Hazard Analysis and Safe Product Design

Robert R. Scheibe, Ph.D., P.E.
GT Engineering
UW Department of Mechanical Engineering

Steps to Consider for Safe Design

- Determine scope of the product's use
- Identify the environment product will be used in
- Describe the user population
- Determine all possible hazards
- Determine the probability of certain hazards
- Determine the seriousness of possible injury/loss

Weinstein, 1978

Steps to Consider, cont.

- Postulate alternative design features to mitigate or eliminate hazards (incl. warnings, instructions)
- Determine whether alternative design introduces new hazards (incl. warnings, instructions)
- Investigate similar products or environments

Steps to consider, cont.

- Determine cost of alternative design
- Determine whether warnings or instructions will be followed by the user (i.e., test them)

Hazard Analysis Techniques

- Gross-hazards analysis
  - Done early in design process
  - Considers overall performance rather than individual components
- Classification of hazards
  - Identifies types of hazards from above
  - Displays them according to severity

Hazard Analysis Techniques, cont

Failure mode and mechanism analysis

- Modes
  - Plastic collapse
  - Excessive deformation
  - Fatigue
  - Instability (elastic or inelastic)
  - Brittle Failure
  - Creep
  - Corrosion
- Mechanisms
  - Force/displacement
  - Time (history of initiation or occurrence)
  - Dimensions
  - Temperature
  - Environment (chemical or physical)
  - Material State

Hodge and Phillip, 1971

Hazard Analysis Techniques, cont

- Reliability-risk analysis
  - Uses statistical data to assess confidence levels and probability of failure
- Fault tree analysis
  - Outlines possible sequences of events leading to an incident
- Energy release analysis
  - Determines energy release in catastrophic event

Hazard Analysis Techniques, cont

- Catastrophic analysis
  - Identifies modes of failure that would create a catastrophic event
- Systems analysis
  - Reveals interfaces and interrelationships between systems
- Maintenance hazards analysis
  - Evaluates performance of maintenance procedures and whether such actions create new hazards

Hazard Analysis Techniques, cont

- Human factors analysis
  - Defines skills needed to operate and maintain systems
  - Evaluates role human capability and error

Brown, 1991

Fault Tree Analysis

- A logic event diagram showing symbolic representation of the necessary and sufficient subsystem failures needed to result in an undesired event

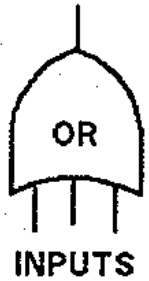
Fault Tree Analysis

- Most important step: clearly defining the top undesired event

Fault Tree Symbology

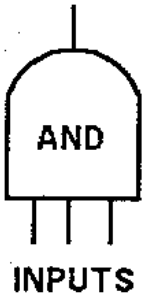
System component or basic fault event.

The diamond is used to represent a fault event which is not developed further due to lack of information.



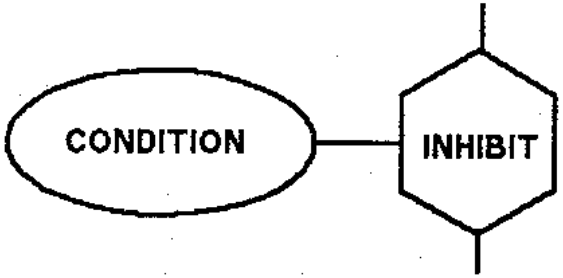
OR GATE
This gate is in the failed state if at least one of its inputs is in the failed state.

TRANSFER SYMBOLS.
These symbols are used to transfer an entire part of the tree to other locations on the tree.



AND GATE
This gate is in the failed state only if all of its inouts are simultaneously in their failed states.

Fault Tree Symbology, cont.

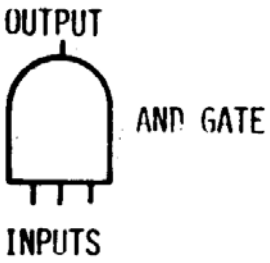


INHIBIT GATE.
This represents an event which occurs with some probability of occurence. The inhibit gate is in the failed state only if its inputs are in the failed state and the inhibit condition has occured.

EVENT DESCRIPTION.
The rectangle is used to describe the event represented by the gate.

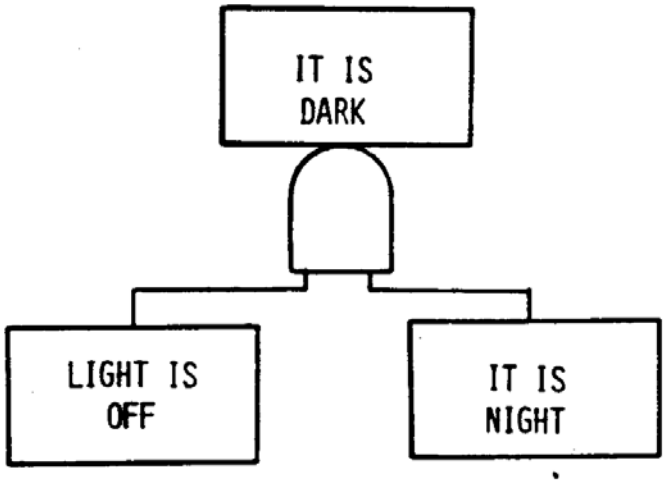
The house represents an event which is normally expected to occur.

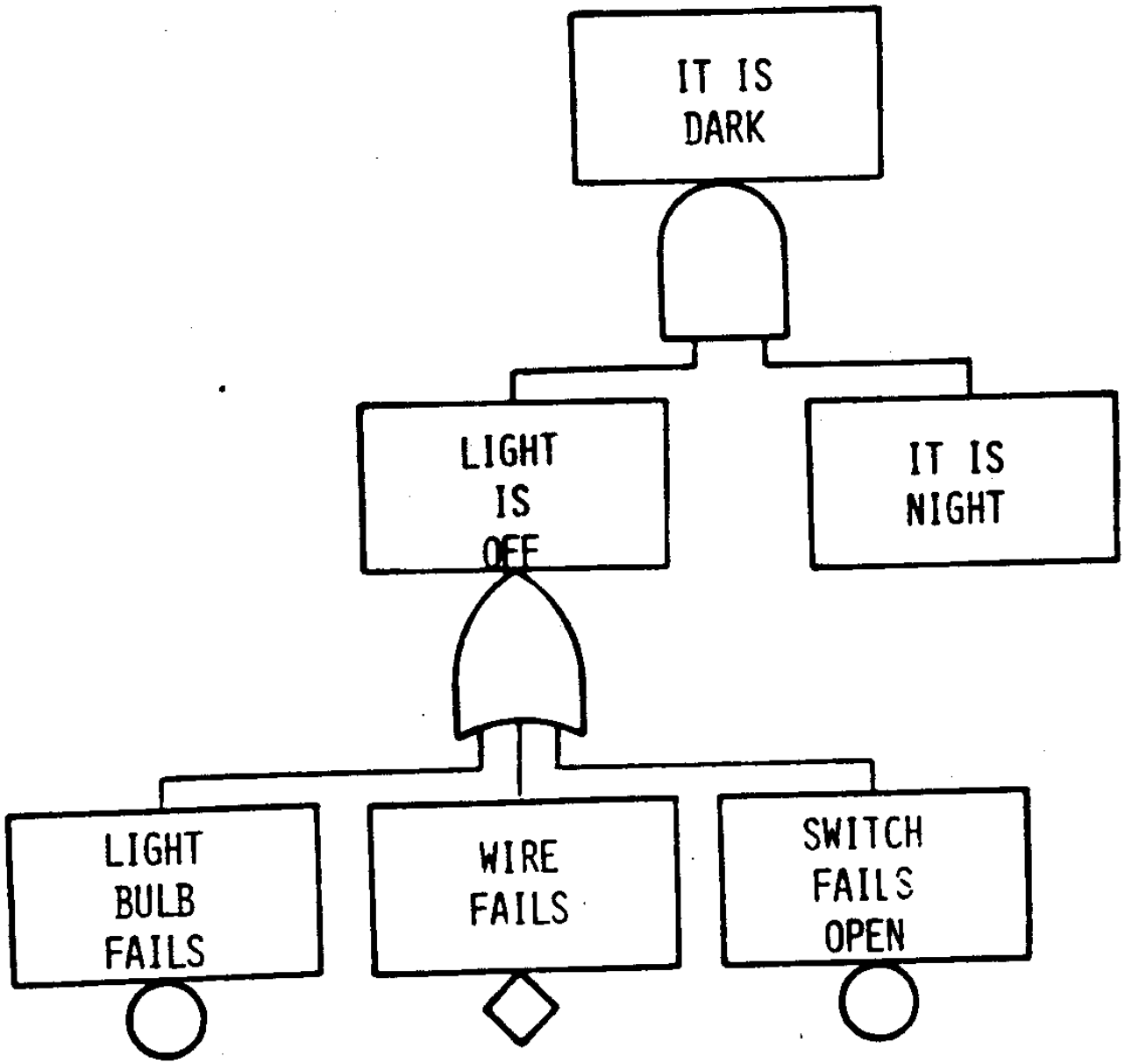
LOGIC SYMBOL



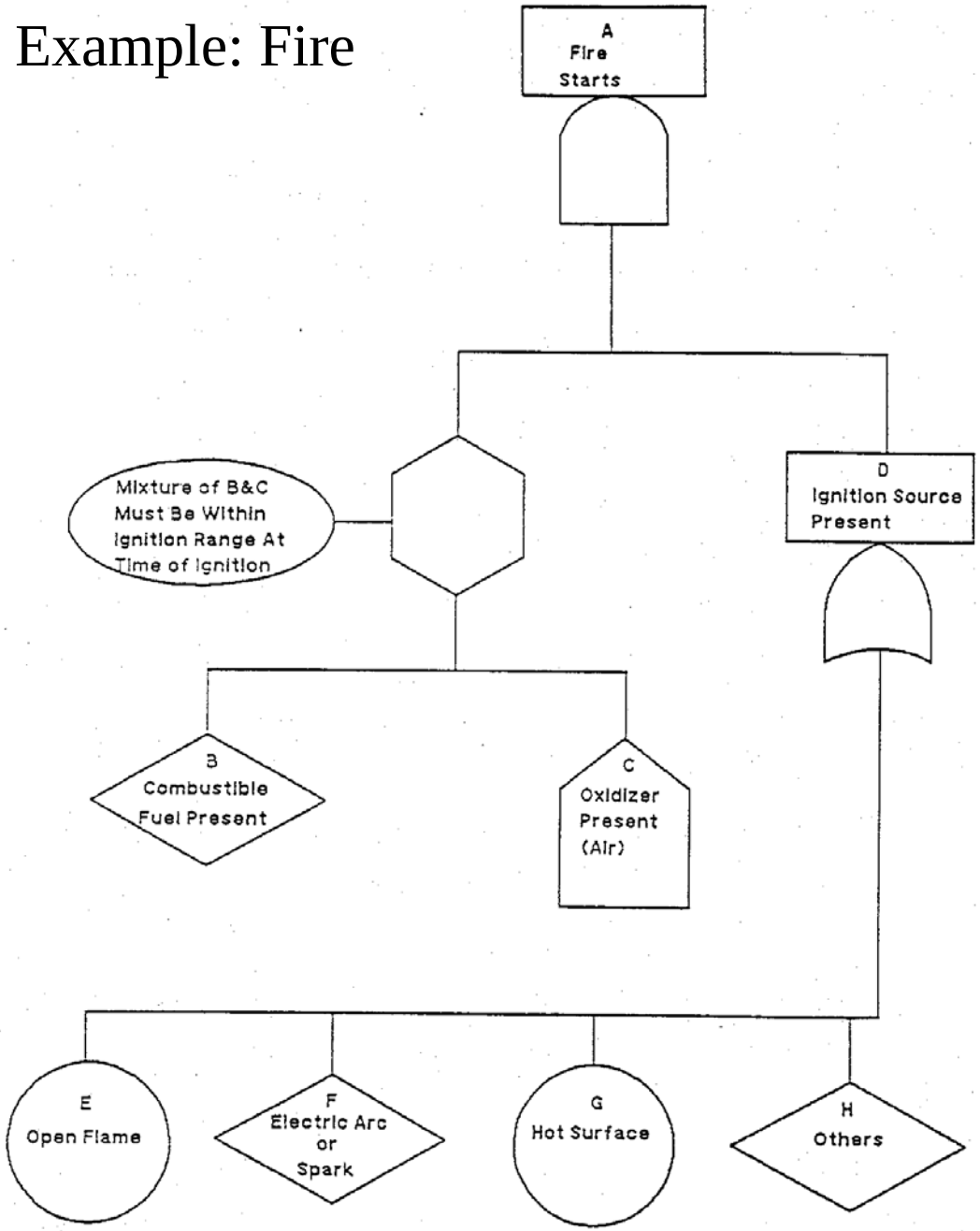
COEXISTENCE OF ALL INPUTS IS REQUIRED
TO PRODUCE OUTPUT

EXAMPLE

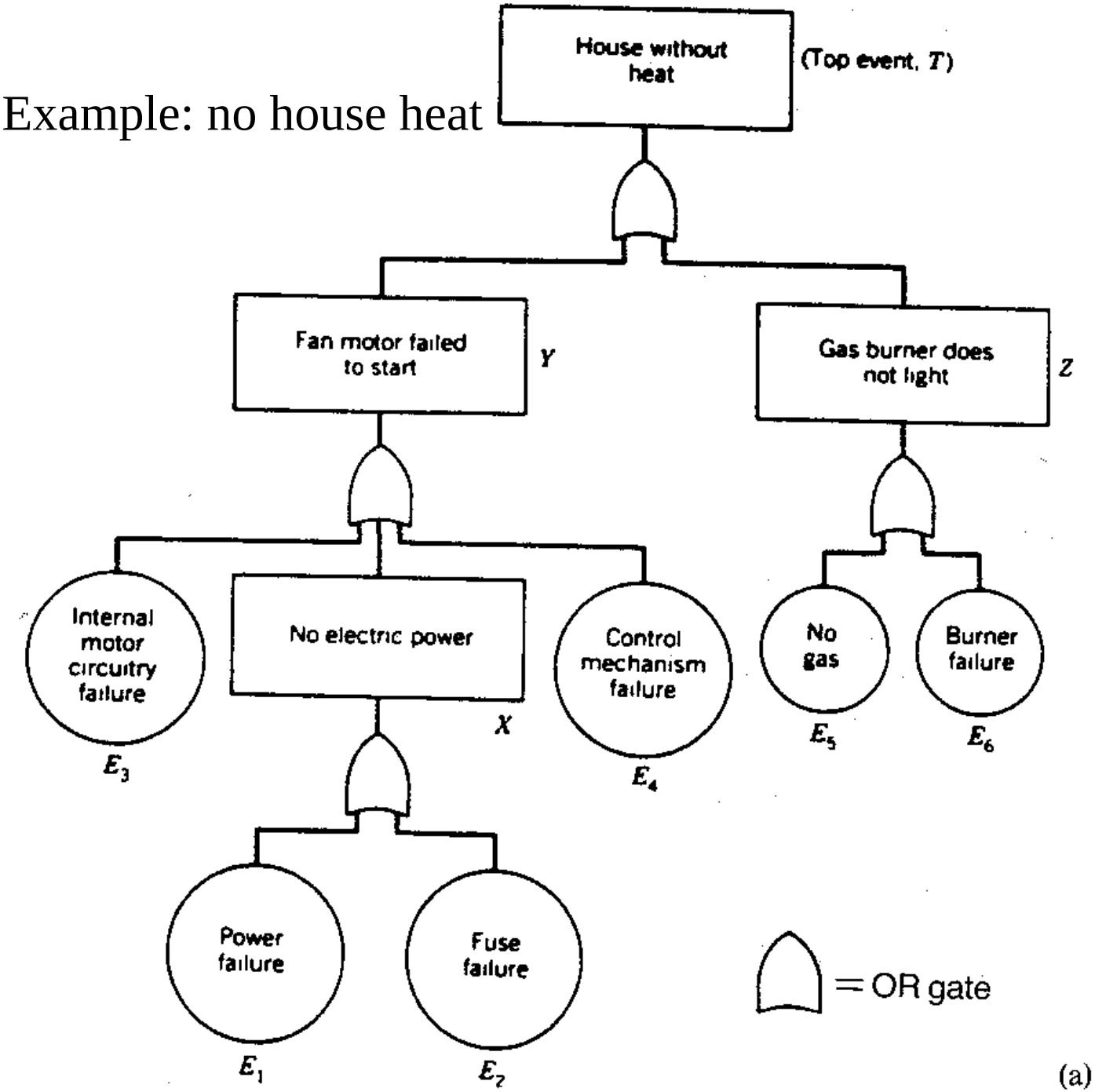



IT IS DARK
LIGHT IS OFF
IT IS NIGHT
LIGHT BULB FAILS
WIRE FAILS
SWITCH FAILS OPEN

Example: Fire



Example: no house heat



Fault Tree Analysis

- Advantages
  - Formalized, systematic deductive analysis approach
  - Forces thought about possible product hazards
  - Results in clear graphic record of the process
  - Readily identifies logical causes of accidents
  - Can be evaluated qualitatively or quantitatively
  - Useful in evaluation of design or procedural alternatives
  - Identifies areas for detailed evaluation by other techniques

Fault Tree Analysis

- Limitations
  - Requires thorough understanding of system and its operation in normal and abnormal states
  - No formalized way to ensure consideration of human factors
  - Quantification is difficult

End