A New Accident Model for Engineering Safer Systems

16.842 – 13 November, 2009

Student 10, T. Ishimatsu, and Student 11

Introduction

- Traditional accident models view accidents as resulting from a chain or sequence of events.
- But today, the types of systems and the context in which they are built have been changing:
  - Fast pace of technological change
  - Changing nature of accidents
  - New types of hazards
  - Decreasing tolerance for single accidents
  - Increasing complexity and coupling
  - More complex relationships between humans and automation
  - Changing regulatory and public views of safety
- These changes are facing the limits of current accident models and new approaches are needed.

Event Chain Model

- Includes FTA, FMECA, Event Trees, etc.
- Explains accidents in terms of multiple events sequenced as a chain over time.
  - Ignores non-linear causality relationships including feedback.
- Is subjective in the choice of events to include.
  - There is no well-defined "start" of the causal chain involved in accidents.
- May provide too superficial an explanation of why the accident occurred.

→ Shift from "cause" to "reasons"

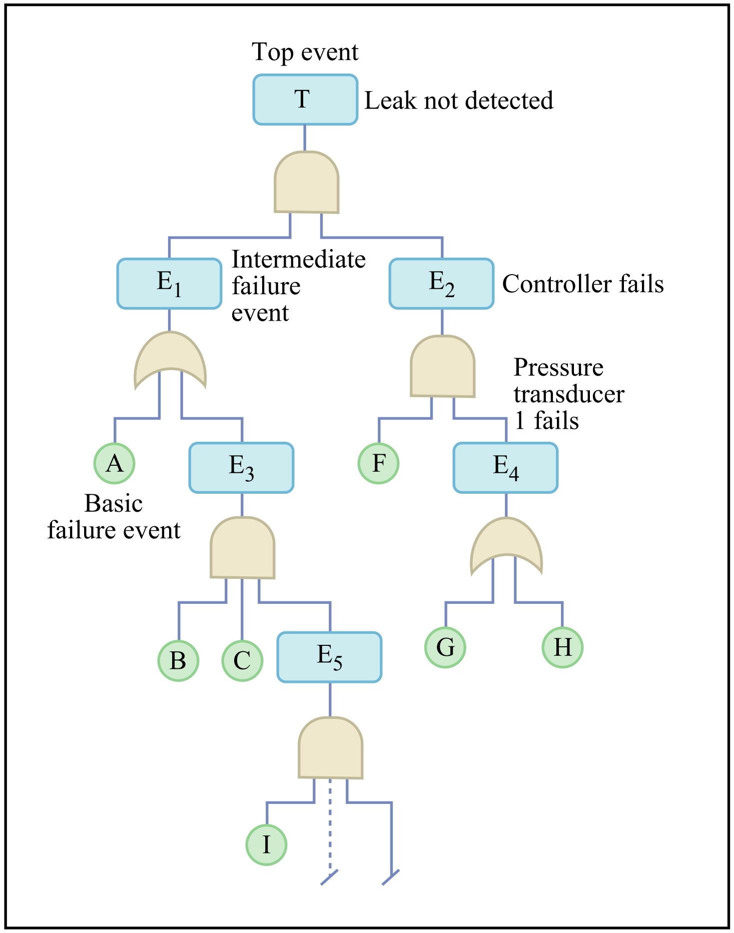


Image by MIT OpenCourseWare.

Example of a fault tree

AA965 Cali Accident

- Crew Procedure Error
- Pilot Error
- Approach Chart and FMS Inconsistencies
- FMS Design Deficiency
- American Airlines Training Deficiency
- Manufacturer’s Deficiencies
- International Standards Deficiency

Limitations of Event Chain Models

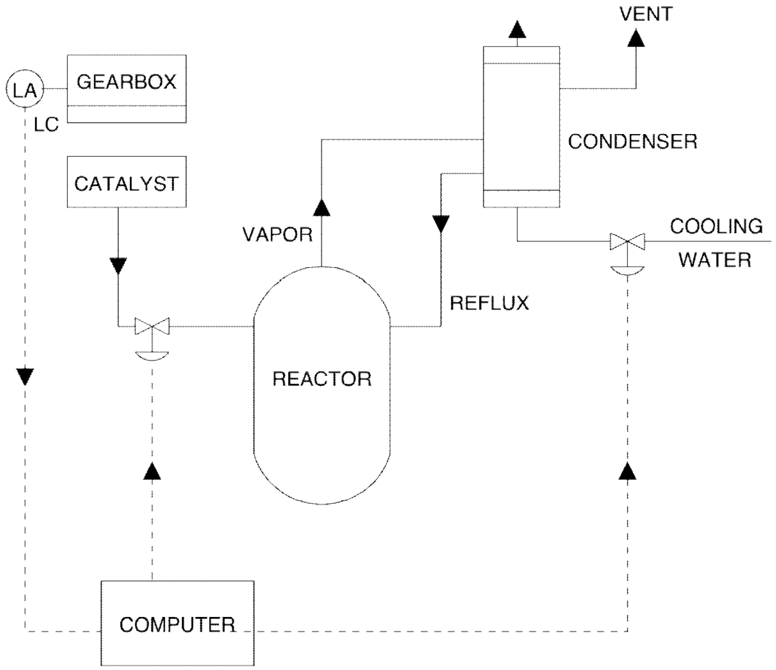
- Event-based models do NOT account for:
  - Social and organizational factors
    - Structural deficiencies in the organization
    - Management deficiencies
    - Flaws in the safety culture of the company or industry
  - System accidents and software errors
    - Reducing the ability to detect all potential undesired interactions
    - Increasing the incidence of system accidents
  - Human error
    - May appear safe and rational locally.
    - May be unsafe in the larger socio-technical system as a whole.
  - Adaptation over time
    - Under pressure toward cost-effectiveness and increased productivity in an aggressive, competitive environment
  - Component interaction accidents
    - Violate the safety constraints

STAMP: Systems-Theoretic Accident Model and Processes

- Safety is viewed as a control problem.
  - The system is defined to encompass product and social structure.
  - Controller enforces constraints to ensure safety.
    - Development (process and resulting design)
    - Operation
  - Accident ==> ineffective control structure
    - Which safety constraints were violated?
    - Why were they violated?
  - Continuous system-level task instead of simply preventing component failure.
- Three basic concepts
  - constraints,
  - control loops and process models, and
  - levels of control.
- Classification of accident factors

Constraints

- Control laws related to the behavior of system components.
- Most basic concept in STAMP (as opposed to event for most accident analysis).
- Accidents are result of lack of appropriate constraints.
- Digital control systems relax physical constraints and increase flexibility, but constraints are still needed for safe operation.



Courtesy of Nancy Leveson. Used with permission.

Control Loops and Process Models

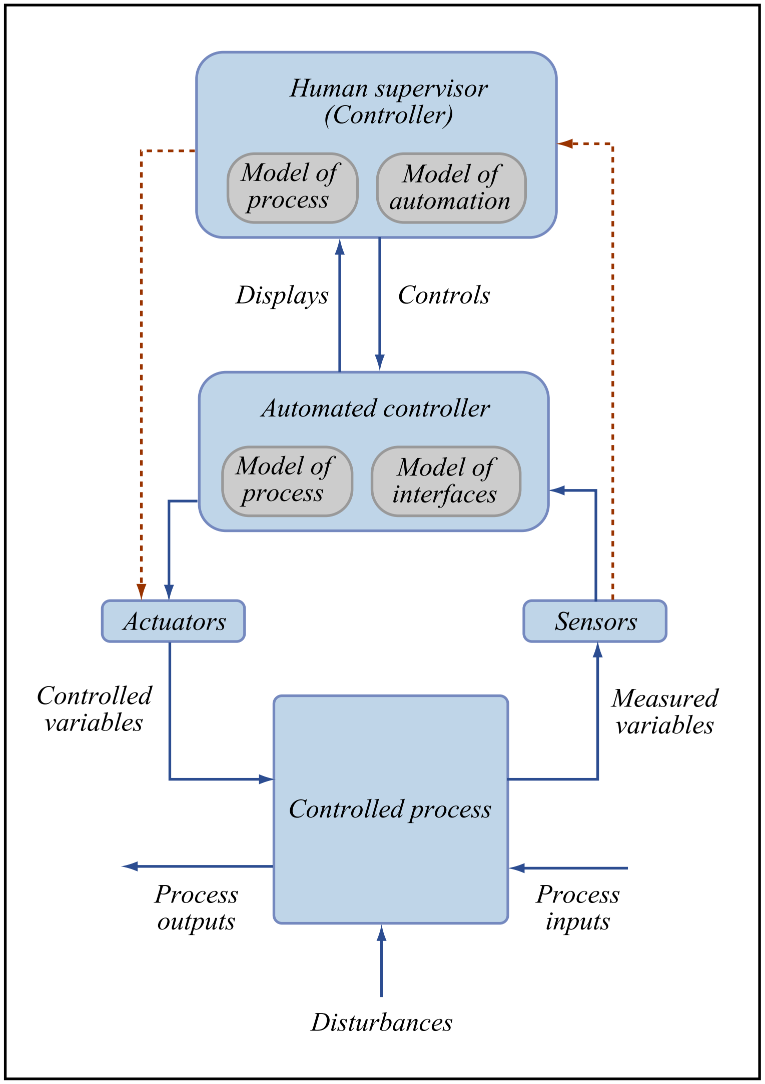
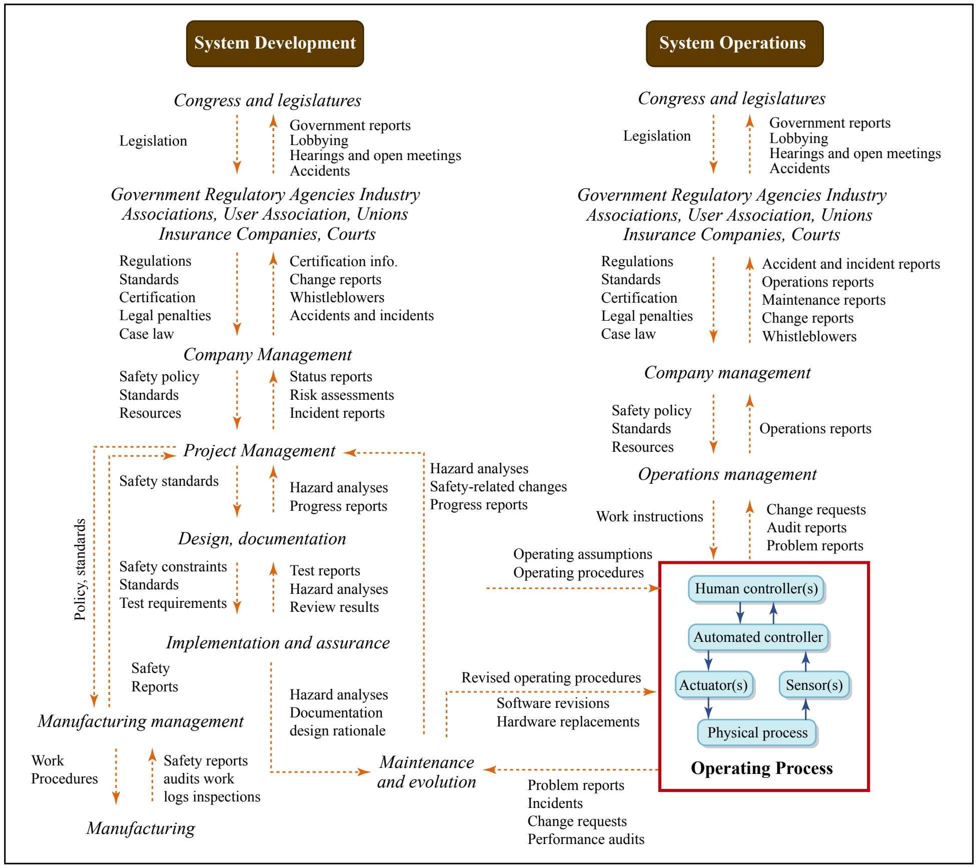


Image by MIT OpenCourseWare.

- System is kept in dynamic equilibrium (safe state) by feedback loops of information and control.
- Controller must have:
  - Goal(s)
  - Ability to change system state
  - A model of the system
  - Ability to observe system state
- May have multiple controllers, human and/or automated

Levels of Control

- Systems are hierarchical
  - Constraints flow down (reference channel)
  - Feedback flows up (measurement channel)
- Parallel chains can have interactions.
- Time lags affect flow, must be included in safety analysis.



System Development

Congress and legislatures

Legislation

Government reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies Industry Associations, User Association, 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

Project Management

Policy, standards

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 Association, 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

Human controller(s)

Automated controller

Actuator(s)

Sensor(s)

Physical process

Operating Process

Revised operating procedures

Software revisions
Hardware replacements

Problem reports
Incidents
Change requests
Performance audits

Image by MIT OpenCourseWare.

Classification of Accident Factors

Inadequate Enforcement

Inadequate Control Algorithms

asynchronous evolution

Inconsistent Process Models

Airplane on ground raises gear

Inadequate Coordination

Who is in control?

Especially important in boundary and overlap areas.

Inadequate Execution

Failure in *reference* channel

- actuator fault/failure
- communication failure
  - control commands
  - design constraints

Inadequate/missing Feedback

Failure in *measurement* channel

- not included in design in first place
- communication failure
- sensor fault/failure
- excessive delay

An Example of System Level Failure

- F-22 Prototype crashed April 25th 1992 while performing a go-around maneuver.
- Initial reports cited a root cause of...?
  - Pilot error! (of course)
- However the accident report concluded that "there were no aircraft malfunctions and that it performed as designed."
- What went wrong?

Factors Contributing to the YF-22 Incident: On the Aircraft

Component Interaction:

Leveson: "*Accidents result from interactions among components that violate the safety constraints—in other words, from a lack of appropriate control actions to enforce the constraints on the interactions.*"

"The gear transient with full stick deflection is the key item that stimulated the PIO [pilot induced oscillation]… …This is because the gear handle commands a large instantaneous change in the flight control laws, and because of the anti-transient logic for the control surfaces."[1]

Pilot's Mental Model:

Leveson: *"Human controllers interacting with automated controllers, in addition to having a model of the controlled process, must also have a model of the automated controllers' behavior in order to monitor or supervise it. Accidents may result from inaccuracies in this mental model."*

"The first time I knew something really was wrong, I felt a very strong nose-over pitch. I was looking at a lot of runway and the airplane had never done anything like that before... ...I thought something had broken and I didn't see any warning lights."[1]

[1] REPORT PINPOINTS FACTORS LEADING TO YF-22 CRASH, Aviation Week & Space Technology, November 9,1992

Factors Contributing to the YF-22 Incident: Organizational

Leveson: *"The role of the system engineer or system safety engineer is to identify the design constraints necessary to maintain safety and to ensure that the system design, including the social and organizational aspects of the system and not just the physical ones, enforces them."*

Failure to Constrain the System

"PIO measures are in Mil-Std-1797 handling specifications, but...''it's typical to not check for PIO during design,'' particularly if the aircraft is designed to have good Level 1 handling qualities."[1]

Failure to Enforce Constraints

"...flight control engineers said vectoring should be off at low altitudes for ''flight control reasons,'' but they did not issue an operating limit ''because they had no known or suspected reason to do so.'' Not all individuals in the YF-22A program were aware of the card instruction, and whether it was being obeyed."[1]

[1] REPORT PINPOINTS FACTORS LEADING TO YF-22 CRASH, Aviation Week & Space Technology, November 9,1992

Questions

- Does anyone have experience designing safety into a system?
  - What problems did you experience with traditional system safety methodologies?
  - Has anyone used STAMP?
- How does safety fit into our model of the system engineering process?
- Would it be useful to model the system as a network rather than a hierarchical chain?
- Does the move towards safer systems require a reduction in human control over the system?