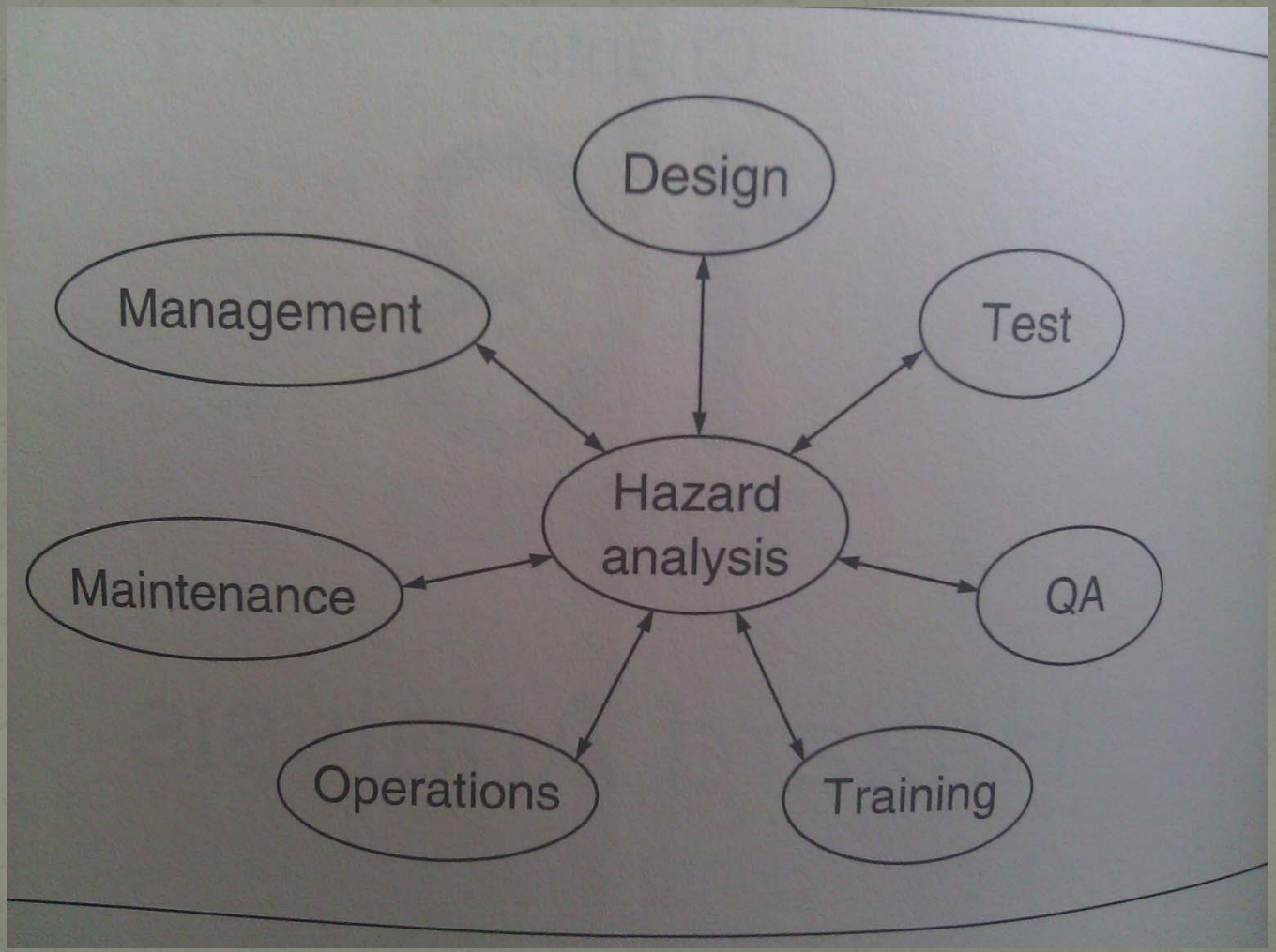
Hazard Analysis

Andrew Hillocks

Quote by Richard Feynman

- "The argument that the same risk was flown before without failure is often accepted as an argument for the safety of accepting it again. Because of this, obvious weaknesses are accepted again and again, sometimes without a sufficiently serious attempt to remedy them, or to delay a flight because of their continued presence."

Hazard analysis provides visibility and coordination



Goals of Hazard Analysis

- 1. **Development**: the examination of a new system to identify and assess potential hazards and eliminate or control them.
- 2. **Operational management**: the examination of an existing system to identify and assess hazards in order to improve the level of safety, to formulate a safety, to formulate a safety management policy, to train personnel, and to increase motivation for efficiency and safety of operation.
- **Certification**: the examination of a planned or existing system to demonstrate its level of safety and to be accepted by the authorities.

Qualitative vs. Quantitative Analyses

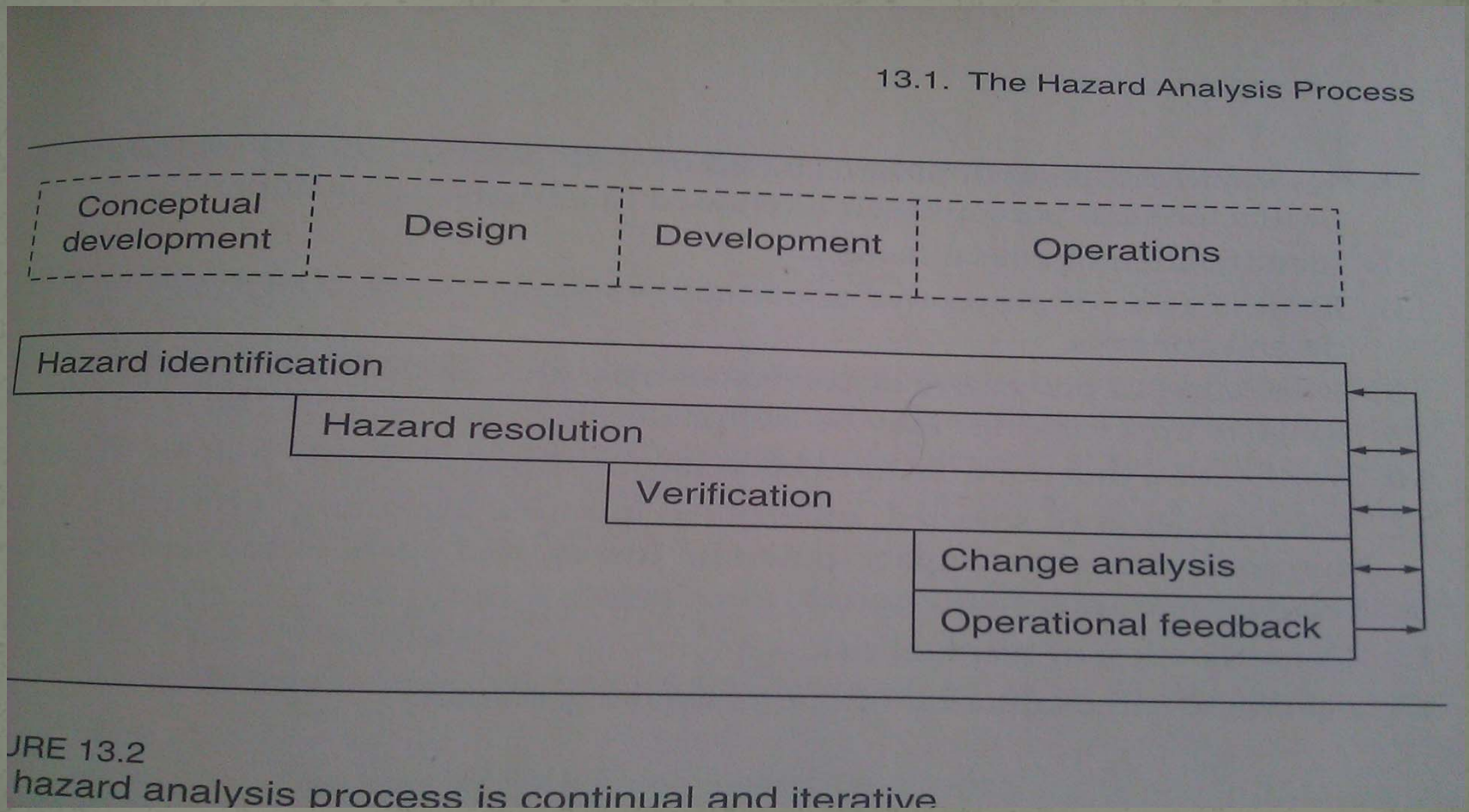
- Simple VS advanced
- Causal factors VS numerical values
- Before VS during
- Ranking VS data

- Analysis can often end with qualitative aspects. Causal factors must be identified before numerical values can be assigned for a quantitative analyses. Important factors such as design deficiencies and comparing reliability can only be measured by quantitative Analyses however.

Role and Qualifications of the Analyst

- Role: to generate alternatives as well as eliminate them.
- New alternatives can be much more valuable than analyzing given approaches.
- Safety programs should be less expensive than other alternatives, while having better safety, and few trade-offs.
- Qualifications:
- Understanding of system under consideration.
- Engineering expertise
- Good Judgment

The hazard analysis process is continual and iterative



URE 13.2
hazard analysis process is continual and iterative

Steps in the Process

- 1. Definition of objective
- 2. Definition of scope
- 3. Definition and description of the system
- 4. Identification of Hazards
- 5. Collection of data
- 6. Qualitative ranking of hazards
- 7. Identification of causal factors
- 8. Identification of preventive/corrective measures
- 9. Evaluation of preventive/corrective measures
- 10. Verification of controls
- 11. Quantification of unresolved hazards
- 12. Quantification of residual risk
- 13. Feedback and evaluation of operational experience

Hazard Identification

- 1. Determining what hazards might exist during operation of the system and their relative magnitude.
- 2. Developing guidelines, specifications, and criteria to be followed in system design.
- 3. Initiating actions for the control of particular hazards.
- 4. Identifying management and technical responsibilities for action and risk acceptance and assuring that effective control is exercised over the hazards.
- 5. Determining the magnitude and complexity of the safety problems in the program.

Hazard Level

- The hazard category or level is defined by likelihood and severity.
- Ex:
- Category I: Catastrophic; may cause death or system loss.
- Category II: Critical; may cause severe injury, severe occupational illness, or major system damage.
- Category III: Marginal; may cause minor injury, minor occupational illness, or minor system damage.

Operational Phase

- Whether an accident actually occurs as a result of a hazard and the severity of the hazard may depend upon the operational phase—the system and environmental conditions—in which the hazard occurs

- Ex: rocket

Hazard causal analysis

- After being identified, the cause of the hazard must be determined.

- System Hazard Analysis
- Subsystem Hazard Analysis
- Software Hazard Analysis
- Operational Hazard Analysis

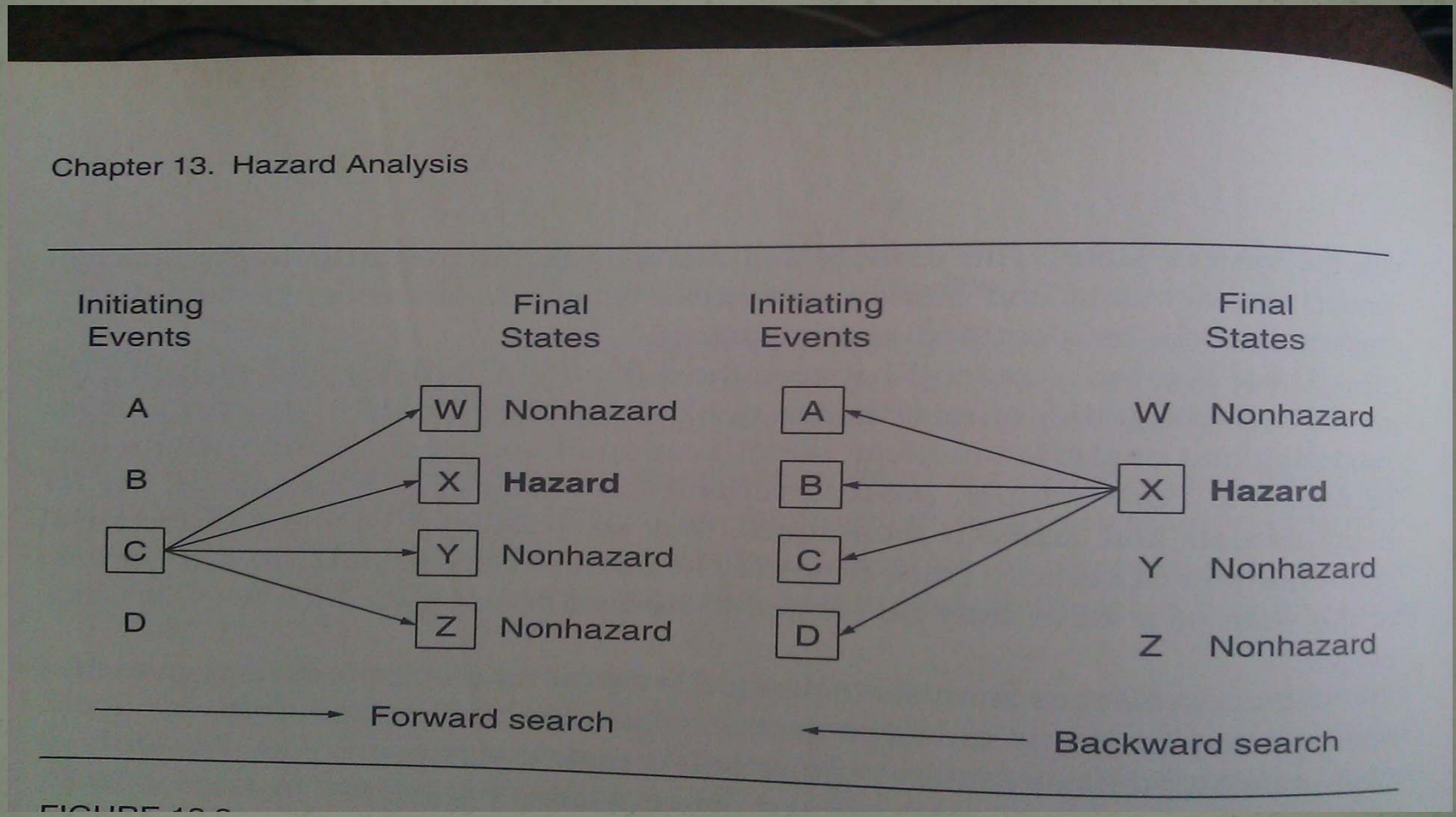
Risk Assessment and Acceptance Analysis

- Once design and development are complete, the system design can be evaluated. Final product is evaluated as a whole.
- Asses Harmful Consequences
- Asses Human Error

Types of System Models

- **Material**: represents a complex system by another physical system that is simpler yet similar in respect
- **Dynamic**: features of the model vary with time
- **Stochastic** : containing probable or random events that affect the outcome or response of model
- **Iconic**: visually represents aspects of the system
- **Formal**: represents structural properties
- **Analog**: employs one set of properties to represent another set
- **Symbolic**: uses math or logic operations to predict behavior

Forward VS. Backwards searching



Questions?