

System Safety and Hazard Analysis

CSE 308: Software Engineering
SUNY at Stony Brook

Origins of System Safety

- * Rooted in industrial safety engineering
 - * Dates back to the 19th century
- * System safety emerged following WW II
 - * Systems engineering and systems analysis were developed to cope with complex systems

Safety Before WW II

- * Industrial Revolution
 - * Factory workers were “expendable”
 - * When workers accepted jobs, they accepted the risks and should be smart enough to avoid danger
- * Factories were full of hazards
 - * Workers were killed or maimed daily

Worker's Compensation

- * Employers did not have to pay if:
 - * Employee contributed to the cause of accident
 - * Another employee contributed to the accident
 - * Employee knew of the hazards involved
 - * Employee caused injury to a third party

Safety Standards

- * Initially, safety came in the form of hardware guards (interlocks, etc.)
- * Hansen's Universal Safety Standards (1914):
 - * Afford all possible safety to operator
 - * Be automatic in its action or operation
 - * Be an integral part of the machine itself
 - * Not materially diminish output or efficiency

Safety Studies

- * Heinrich's Pyramid (1929)
 - * For every serious injury, there were 29 minor injuries and 300 non-injury incidents
- * Study on safety vs. efficiency
 - * Production and safety increased together
 - * Hazards of mechanization: elimination of hand tools, exposure to machine hazards, increased operating speed

Systems Theory

- * Response to coping with complexity
- * Complementary approach to scientific reductionism
- * Reduction divides problems into distinct parts
- * Makes assumptions that hold for organized simplicity

Types of Systems

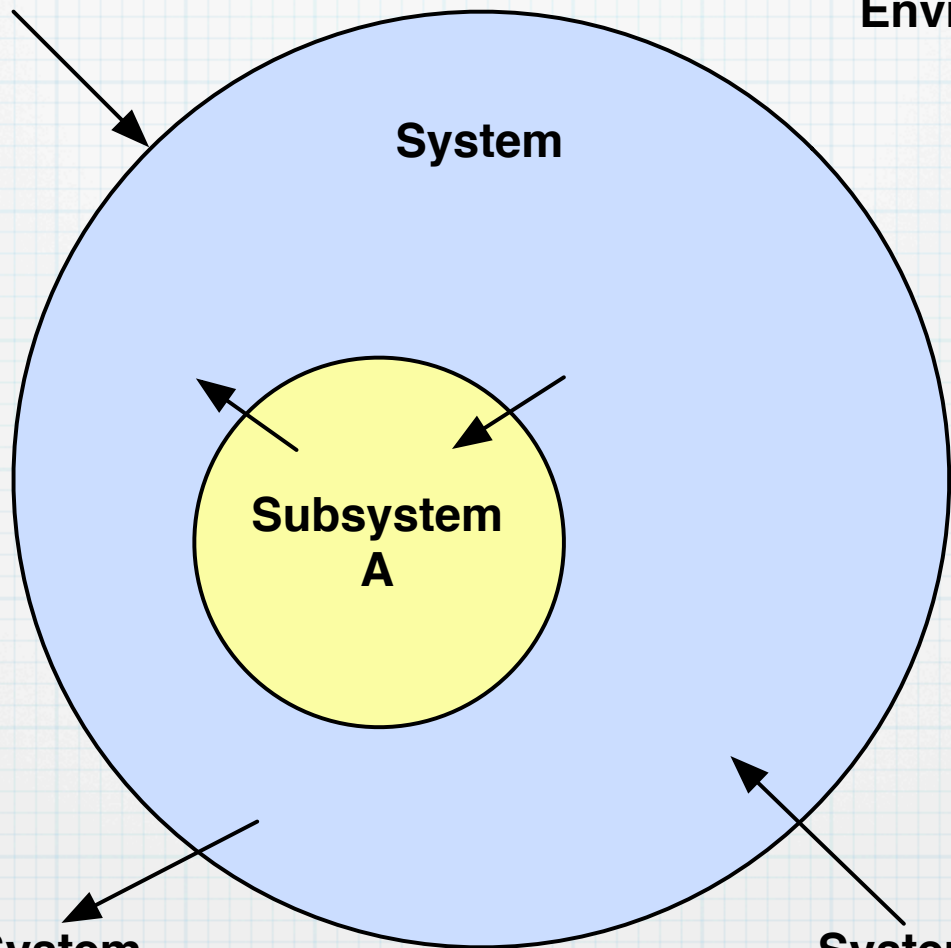
- * Organized simplicity
 - * Precise nature of components and interactions is known
- * Unorganized complexity
 - * Behavior can be studied statistically
- * Organized complexity
 - * Too complex for complete analysis, but too organized for statistics

Definitions

- * **System:** A set of components that act together as a whole to achieve some goal
- * **System state:** Set of relevant properties describing the system at some time
- * **Environment:** Set of components that are not part of the system but whose behavior affects the system

System boundary

Environment



System

**Subsystem
A**

**System
outputs**

**System
inputs**

Emergence and Hierarchy

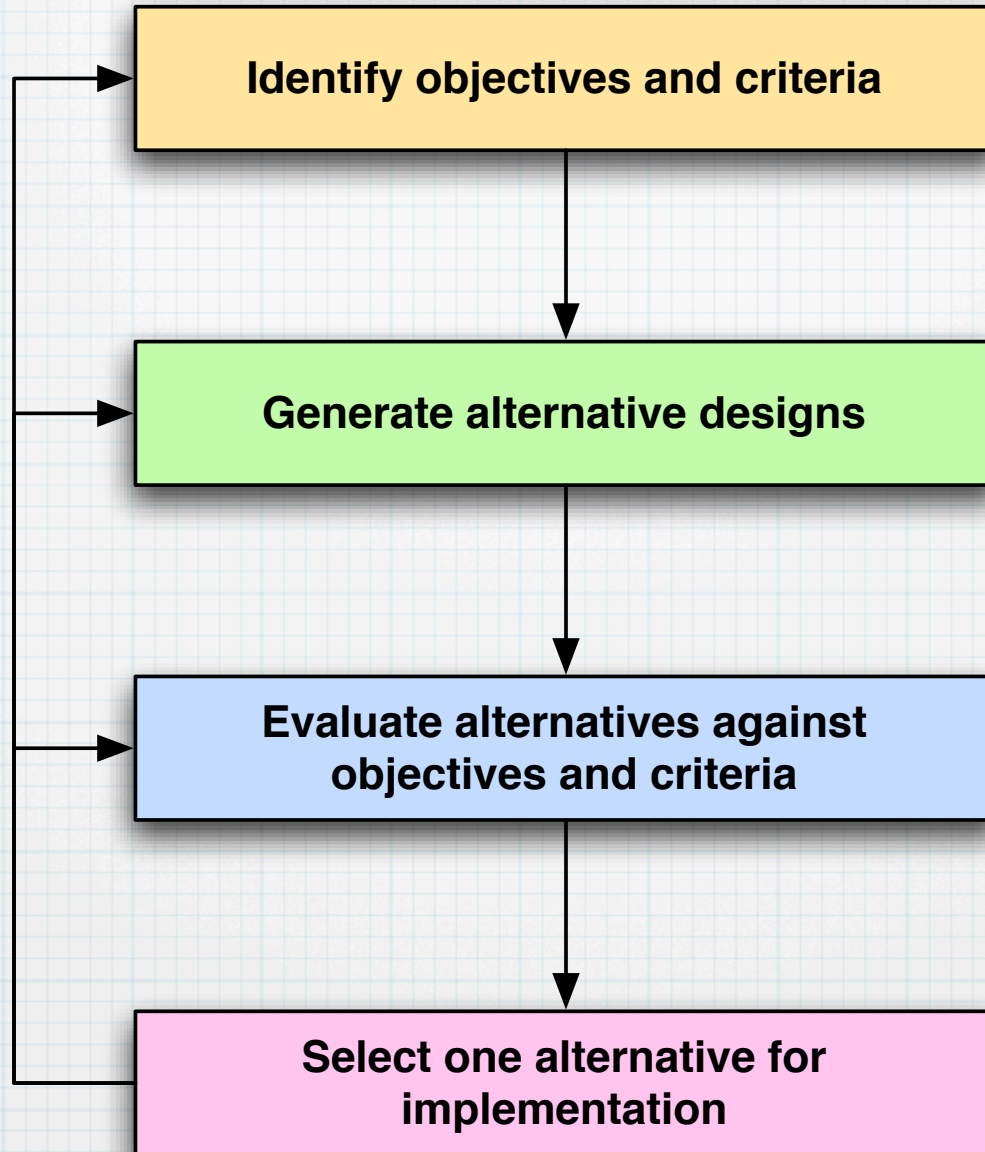
- * A system is composed of a hierarchy of levels of organization
- * Each level is more complex than the one below
- * Each level has emergent properties
 - * At a given level of complexity, some properties are irreducible
- * Safety is an emergent property of systems

Systems Engineering

- * Systems engineering is concerned with systems that are:
 - * Large (# of parts, # of functions, cost)
 - * Complex (esp. in terms of nonlinear change)
 - * Semi-automatic (human-machine interface)
 - * Unpredictable (random)

Systems Engineering

- * Shift in emphasis rather than a change in content:
 - * Defining goals, relating performance to goals
 - * Establishing/using decision criteria
 - * Developing alternatives
 - * Modeling systems for analysis
 - * Controlling/managing implementation and operation



Reliability

- * Reliability

- * The probability that a piece of equipment will perform its intended function satisfactorily for a prescribed time and under specific environmental conditions

- * Unreliability is the probability of failure

Failure

- * Failure

- * The nonperformance or inability of a system to perform its intended function for a specified time under specified environmental conditions
- * Failure may be systemic (a design flaw) or may result from deviation from the originally designed behavior
- * Ex. wear and tear, environmental change

Errors

- * Error
 - * A design flaw or deviation from a desired or intended state
 - * Note that an error is a static condition, not an event
 - * Errors may lead to failures, and vice versa

Faults vs. Failures

- * A failure is a basic abnormal event
 - * ex. a short circuit
- * A fault is a higher-order event
 - * Leads to an erroneous state
- * All failures are faults, but not all faults are failures

Types of Failures

- * **Primary fault/failure**
 - * **A component fails within the design envelope**
 - * **May be caused by defective design or manufacture**
 - * **May be caused by wear or improper maintenance**

Types of Failures

- * Secondary fault/failure
 - * Component fails due to excessive environmental stresses
 - * These failures occur randomly, and are characterized by constant failure rates

Types of Failures

- * **Command fault**
 - * **Inadvertent operation of a component because of the failure of a control element**
 - * **Ex. a relief valve opening due to an erroneous signal**

Accidents and Incidents

- * Accident

- * An undesired and unplanned event that results in a specified level of loss

- * Accidents are not necessarily unexpected!

- * Incident (near miss)

- * An event that involves no/minor loss, but with the potential for loss

Hazards

- * Hazard
 - * A state or set of conditions of a system that, together with other conditions, will lead inevitably to an accident
 - * Characteristics: severity and likelihood
 - * Hazards may be endogenous or exogenous

Risk

- * Risk

- * The hazard level (severity + likelihood), combined with:

- * Danger (likelihood of hazard leading to an accident)

- * Latency (hazard exposure/duration)

Types of Analysis

- * Hazard analysis
 - * identification of hazards and assessment of hazard level
- * Risk analysis
 - * hazard analysis, plus identification of environmental conditions and latency

Accident Models

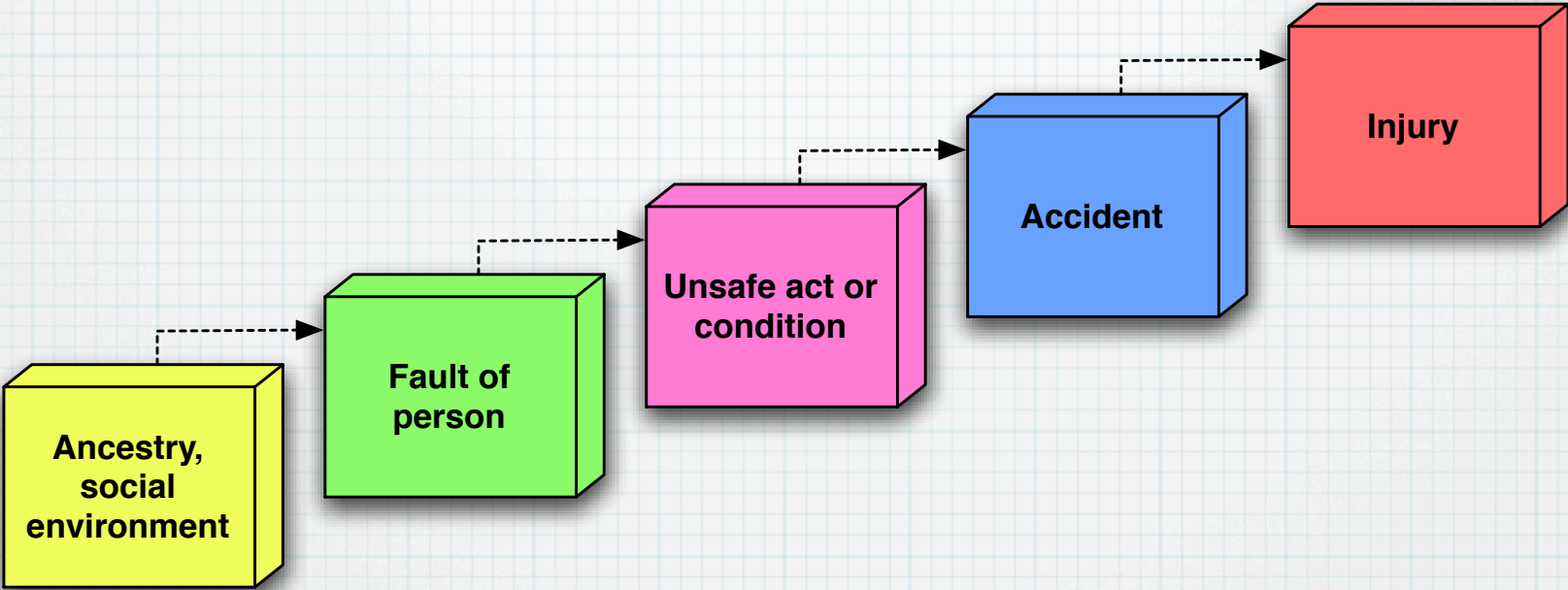
- * Describe accidents as a set of events and conditions
- * Used to understand past accidents
 - * Identify important factors
 - * Establish patterns
- * Used for accident prediction

Basic Energy Models

- * Accident = result of an uncontrolled and undesired release of energy
- * Barriers can be used to reduce accidents
- * Energy transformation accidents
 - * Ex. combustion
- * Energy deficiency accidents
 - * Ex. loss of electrical power

Domino Models

- * People, not things, cause accidents
- * Injuries result from a completed sequence of factors
- * Each factor's failure leads to (or encourages) the failure of the next one
- * Third "domino" is the easiest to remove



Revised Domino Model

1. Lack of control by management
2. Basic causes (personal and job factors)
3. Immediate causes (substandard practices)
4. Accident or incident
5. Loss

Chain-of-Events Model

- * Events are chained together into chronological sequences
- * Unsafe conditions are identified as a starting point
- * Problem: how far back do we go?
 - * “If only the employee hadn’t been born...”

Hazard Analysis

- Identifies potential problems and helps to coordinate responses/repairs
- Knowing that a hazard exists may be sufficient without knowing what caused it
- Continues throughout the life of a system, in ever-increasing depth

Hazard Analysis Goals

- Development
 - Examines new systems for hazards
- Operational management
 - Controls hazards in existing systems
- Certification
 - Demonstrates a system's level of safety

Steps Involved

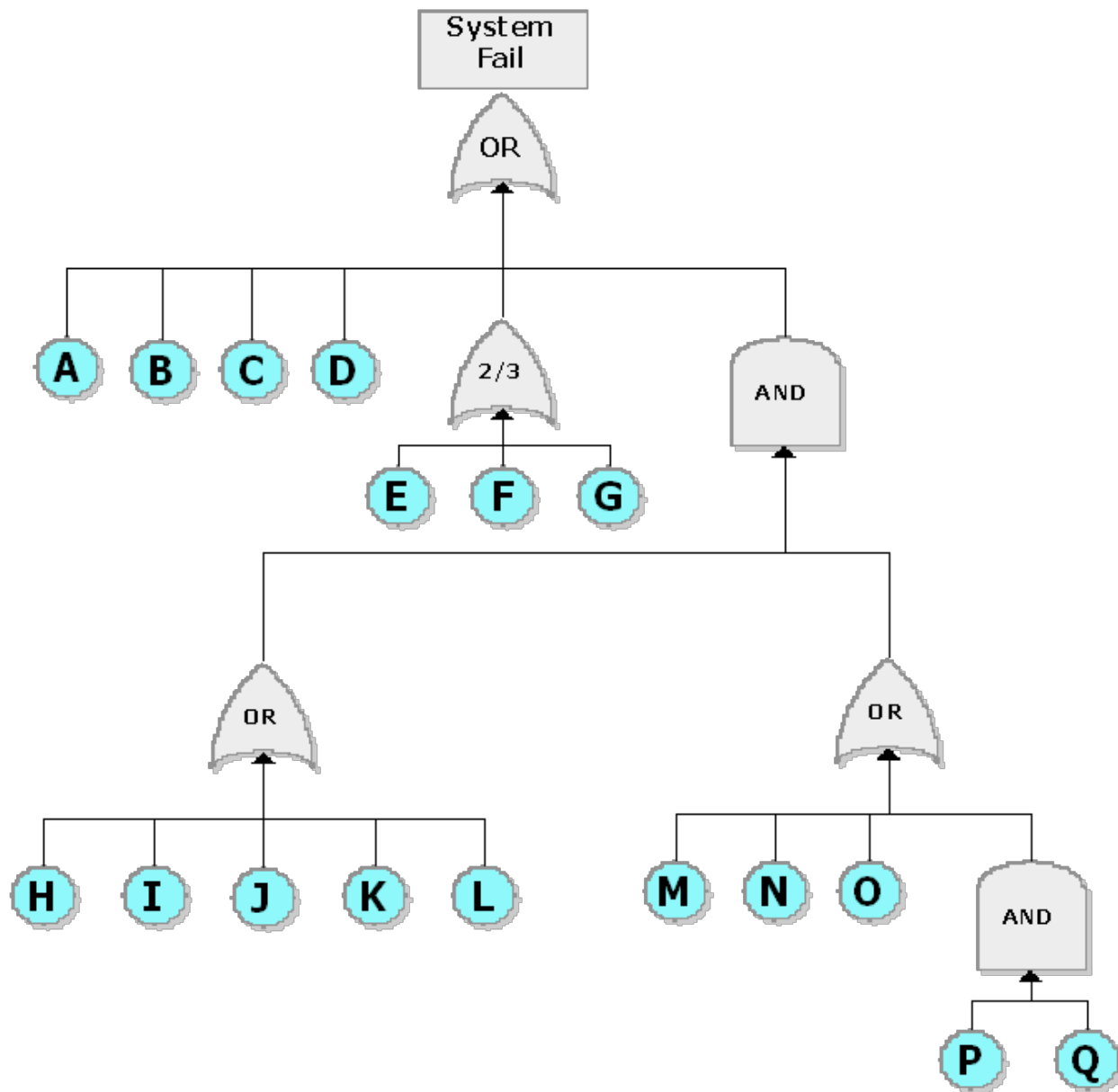
- Hazard identification
- Hazard resolution
- Verification of elimination
- Change analysis
- Operational feedback

Types of Analysis

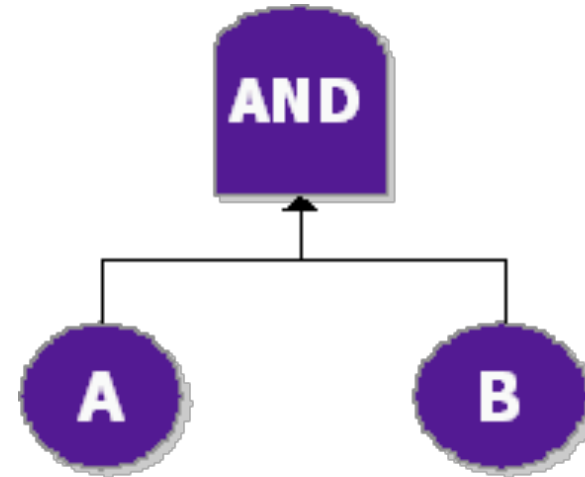
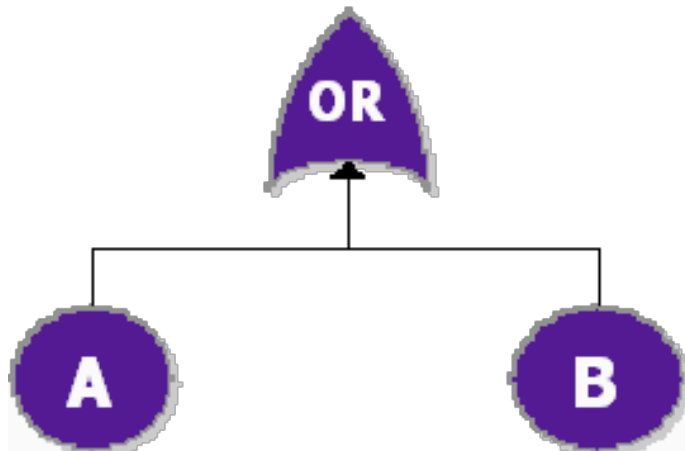
- Forward and Backward searches
 - Trace an event forward or backward to find possible results or causes
- Top-Down and Bottom-Up searches
 - Break down high-level abstractions into their constituent parts (events, conditions, etc.)

Fault Tree Analysis

- Top-down, Boolean logic-based method for analyzing the causes of a given hazard
 - Doesn't identify new hazards
- Used to describe combinations of individual faults that constitute a hazardous event
- Each level lists events that are necessary and sufficient to cause the problem above



Fault Tree Operations



Next Time

- Layered Software Development