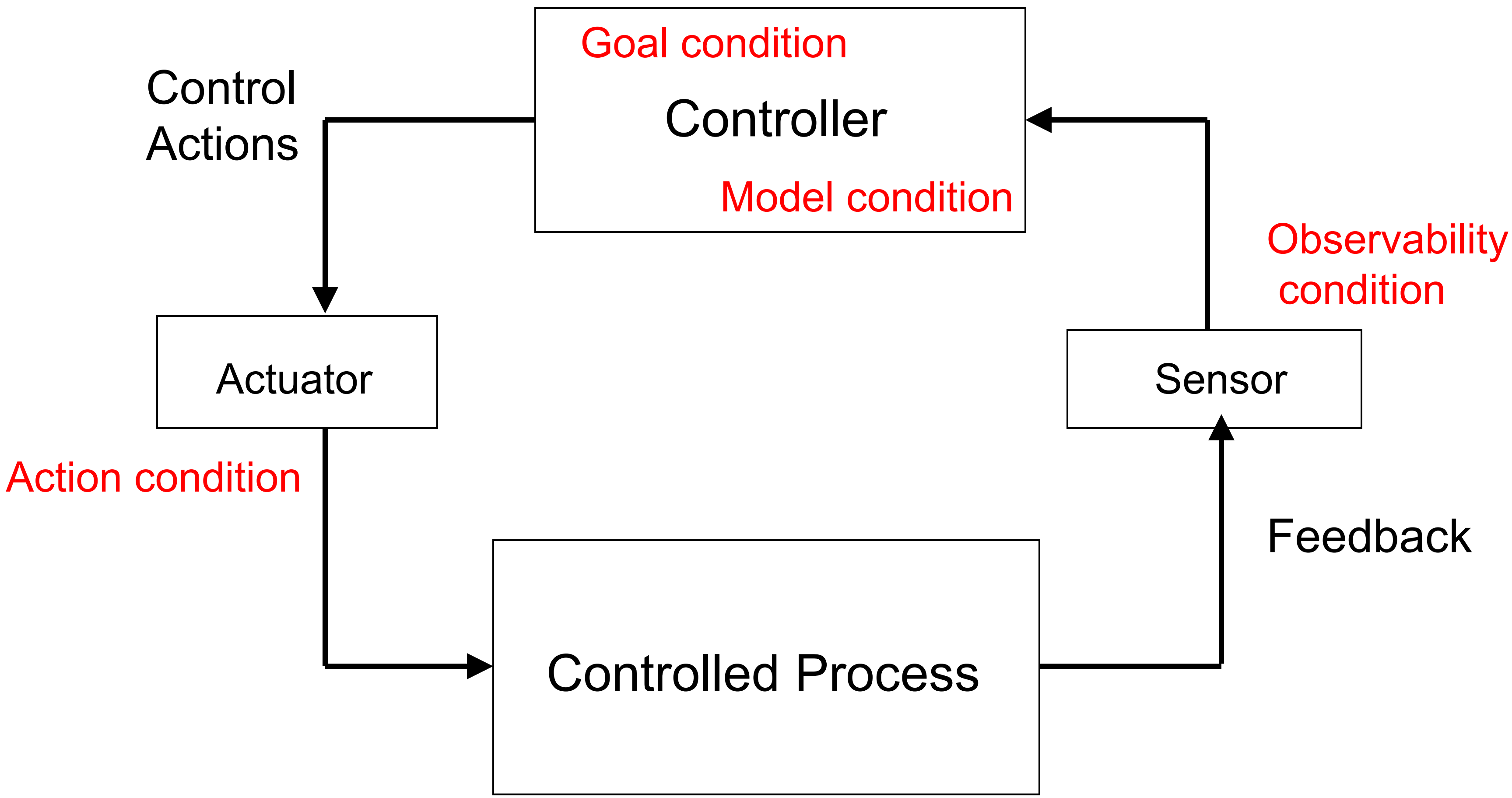
Safety Constraints

- 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 process

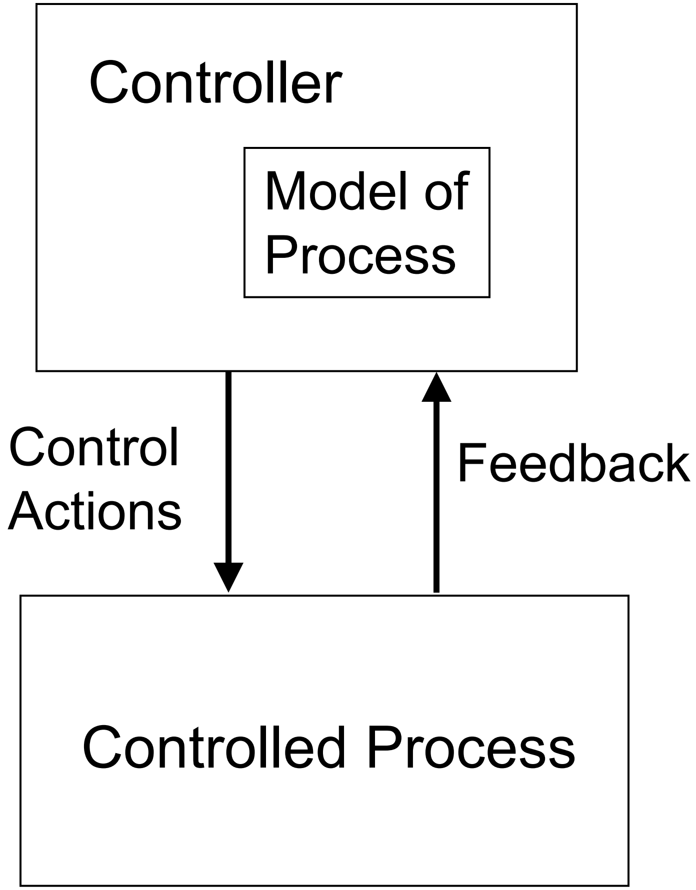
Communication and Control

- Hierarchies characterized by control processes working at the interfaces between levels
- Control in open systems implies need for communication

Control processes operate between levels of control



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

Relationship Between Safety and Process Models

- How do they become inconsistent?
  - Wrong from beginning
  - Missing or incorrect feedback
  - Not updated correctly
  - Time lags not accounted for

  Resulting in

    Uncontrolled disturbances

    Unhandled process states

    Inadvertently commanding system into a hazardous state

    Unhandled or incorrectly handled system component failures

Relationship Between Safety and Process Models (2)

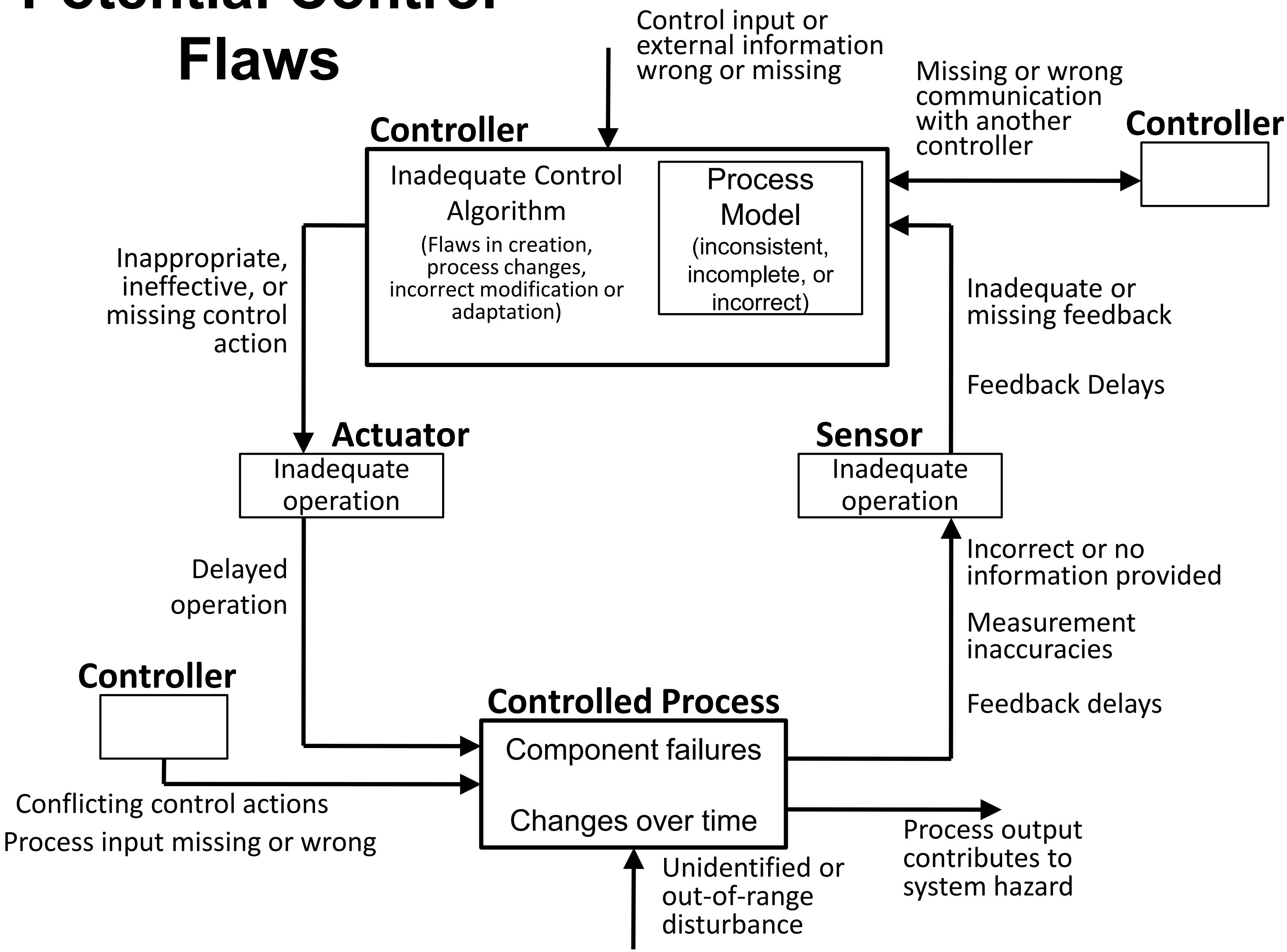
- Accidents occur when models do not match process and
  - Required control commands are not given
  - Incorrect (unsafe) ones are given
  - Correct commands given at wrong time (too early, too late)
  - Control stops too soon or applied too long

Explains software errors, human errors, component interaction accidents …

Relationship Between Safety and Human Mental Models

- Explains most human/computer interaction problems
- Explains many operator errors
- Also explains developer errors. May have incorrect model of
  - Required system or software behavior for safety
  - Development process
  - Physical laws
  - Etc.

Potential Control Flaws



STAMP:
System-Theoretic Accident Model and Processes

STAMP: Safety as a Control Problem

- Safety is an emergent property that arises when system components interact with each other within a larger environment
  - A set of constraints related to behavior of system components (physical, human, social) enforces that property
  - Accidents occur when interactions violate those constraints (a lack of appropriate constraints on the interactions)
- Goal is to control the behavior of the components and systems as a whole to ensure safety constraints are enforced in the operating system.

STAMP (2)

- Treats 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

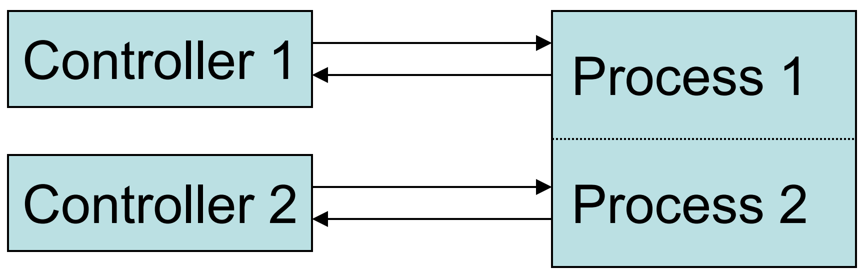
Summary: Accident Causality

- 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)

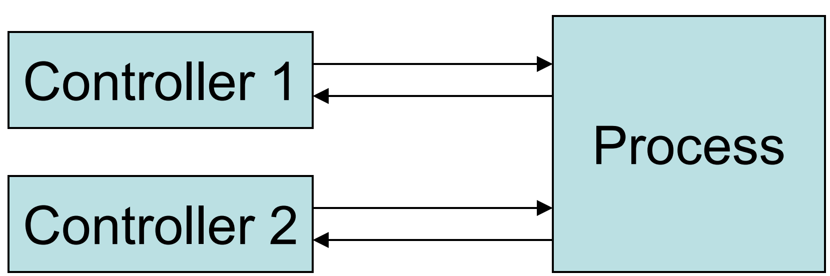
A Third Source of Risk

- Control actions inadequately coordinated among multiple controllers

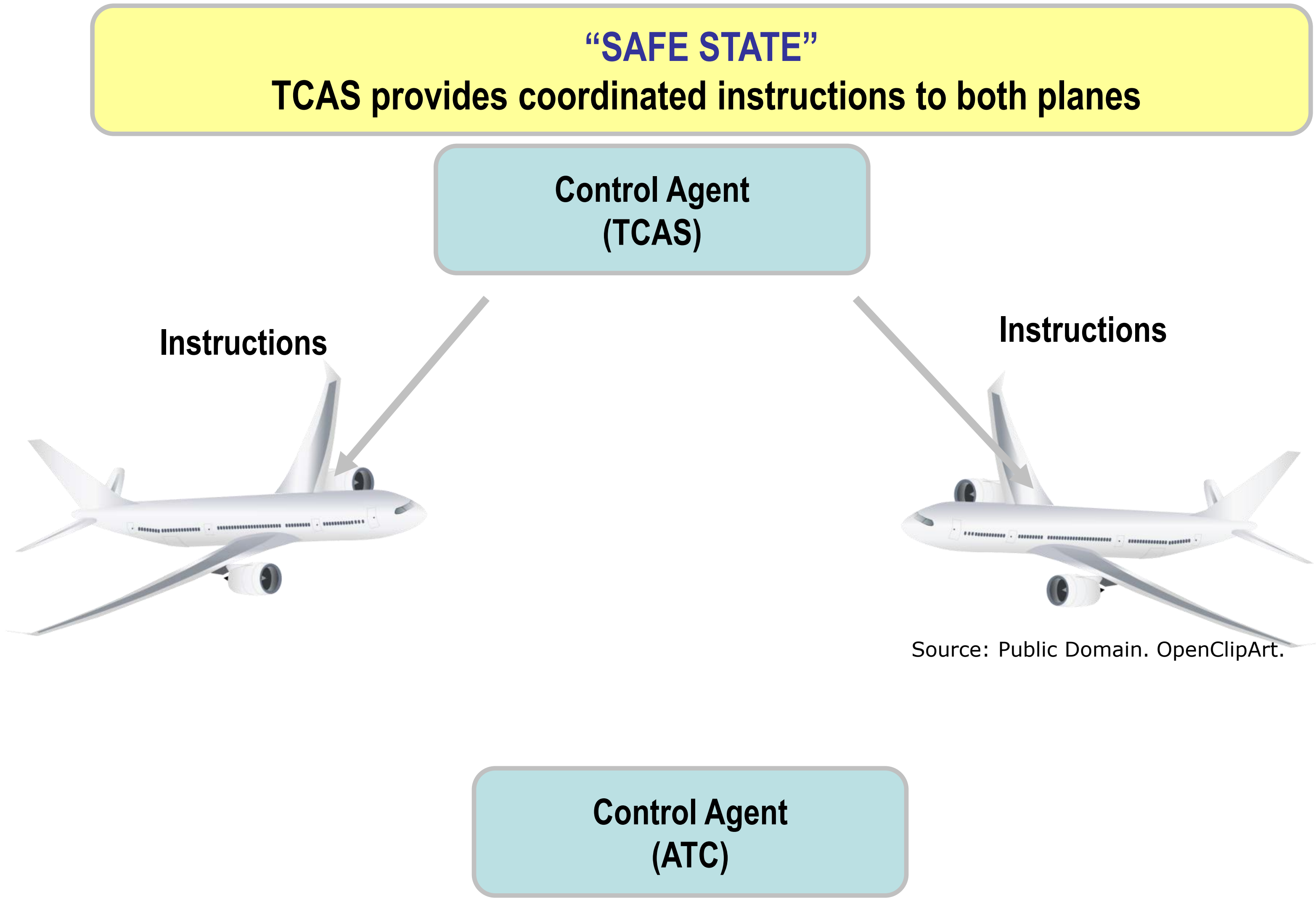
Boundary areas



Overlap areas (side effects of decisions and control actions)

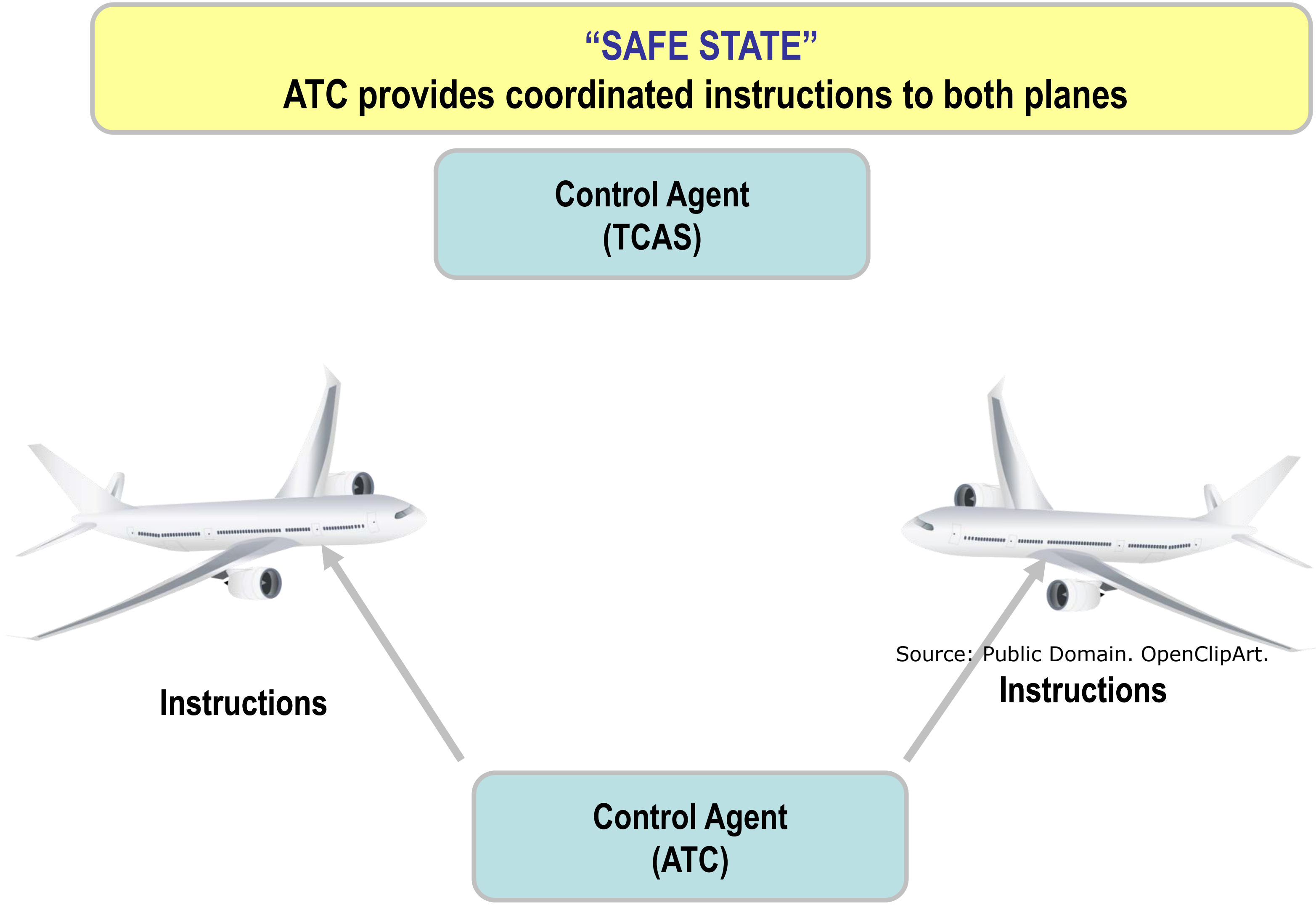


Uncoordinated "Control Agents"



Source: Public Domain. OpenClipArt.

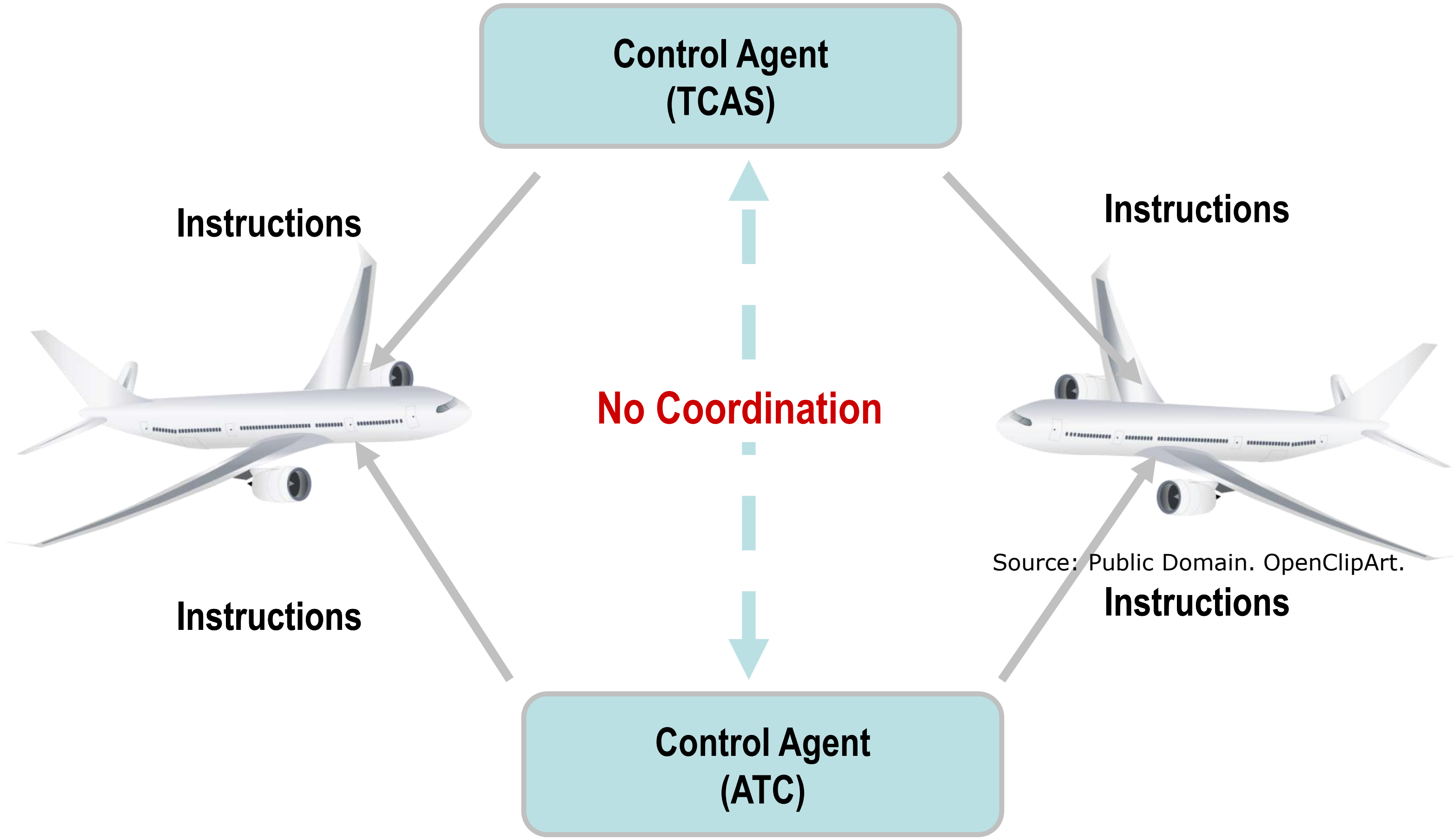
Uncoordinated "Control Agents"



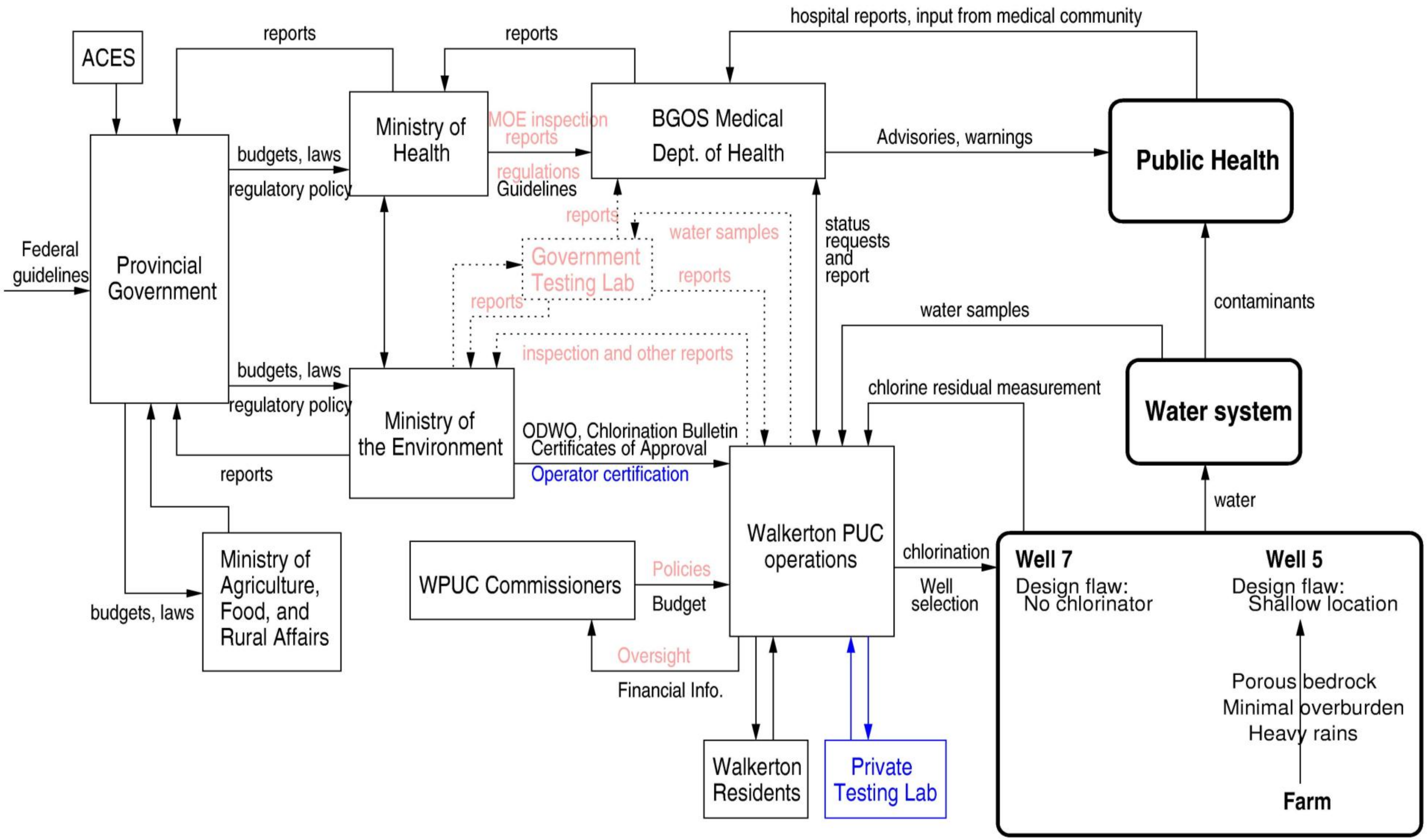
Uncoordinated “Control Agents”

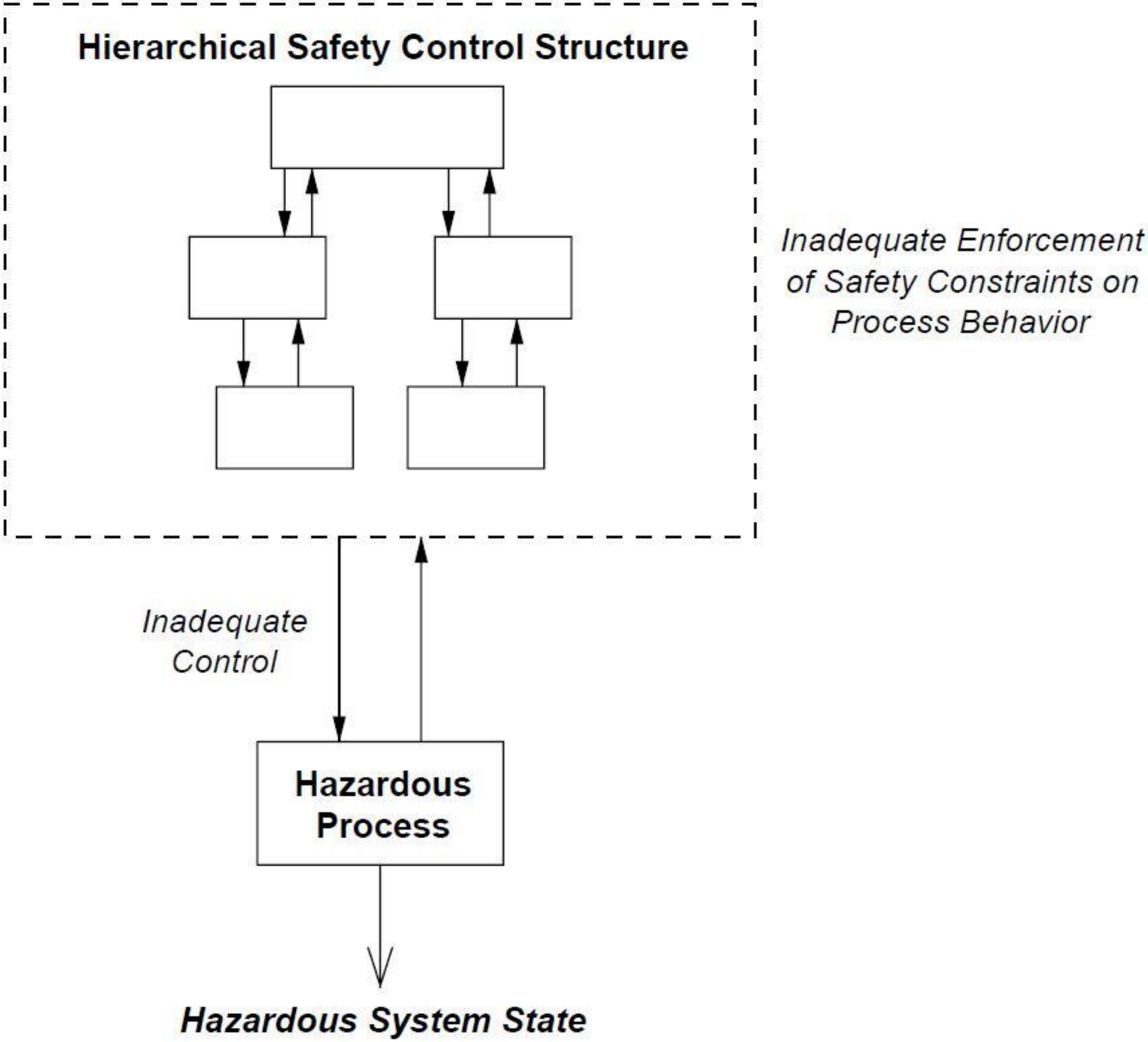
“UNSAFE STATE”

BOTH TCAS and ATC provide uncoordinated & independent instructions



Source: Public Domain. OpenClipArt.


hospital reports, input from medical community
ACES
reports
reports
Ministry of Health
BGOS Medical Dept. of Health
Public Health
MOE inspection reports
regulations
Guidelines
Advisories, warnings
budgets, laws
regulatory policy
Provincial Government
Federal guidelines
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
Walkerton PUC operations
chlorination
Well selection
Well 7
Design flaw:
No chlorinator
Well 5
Design flaw:
Shallow location
Ministry of Agriculture, Food, and Rural Affairs
budgets, laws
WPUC Commissioners
Policies
Budget
Oversight
Financial Info.
Porous bedrock
Minimal overburden
Heavy rains
Farm
Walkerton Residents
Private Testing Lab



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

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”)