Introduction to STAMP (Part 1 and 2)

STAMP - System-Theoretic Accident Model and Processes.

https://www.youtube.com/watch?v=_ptmjAbacMk
http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STAMP-Tutorial.pdf

Part 1

Prof. Nancy G. Leveson

She started in 1980s with torpedos safety (it won't return and hit a launcher). She found that reliability and safety wasn't connected, they often not connected. Spent on it 40 years, worked with many comparity.

STAMP is relatively new. But used in hundreds and hundredds places, petrochemicals, robotics, mining, aviation, nuclear, etc. etc.

5/

What's safety?

- Mishap, accident = loss. Includes injurecies, finince, human lifes, etc. Also inadvertant and intentional.
- Constraints vs goals. Most times safety not in goals but in constraints.
- Safety? Absent of losses.
  This applies to many fields

6/
Cartoon: "we've been stuffing him with worms all day .. and it's still hungry". Means we put efforts into wrong directions. People work hard but it's not effective.

7/
About agenda.

8/ Causality model

It predicts how will system work in future. No wrong or right. Models just to filter information in messy world.

We want simple question to complex problems.

Example of model:

COE. Chain of events model

Most old. It presents linear chain of events: E2 happens if and only if F1 happens. But it was simplification, it doesn't work now in complex world. And there is one root event, it is somewhere in event chain.
Problem: is it usefull? Will it filter out some important factors?

15/

Exercise. Bhopal accient

1984. Thousands dead, injured. Indian state.

- UC (union carbide?) produced pesticides and other (plastics).
- Uded MIC (methyle isocaynade), chemical when in contact with water causes large amount of heat. Hence its effect on lungs, eyes, other.

Union Carbide had safety features. They had specifications. Used "defense in depth": several backup systems that were expected to protect from disaster. Hence probability of diseaster is multiplication of probabilities.
Those were basically several systems that were supporced to cover each other. The MIC chemicals contained in tanks (should be half full), then there were a scrubber that utilized the chemicals, the flare tower to spread extra in atmosphere high above the ground, the water curtain (to pour out if previous ones didn't work), and the refrigirator that kept temp around 0 deg. The alarm was there if temp reached 11 deg.

'Chain' of events. My notes:

- Worker was not taught well so he/she didn't insert those safety disks.
- No body checked no safety disks.
- When gauges showed pressure and temp rise no relevant procedures taken. They ignored them. So the operators not taught well enough. Hence the directors or those in control is responsible for not teaching those operators.
- Operators didn't react quickly to the leak when noticied.
- Superviser ignored the urgent report.
- Backup systems didn't work. The chemical escaped in a fountain high above the ground. So the designers of those backup systems did bad also.
- In emergency. Superviser and ooperator didn't risk to help the situation. So they hired wrong people?
- The gauge for soda circulation.
- The detector for spare tank not working. Technicians' bad.
- And on and on. Police, siren.

> Mine view: Everybody did bad. No root cause? Owners of this is the root cause. They didn't make sure all procedures done.

Root cause selection is arbitrary because we want to feel better like we are in control. Overall seeking root cause is bad.

UC made the worker guilty - wrong.

But many questions raised: why all backup system failed, why they didn't attend before tea break, etc., etc. So this is not a chain of events. We want to look at conditions of events. This is level 2. Level 3 is systemic factors.

Hierarchical models:

- Level 3: systemic factors
- Level 2: factors
- Chain of events.

Addional info:

In theory failure probabilities are low but in practice opposite! Flare town, scrubber, curtain, etc. were not operating as expecting, couldn't handle those conditions, etc. This is not uncommon: gauges turned off, procedures not followed, instructions were not full (insert slip disk), worker very low trained, alarm siren fired too often so turned off, etc. etc.

My view now:

> So all factors are bad, whole plant should have been closed by some state inspection. Agree, no root cause.

And additional questions raised. Why no supervision for the worker, why maintainance so poor, where is operation safety group? etc. etc.

Level 3. Systemic factors.

- Systemic factors link to conditions and even to events.
- Often dropped from accident reports.
- They are 'safety culture'. They are widely applied.

Systemic factors at Bhopal:

- Low demand for MIC. Hence reduction in expenses on safety.
- Training at US stopped for workers.
- Skilled workers live the plant for better places.
- Indian gov. requires only indians workers. Last US superviser visit 3 years ago.
- Safety engineer resigned 1 year ago and replaced with unskilled worker.
- Low moral
- Refrigirator shut down.
- There was the audit 1 year before but ignored!
- There were several warnings and accidents which were ignored again.

This is **common**. Usually a root cause is some operator who was at the beginning. This might deflects attention from powerful parties, often, esp. if a pilot dies (in case of aircraft accident). There are various names for this COE. We need new causality model.

LESSONS:

- We need to look beyond events, i.e. at conditions, systemic factors.

1.05.00

59\ Dealing with complexity

Complexity in modern world rises: introduction of software, internet, complex system. Starndards for safety created 50-75 years old.

Examples:

- Missle launch by a navy aircraft. Causes, factors? Requirements for software were flawed.
- Mars Polar Lander. Landing crash. Requirements? No. Early start of software.
- A320. Reverse the thurst. Software to protect from turning on thrust if not landed. System required flawed.
- Ferry problem. No way to move cars because they were blocked by car owner company (theft assumed). Flaw? Unkonwn unknowns.

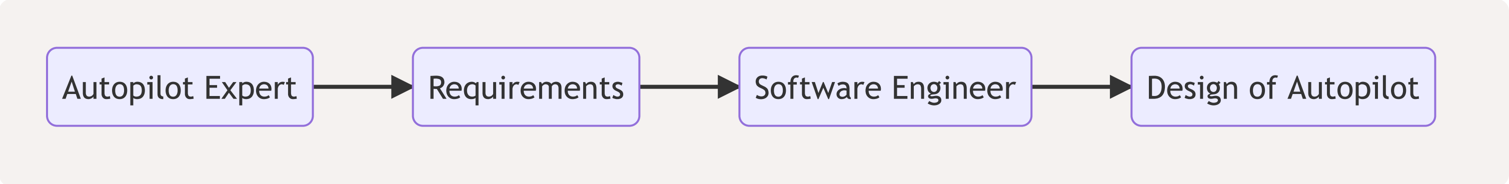
Two types of errors:

- A component(s) failure. Like a landing on Mars.
- Components *interaction* failure, interaction failure between them. Unexpected interaction of components. Like reverse thrust disabled. Software exacerbated this.

Confusing starndard in Safety and Reliability: 1. Unrelable but safe. 2. Unreliable and unsafe. 3 Reliable but unsafe.

Software.

- Software doesn't 'fail'. General Purpose Machine + Software = Special Pupose Machine. Software doesn't fail because it is a pure design.
- Allows unlimited system complexity:
  - Can no longer: plan, anticipate etc. Test thouroughly.
  - **Context** dertermines if safe. COmponents don't fail. But integraion them in other context fails, Like butter knife. Not possible to look at software alone and determine 'safety'. If alone you CAN'T determine if it is safe only in context.
- Role of software in accidents is almost always because of requirements.
  - Incomple or wrong assumptions.
  - New states.
  - Level of rigor nothing to do with safety.



76\ **LESSONS**:

- Need to consider design errors, not just component(s) failures.

- Software - doesn't fail but can lead to unsafe behavior, impossible to test fully.

77\ Software changes the role of humans in systems

78\ Software changes roles.

- Traditional approach seeks a cause(s) in an operator error(s). Hence more training or making their work rigit, etc.
- But accidents show that a cause is complexity. Systems were reliable.
  - Accidents: 1) B757 in Cali; 2) Columbia, Tu-204, Moscow, 2012
- We can't isolate humans and systems in critical situations. But no training in this integration!

85\ Operator error is a symptom, not a cause!

- Because all behavior is affected by the context, role of operators changes.
- Wrong to blame operators when systems are designed so that they lead to errors.

87\ **LESSON**:

- Need to integrate human behavior, software and hardware engineerings together.

87\ Part 2: STAMP

How do we solve those lessons?

We need models that handle 'unknown unknowns', human factor, policy, interaction between components, etc. AND interactions between these.

New tools. Paradigm change. It is not that previous all bad, now is good. Not. It is integrating previous ones and extends them, includes old. STAMP doesn't invalidate CoE but it says that it is not enough.

Wrong approaches:

- Pretend no problems.
- New tech and levels into old methodologies.

94\ STAMP is

- New causality model
- Allows to build more powerful tool.

How to cope with complexity? 1) Analytic decomposition, statistics, systems theory.

96\ Anal. decomposition.

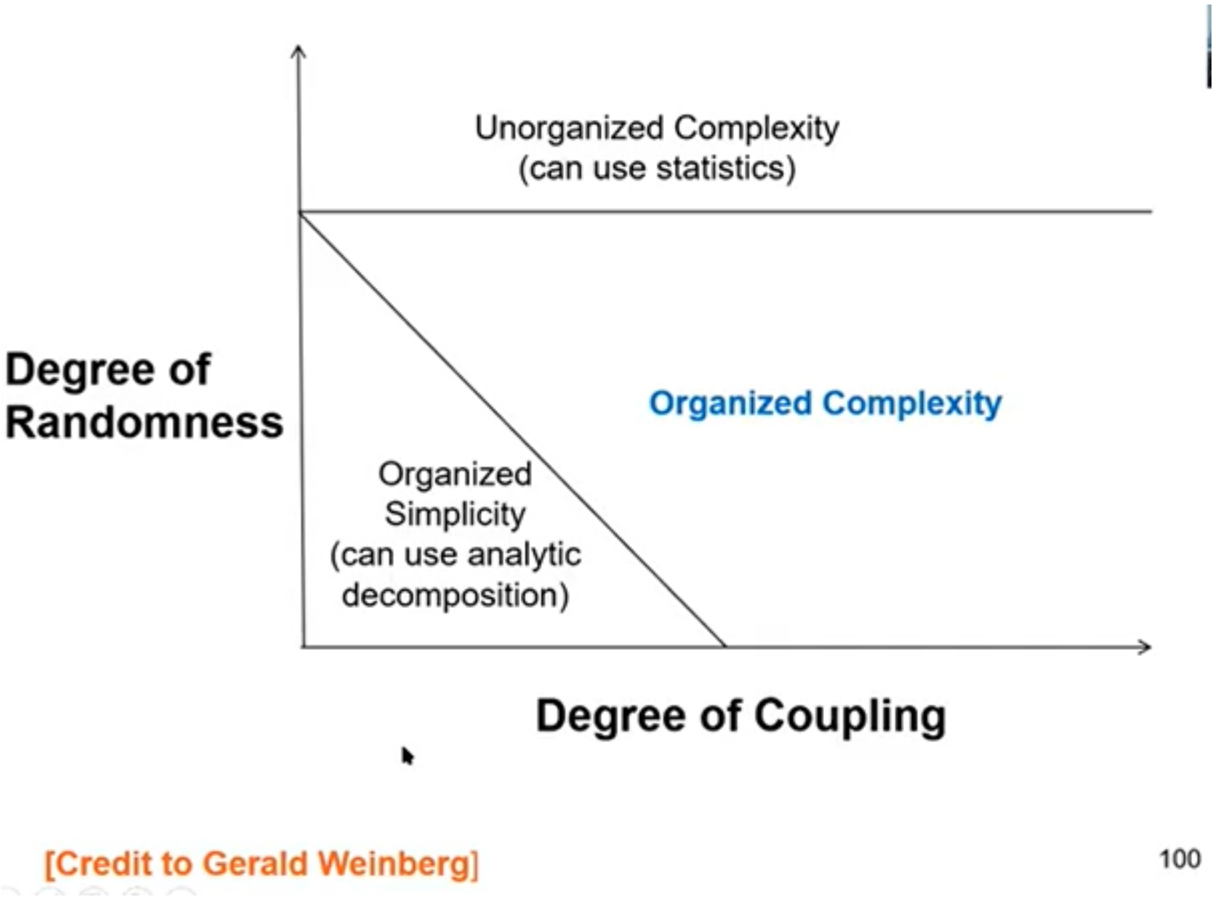
Divide and conquer

1. Divide.
2. Examine pieces separately and combine.
   - Remember it is wrong to assume that components behave separately, etc. So people tried to

decompose accidents and what went wrong there. But that also not good, still bottom up as all systems tightly coupled, software, connected, etc.

  - Need theoretical basis.

At figure below we see that we can't use analytic decomposition.



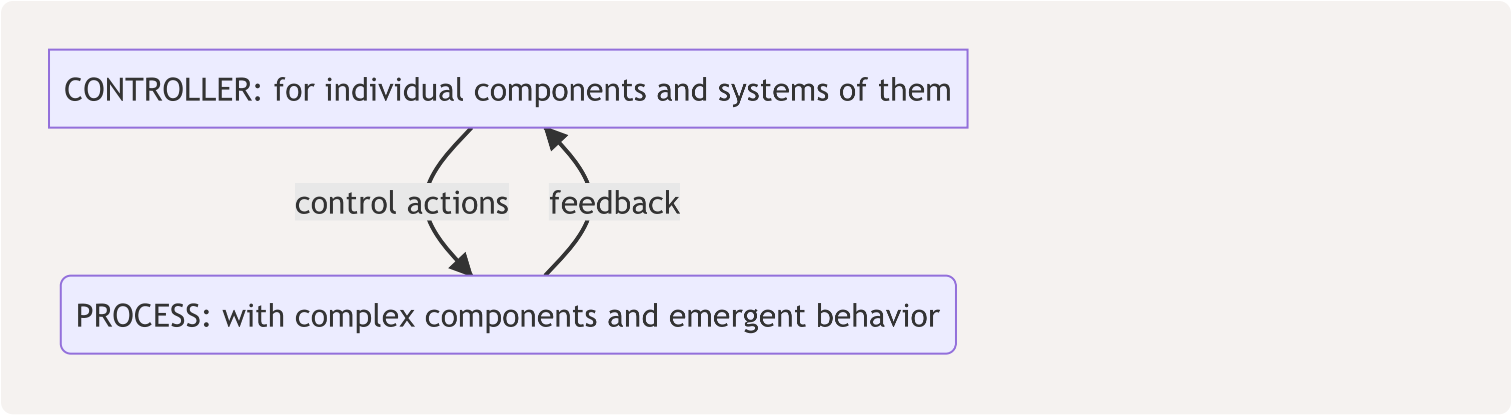
[Credit to Gerald Weinberg]

Systems Theory is a way to deal with complexity. First used in 1950/60s.

Systems theory:

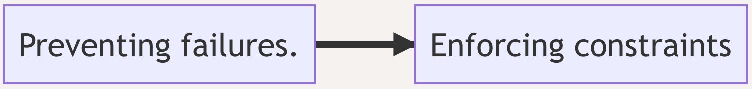
- Focus on a system as whole
- Emergent properties from a whole system. The whole is greater than the sum of its parts. Arise from comp interaction.
  - Safety and security are emergent properties.
  - Example: only taking a valve we can't tell if whole system is safe.

Solution is to have controller for those emergent properties.


CONTROLLER: for individual components and systems of them
control actions
feedback
PROCESS: with complex components and emergent behavior

Safety contraints. These are given requirements, constraints we should address like preventing hazards from leakage, virus contamination, etc. Then we break those into componenets, then to design.

Paradigm shift:

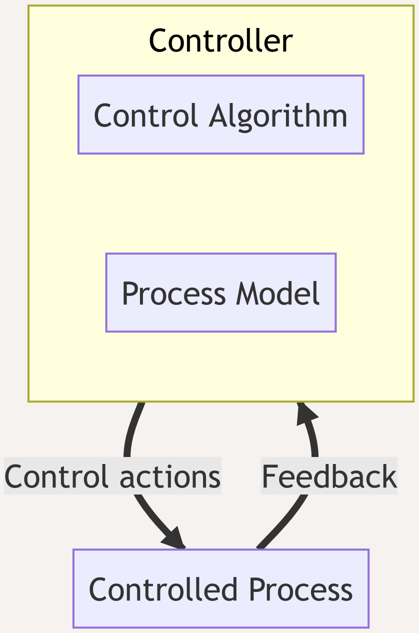


From a reliability problem (a component(s) failure) to a control problem (interaction, emergent behavior).

What's 'Control'?

- Through design to 'control' components interactions.
- Through processes of manufacturing, maintenance, other.
- Through social controls: governmental, culture, insurance, individual motivation, etc.

Safety as control problem:



Examples:

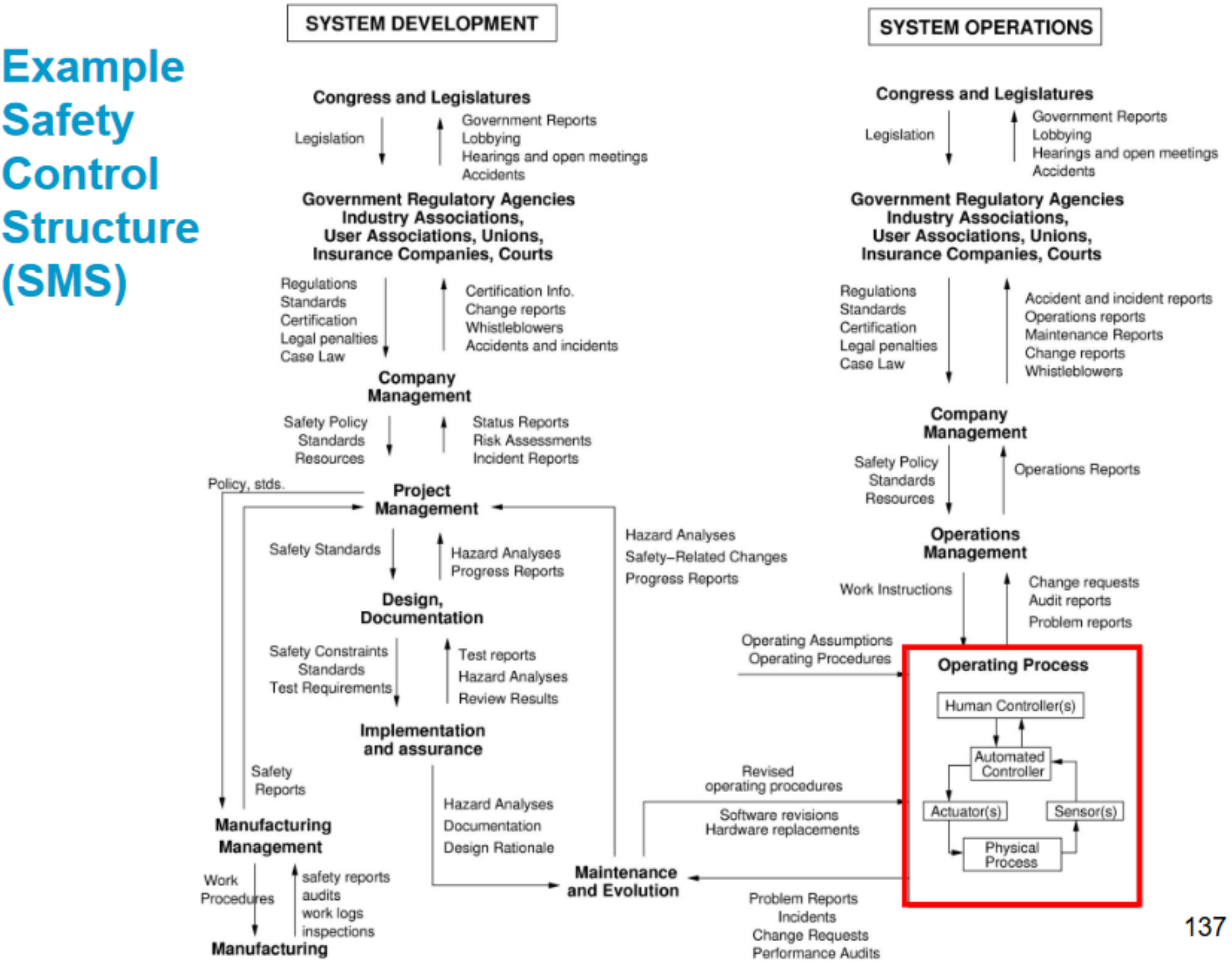
1. Mars Polar Lander. Hazard: too much force on landing. So the control problem is that software (controller) receives signal from a leg (complex process) and treats it as if the space craft landed. And wrong decision: turn off descend engines.
2. Aircraft and reverse thrusters in Warsaw. The control problem is that software controller ignores pilot command to turn on reverse thrusters.
3. Aircraft and reverse thrusters in Moscow. The same as in 2 but additionally some.
4. Missile Release Mishap. Hazard: Friendly Fire. Control problem is Software optimizes missle launch success by launching non-dummy missile.

So analyze hazards and accident with STAMP. We can treat components, systems in this fashion: controller and processes. So that we treat it as control problem.

135\ We can use STAMP for Safety and Security.

Every complex system can be viewed at diff levels as a control problem: software vs hardward, software vs human, human vs human. afety and security are connected to losses. So the same paradigm shift for security.

- Example - Stuxnet (computer worm), it made centrifuges to run fast while got on plant computers (Windows); so how to control? same thing - add a controller: mechanical limiters; so preventing hazards not keeping those worms out.
- Example. Safety Contorl Structure. From System Development to System Operations. Large diagram, see below. We can treat it *all* as control problem. The red rectangle is an example of treating this Operating Process as control problem.



Example Safety Control Structure (SMS)

SYSTEM DEVELOPMENT

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety–Related Changes
Progress Reports

Design, Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation and assurance

Safety Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing Management

Work Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance and Evolution

SYSTEM OPERATIONS

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company Management

Safety Policy
Standards
Resources

Operations Reports

Operations Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

Physical Process

Revised operating procedures

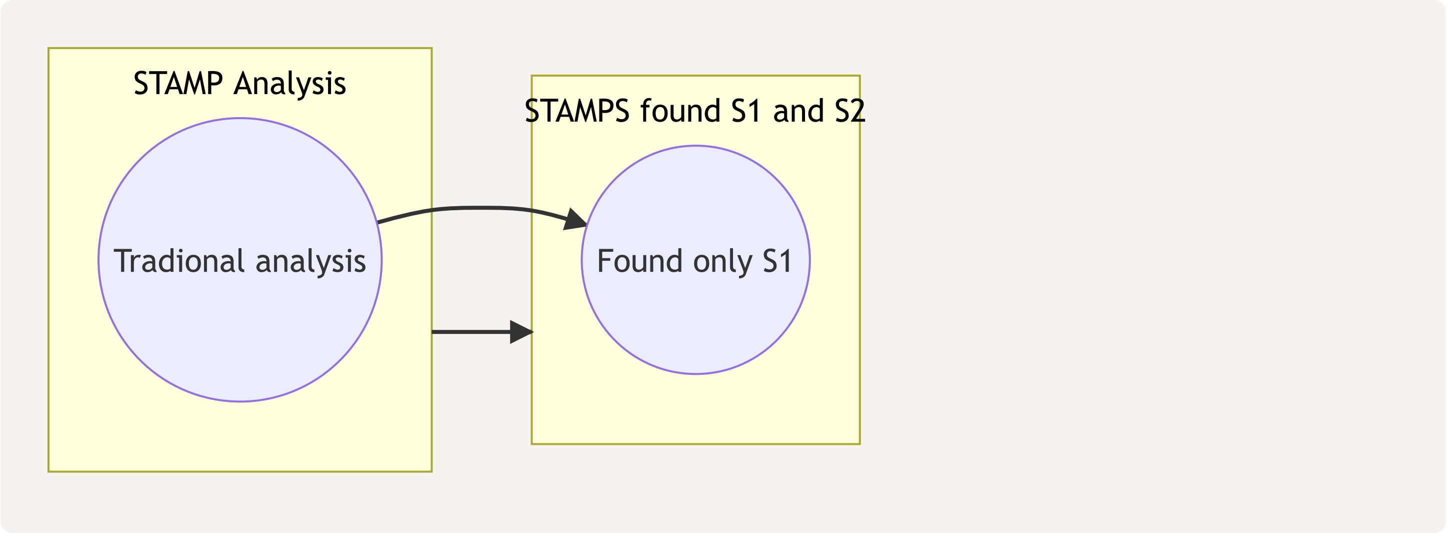
Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

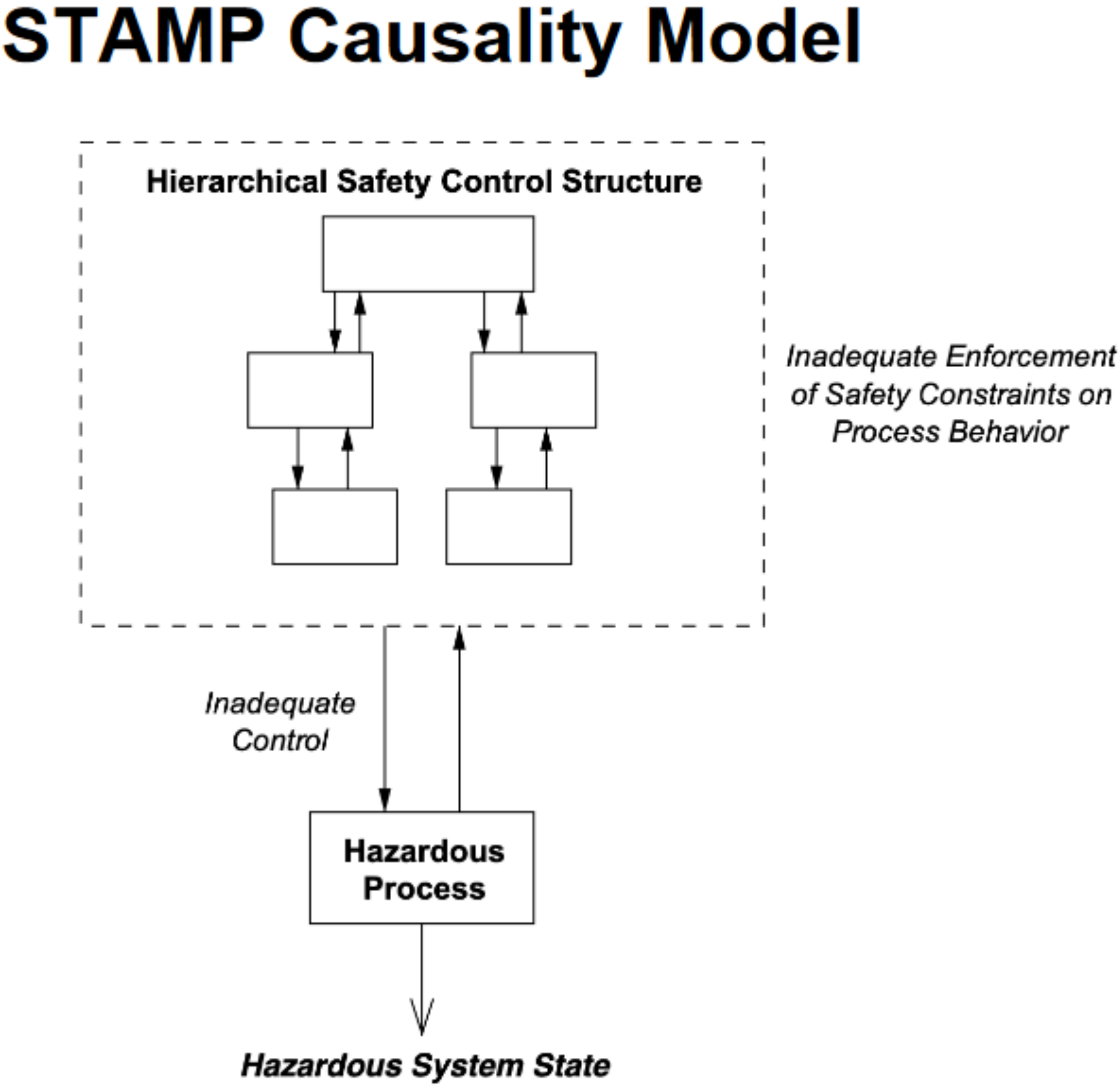
137

139\ STAMP - System-Theoretic Accident Model and Proceses)

- New, causality model
- On systems theory not reliability theory
- As cotrol problem
- To very complex systems
- Includes all previous methods: human errors, software erorrs, etc.



- STAMP causality model:


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

- STAMP include complex interactios. Example is 'Herald of Free Enterprise' accident.

- Systems thinking: not thinking in lines but in circles or more complex.

- Example: Columnbia Shuttle Loss. There are complex connections (one increases /decreases other thing increases / decreases, etc.)

- Safety as Control Problem:
  Goal: design an effective control structure that eliminates or reduces adverse events (losses)

147\ What tools are available?

- Processes: system engineering, risk management, etc
- Tools: Accident Analysis (CAST), Hazard Analysis (STPA), etc.

Does STAMP work? Evidence? Evaluations and estimates of ROI (return of investment):

- Hundreds example. All show STPA is better, requires fewer resources.
- 15-20% for ROI when using STPA.
- She mentions 900 mln USD project.
- Example. Ballistic Missile Defense System (MDA). 2 people in 5 month found many flaws and they fixed those early. Hence saved mlns of usd.
- Example. Blackhawk hylicompter. Found additional hazards.
- Example. Navy Escort Vessels. Found scenarious not found by prev analysis. Nave ignored their analysys. Later accident stamp predicted.
- Example Nuclear power plant. 2 grad sudents spent 2 weeks. Found new 16 accidents that prev analysts didn't know.
- (Other) Found many more causes. Medical. Automotive electric poower steering system. hospital. Organizational. Supply chain. other.

Approach, sumary:

- Emphasizes building in safety rather than measuring it and adding later.
- System as a whole (not components)
- Larger view of causes not just failures.
- Goal is to design and operate NOT to predict the likelihood of a loss.

System Eng Benefits:

- Finds underlying assumptions.
- Finds incomplete info
- Handling intended and unintended func
- Includes all software, operators,etc
- For very complexity systems
- Can do early
- Traceability from requirements to artifacts.
- Models show high level view.
- Augments sys engineering process.

Refs:

- http://psas.scripts.mit.edu
- http://mitpress.mit.edu/books/engineering-safer-world

My questions

- Part 1.
    - Give definition of safety. (Mishap, accident, loss.)
    - 'Chain of events' (CoE) causality model. What's it?
    - Lessons learnt from Bhopal accident? Levels of causality?
    - Dealing with complexity in modern world:
        - Two types of accidents? (When components.)
        - Reliability vs Safety. Name three types of scenarios.
        - Does software fail? Why?
        - For complex systems with software, where is the most likely a flaw? Why?
    - Lessons learnt from model complex system accidents?
- Part 2. STAMP
    - What's the paradigm change? And what's wrong approaches?
    - 96\ Divide and conquer approach
    - Systems theory.
        - What's it? When the theory developed?
        - What it states about a complex system? How to handle it?
    - What's paradigm shift in terms of systems theory? Safety as control problem.
        - Give examples of where there was control problems.
    - Can we use STAMP for security?
    - STAMP abbreviation?
    - Stamp causality model diagram
    - Goal of STAMP?
    - Evidance that STAMP works?

====================================

END