Human Error

Latent Errors and Systems Disasters

Introduction

- Active errors: effects felt immediately
  - frontline operators of a complex system
    - pilots, air traffic controllers, ships' officers, control room crews and the like

- Latent errors: adverse consequences lie dormant within the system
  - evident when combine with other factors
  - whose activities removed in time and space from direct control interface
    - Designers, high-level decision makers, construction workers, managers and maintenance personnel.

Latent Errors

- Greatest threat to safety of a complex system

- Root causes:
  - Present long before active errors are committed

Operators

- Instigators of an accident?
- Inheritors of system defects?
  - Poor design
  - Incorrect installation
  - Faulty maintenance
  - Bad management decisions
- Discover and neutralize latent failures **vs.** minimize active errors

Factors Affecting Human Performance

1. Systems have become more automated
2. Systems have become more complex and more dangerous
3. Systems have more defenses against failure
4. Systems have become more opaque
5. The ironies of automation
6. The operator as temporal coordinator

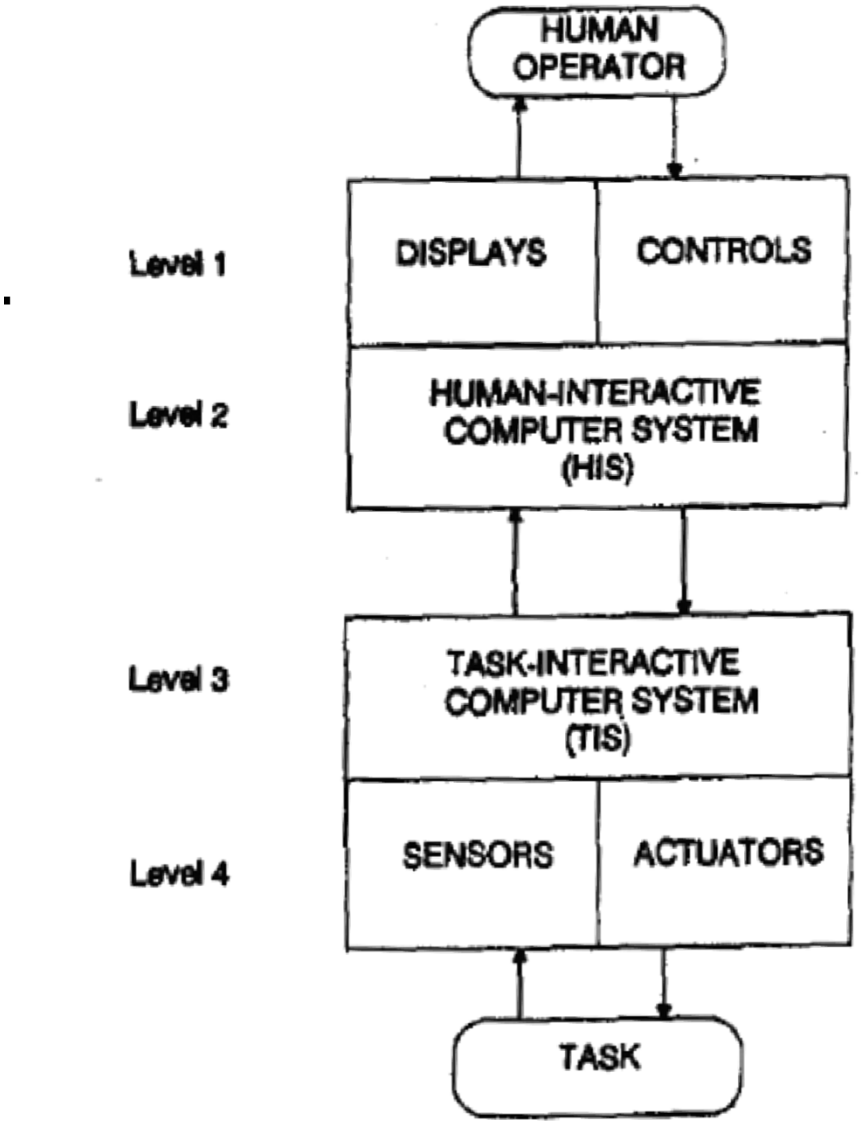

Figure 7.1. The basic elements of supervisory control (after Moray, 1986).

Distinguishing Errors and Violations

- One may err without committing a violation; a violation need not involve error.
- Errors may be defined in relation to the cognitive process of the individual
- Violations can only be described with regard to a social context in which behavior is governed by operating procedures, codes of practice, rules and the like

Violations

- Deliberate deviations from practices deemed necessary to maintain safe operation of a potentially hazardous system

- Boundaries between errors and violations are by no means hard and fast, either conceptually or within a particular accident sequence

Preliminary Classification of Violations

1. The boundary Categories
2. Routine Violations
3. Exceptional Violations

The Boundary Categories

- Intentionality
  - No → erroneous or unintended violations
  - Yes (deliberate) → prior intention to cause damage to the system → yes → sabotage

- Middle ground
  - Some degree of intentionality, but do not involve the goal of system damage

The Boundary Categories

- Routine violations
  - habitual, forming an established part of an individual's behavioral repertoire

- Exceptional violations
  - Singular violations occurring in a particular set of circumstances

Routine Violations

- Natural human tendency to take the path of least effort
- Relatively indifferent environment
  - (i.e. one that rarely punishes violations or rewards observance)
- Transgressing an trivial and rarely sanctioned safety procedure
- Could be minimized by designing systems with human beings in mind at the outset

Exceptional Violations

- Product of a wide variety of local conditions
- System double-binds
  - particular tasks or operating circumstances that make violations inevitable, no matter how well-intentioned the operators might be

General View of Accident Causation in Complex Systems

- Basic elements or production
  - Decision makers
  - Line management
  - Preconditions
  - Productive activities
  - Defences

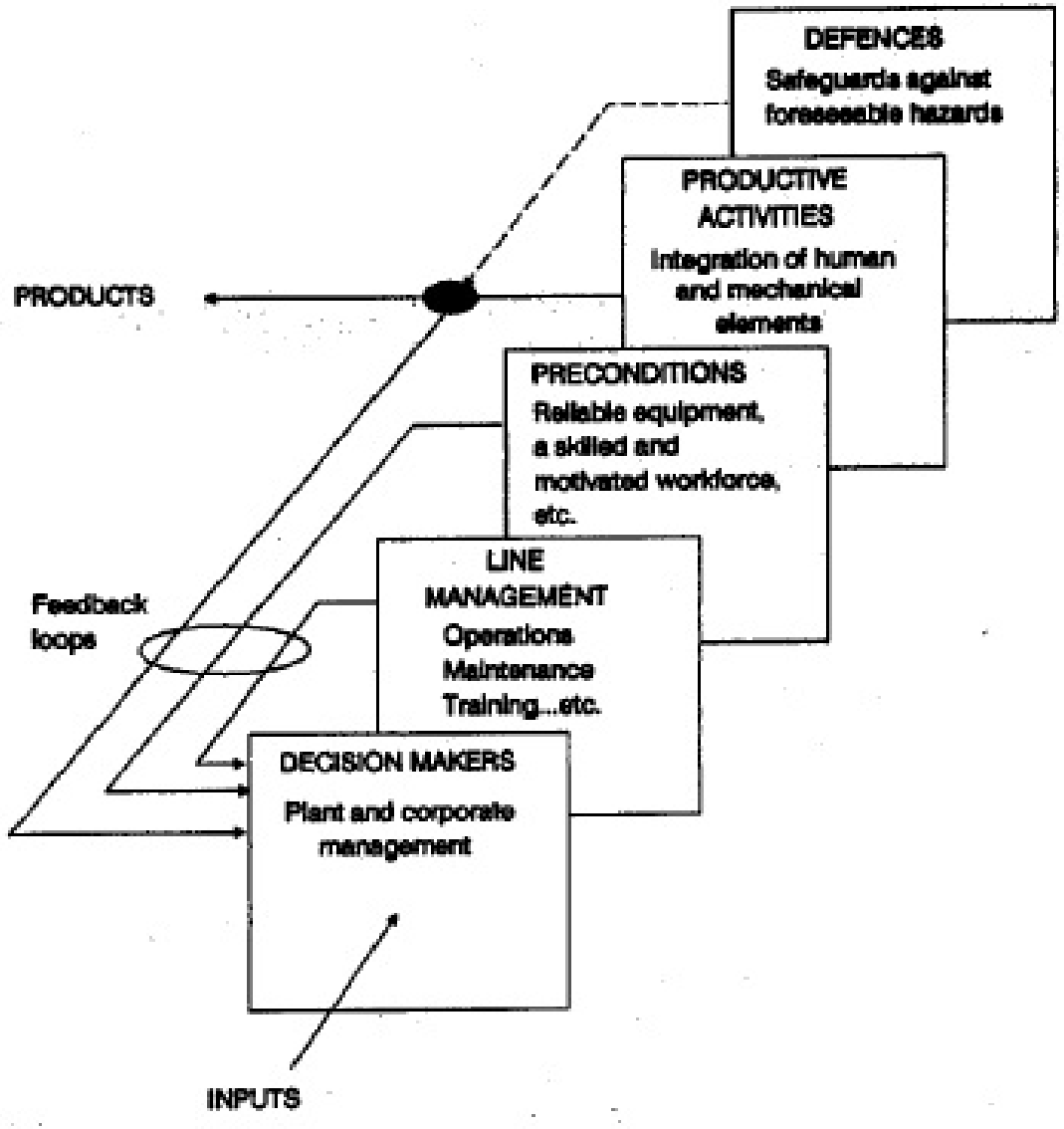

Figure 7.4. The basic elements of production. These constitute the necessary and benign components of any productive system.

Human Elements of Accident Causation

- Fallible decisions
- Line management deficiencies
- Preconditions for unsafe acts
- Unsafe acts
- Defenses: The limited window of accident opportunity

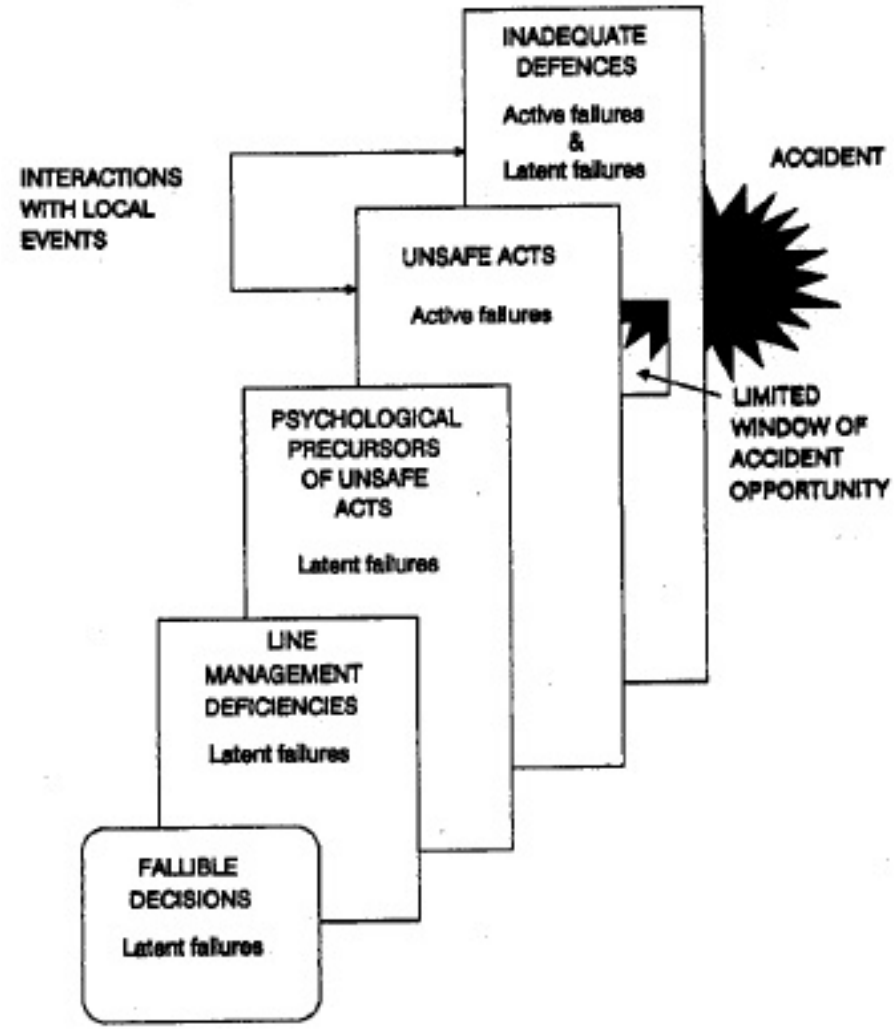

Figure 7.5. The various human contributions to the breakdown of complex systems are mapped onto the basic elements of production. It is assumed that the primary systemic origins of latent failures are the fallible decisions taken by top-level plant and corporate managers. These are then transmitted via the intervening elements to the point where system defences may be breached.

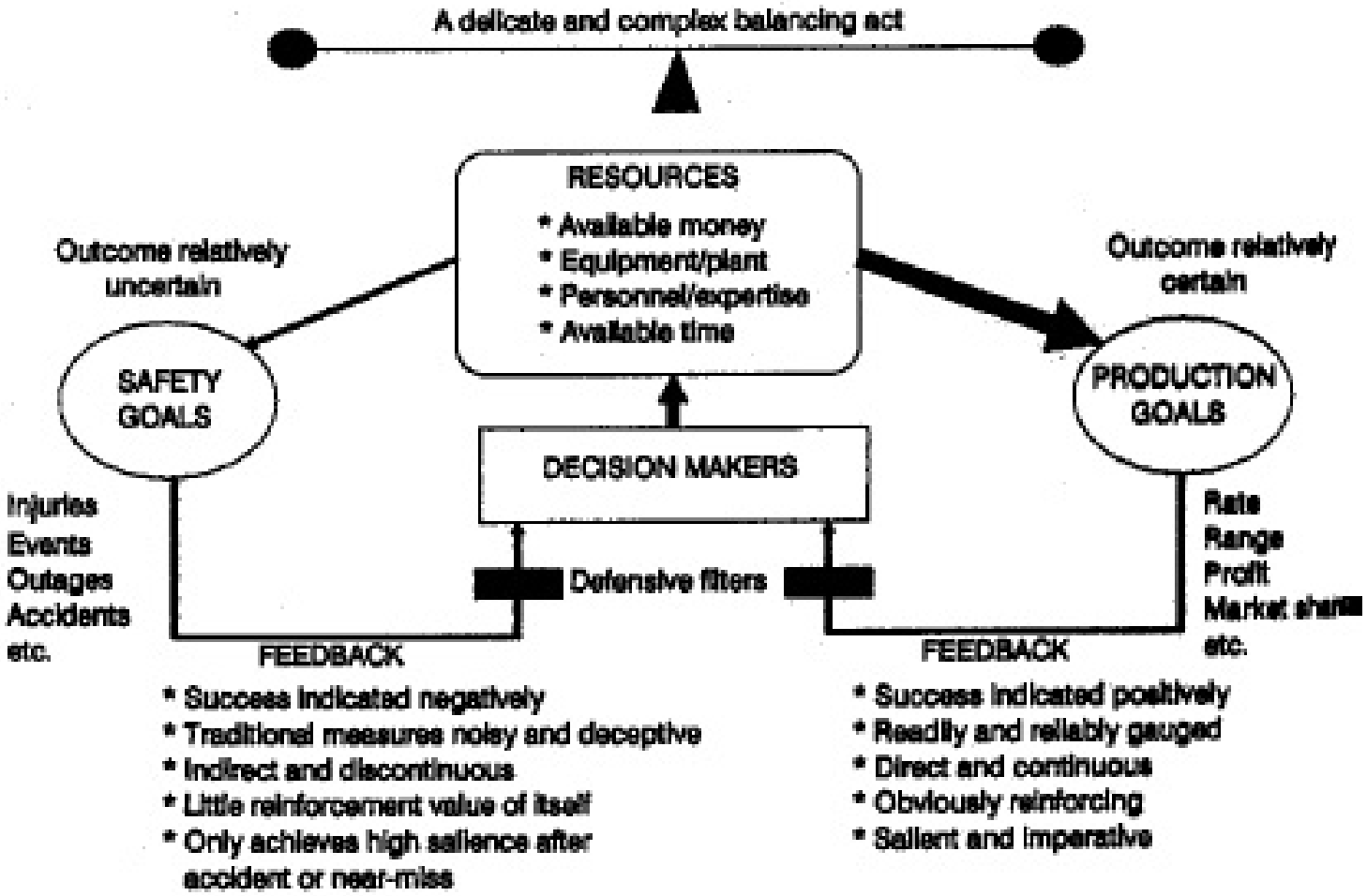

Figure 7.6. A summary of some of the factors that contribute to fallible, high-level decision making. Resources allocated to production and safety goals differ (a) in their certainty of outcome, and (b) in the nature and impact of their respective feedback.

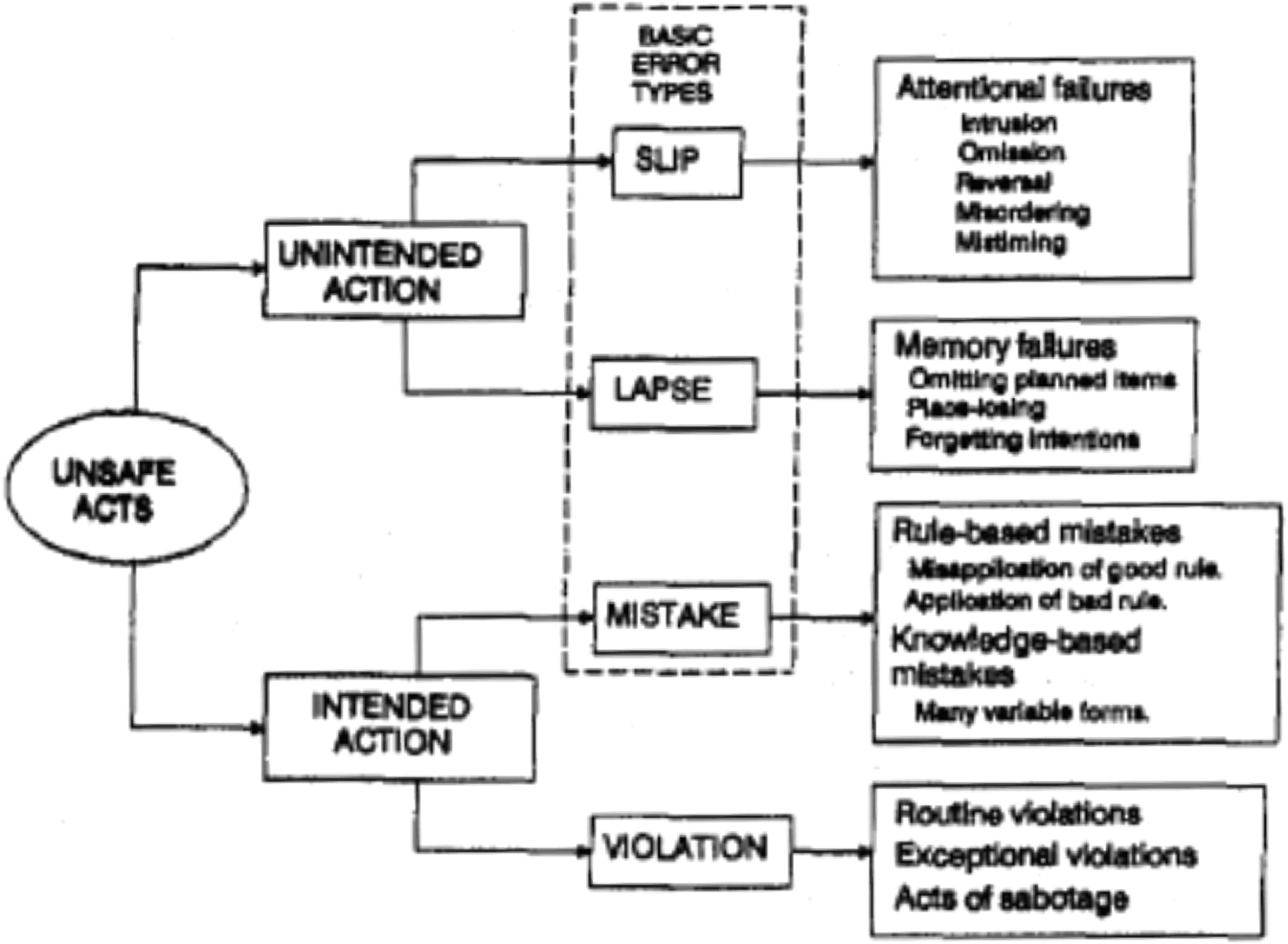

Figure 7.7. A summary of the psychological varieties of unsafe acts, classified initially according to whether the act was intended or unintended and then distinguishing errors from violations

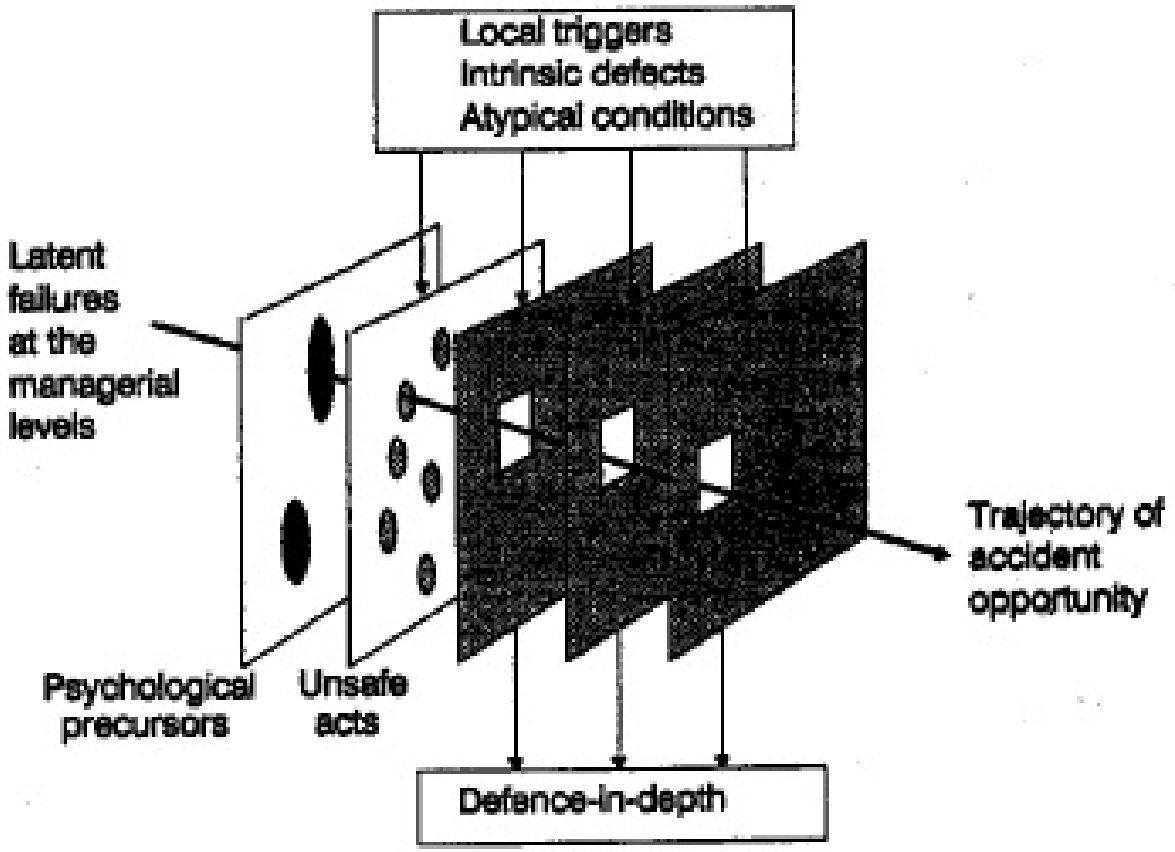

Figure 7.8. The dynamics of accident causation. The diagram shows a trajectory of accident opportunity penetrating several defensive systems. This results from a complex interaction between latent failures and a variety of local triggering events. It is clear from this figure, however, that the chances of such a trajectory of opportunity finding loopholes in all of the defences at any one time is very small indeed.

Controlling Safer Operations

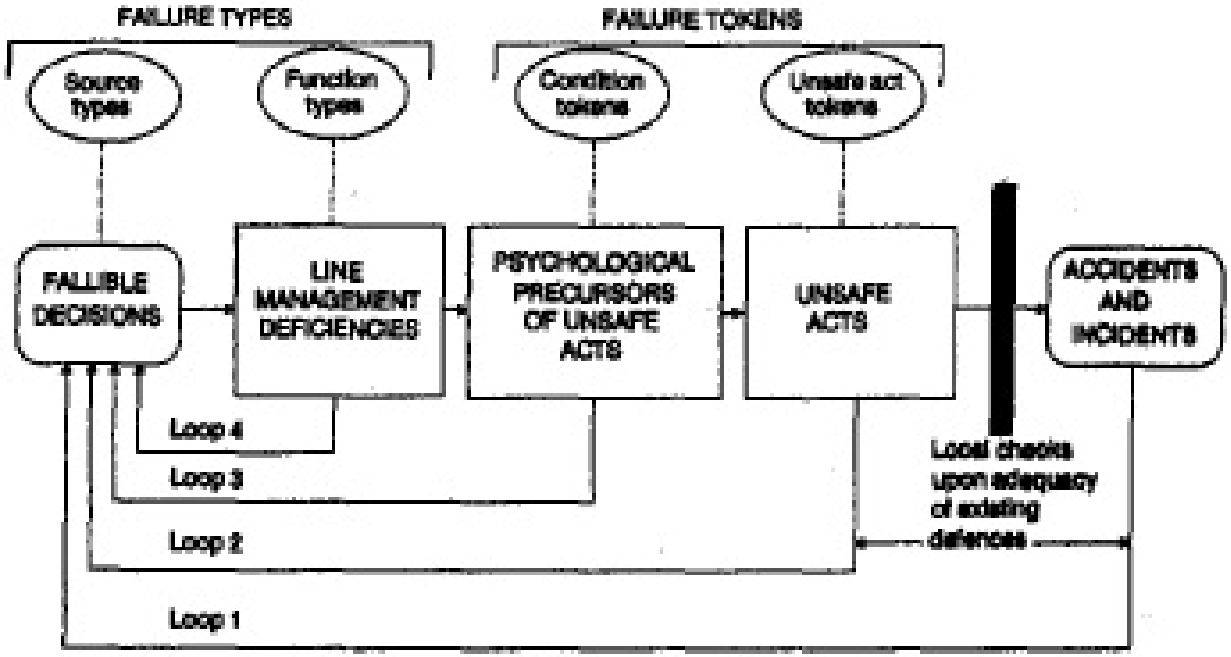

Figure 7.9. Feedback loops and indicators. The indicators are divided into two groups: *failure types* (relating to deficiencies in the managerial/organisational sectors) and *failure tokens* (relating to individual conditions and unsafe acts).

Controlling Safer Operations

- Continuous process
- Prerequisites for adequate safety control are:
  - Sensitive multichannel feedback system (SIS)
  - Ability to respond rapidly and effectively to changes

Organizational Responses to Hazards

- Denial Actions
  - **Suppression:** observers punished, observations erased
  - **Encapsulation:** observers retained, observations validity disputed or denied
- Repair Actions
  - **Public Relations:** observations emerge publicly, significance denied; sugar-coated
  - **Local Repair:** problem fixed at local level, wider implications denied
- Reform Actions
  - **Dissemination:** problem admitted to be global, global action is taken upon it
  - **Reorganization:** reconsideration and reform of the operational system

Organizational Responses to Hazards

- More effective the organization
  - Respond to safety data with actions from the bottom (i.e., reform),
- Less adequate will employ responses from the top (i.e., denial)

Pathological Organizations

- Safety measures are:
  - inadequate,
  - sacrifice safety goals in the pursuit of production goals,
  - often under severe economic pressures
  - Actively circumvent safety regulations

- Information about hazardous conditions is denied (suppressed or encapsulated)

Calculative Organizations

- Do the best job they can
- Using 'by-the-book' methods
- Adequate under normal operating conditions
- Fail when encounter unforeseen circumstances

Generative Organizations

- High degree of irregular activity in furthering their goals
- Set targets beyond ordinary expectations and fulfill them
- Emphasize results rather than methods
- Value substance more than form
- Hazards quickly discovered and neutralized

Learning the right lessons from past accidents