

A System Theory Approach to Hazard Analysis

Mirna Daouk

daouk@mit.edu

Motivation

- Hazard Analysis Techniques currently used are mostly **event-based**
- The event-oriented, open-loop view leads to an event-oriented, reactionary approach to problem solving
 - Real systems include feedback, non-linearities, time delays, adaptation, and other elements of dynamics complexity
- Most accidents arise from **interactions/ interfaces** or lack of **constraints** (absent or violated)
- A **system-oriented** approach thus seems necessary

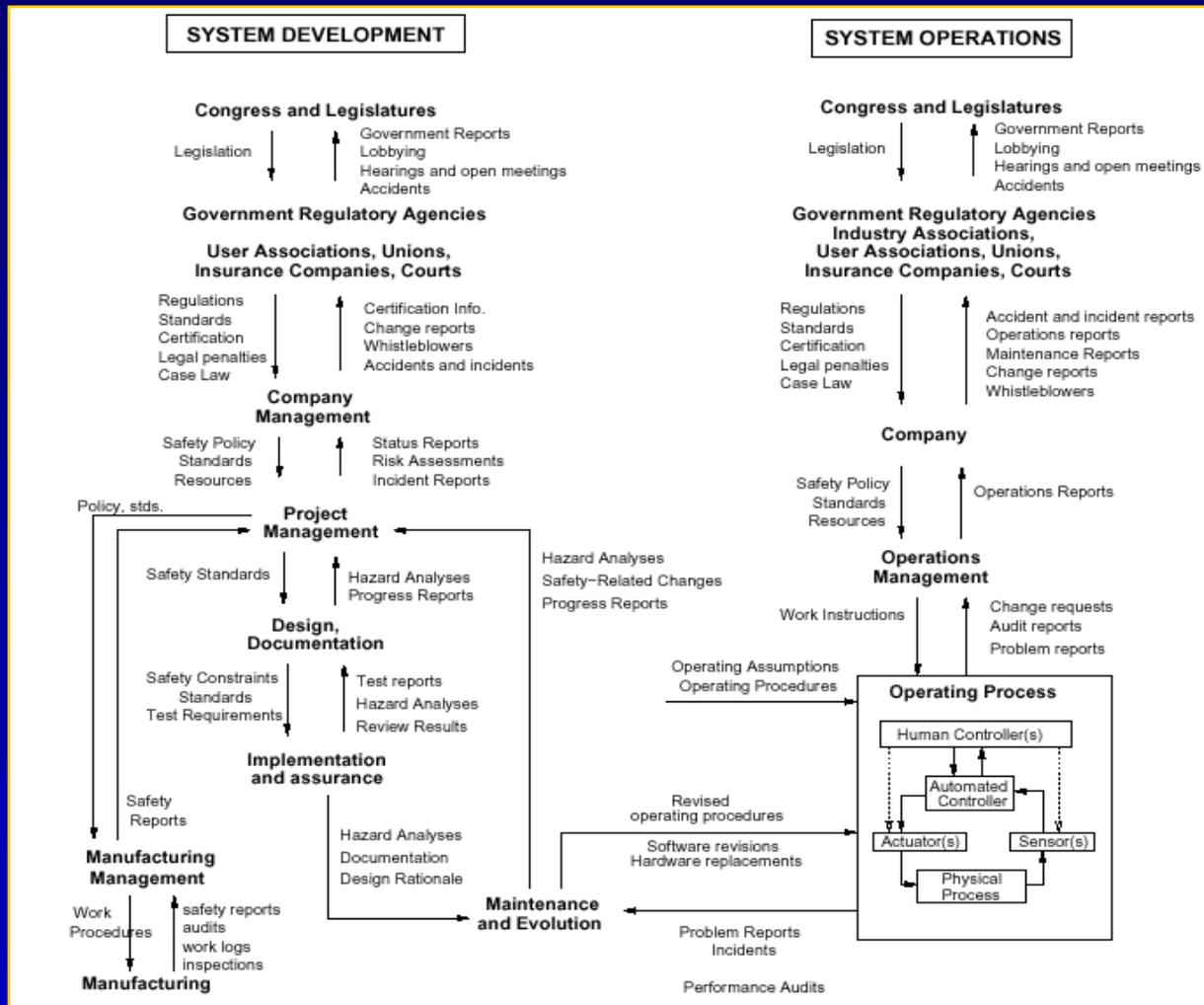
Background

- A large body of research exists on **system theory** and on the **systemic nature of accidents**
- Although accidents manifest themselves physically, they can often be traced up to a lack of constraint in the **organization**
- **Human error** and **software “errors”** are also often ignored in traditional approaches
- A few accident models reflecting this systemic, socio-technical aspect of accidents have been proposed
 - **Rasmussen (1997)**, **Vincente (2002)**, **Leveson (2002)**

System Theory Accident Modeling Process (Leveson, 2002)

- Systems viewed as interrelated components kept in dynamic equilibrium by **feedback loops** of information and control
- System safety goals are achieved if the **constraints** necessary to limit system behavior to safe changes are continuously met
- Systems divided into **hierarchical, socio-technical** levels, with control processes operating at interfaces
- **Control processes** include goals, feedbacks, constraints, time constraints and delays, etc.

STAMP: General Form of a Model of Socio-Technical Control



System Theory Hazard Analysis: Proposal

- **Only a few attempts were made to incorporate management factors to hazard analysis (e.g., MORT, Johnson, 1980)**
- **The proposed hazard analysis process is:**
 - **Place the new system in existing control structures**
 - **Identify and enforce constraints needed at the interfaces with the existing system**
 - **Define the control structures internal to the new system as the system is developed**
 - **Identify and enforce constraints within the new structure**
 - **Iterate**

The European Air Traffic Control System

- The proposed approach is most useful when applied to *Engineering Systems*: large-scale, complex systems where human and non-human elements interact
- Air Traffic Control presents all these features
- European ATC is particularly **complex** because of the multi-national, multi-organizational authorities involved
- European ATC is also undergoing **major changes**, and new hazard analysis techniques are much needed

European ATC: Current Safety Efforts

- **Role of the EATMP Safety Activities:** develop, promote and implement a harmonized approach for the safety management of air navigation services
- Current emphasis on **accident investigation and reporting** (e.g. SOFIA by EUROCONTROL)
- Other priorities: Safety Nets, commitment to decisions on safety enhancements, human factors
- Some of the proposed or implemented changes seem risky when viewed at the systemic level
 - Current risk assessments may not be exhaustive

Future Work

- Provide a more **rigorous description** of the proposed system theory hazard analysis process
- Apply the process to some of the proposed changes in the **European ATC** system
 - Identify the constraints that make today's ATC safe
 - Understand how the new changes might affect these constraints
- *Possibly* extend the results to the **US ATC** system

Thank You