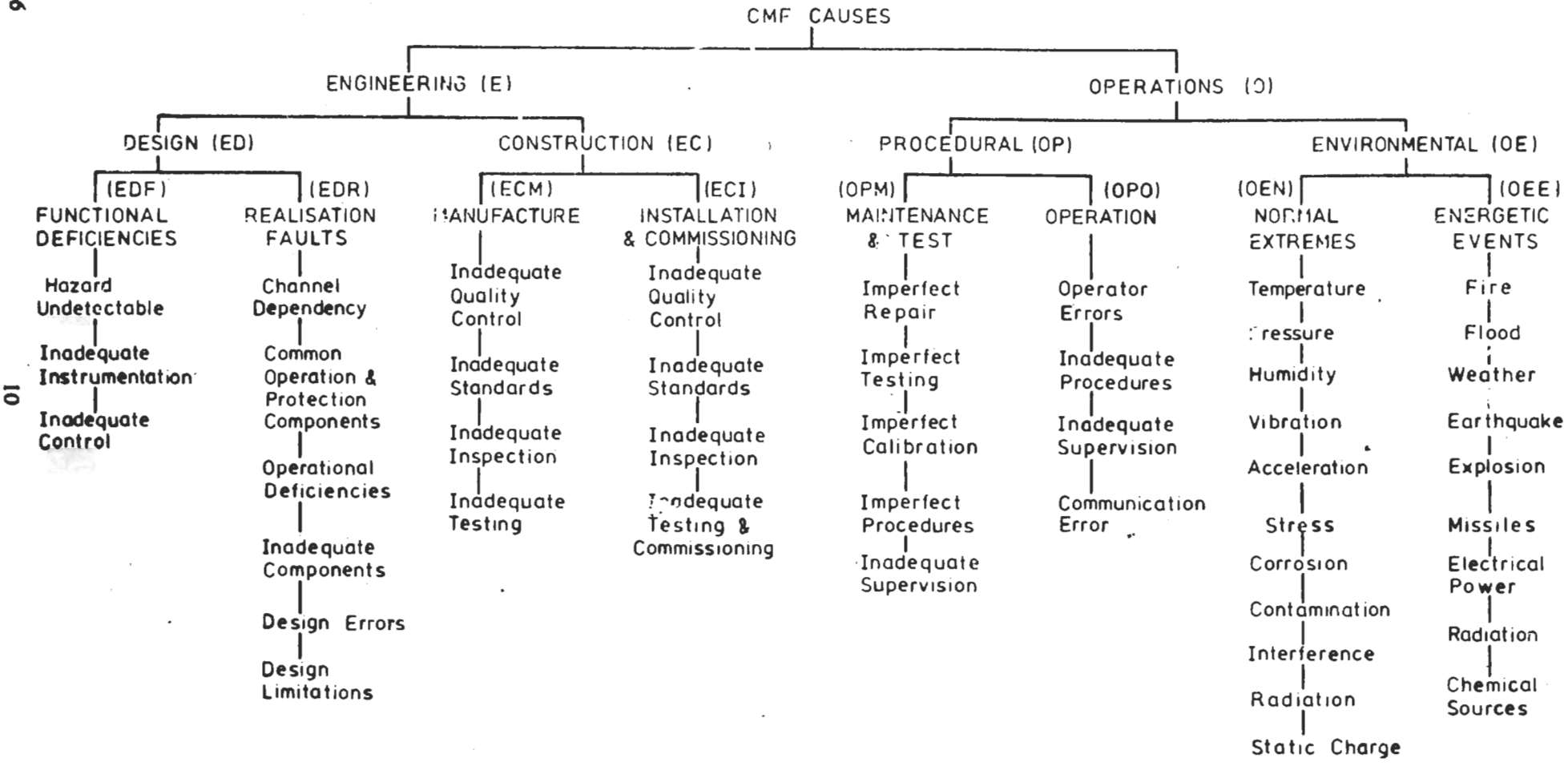


FIG 2 CLASSIFICATION SYSTEM FOR COMMON-MODE FAILURES

TABLE 1.1
Studies of Human Error in the CPI: Magnitude of the Human Error Problem

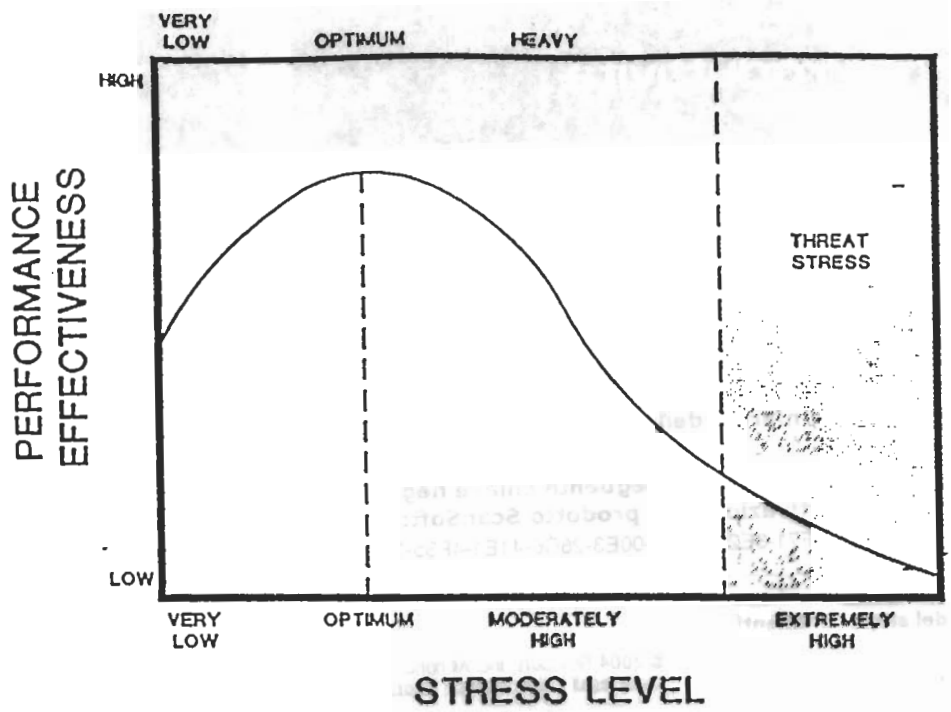
STUDY	RESULTS
Garrison (1989)	Human error accounted for $563 million of major chemical accidents up to 1984
Joshchek (1981)	80–90% of all accidents in the CPI due to human error
Rasmussen (1989)	Study of 190 accidents in CPI facility: Top 4 causes: • insufficient knowledge 34% • design errors 32% • procedure errors 24% • personnel errors 16%
Butikofer (1986)	Accidents in petrochemical and refinery units • equipment and design failures 41% • personnel and maintenance failures 41% • inadequate procedures 11% • inadequate inspection 5% • other 2%
Uehara and Hoosegow (1986)	Human error accounted for 58% of the fire accidents in refineries • improper management 12% • improper design 12% • improper materials 10% • misoperation 11% • improper inspection 19% • improper repair 9% • other errors 27%
Oil Insurance Association Report on Boiler Safety (1971)	Human error accounted for 73% and 67% of total damage for boiler start-up and on-line explosions, respectively.

tween different levels of management and the workforce, will have a major impact on the safety culture. The existence of clear policies that will ensure good quality procedures and training will also impact strongly on error likelihood.

The next level represents the organizational and plant design policies, which will also be influenced by senior management. The plant and corporate management policies will be implemented by line management. This level of management has a major impact on the conditions that influence error. Even if appropriate policies are adopted by senior management, these policies may be ineffective if they do not gain the support of line management. Factors that

In definitiva, l'uomo, nell'ambito dell'impianto, è un componente tutto particolare, cui sono assegnati molti compiti, normali (frequenti) o eccezionali (non frequenti). A differenza degli altri componenti fisici dell'impianto ha queste particolarità:

- è molto sensibile alle condizioni esterne;
- è un componente adattativo; in funzione delle condizioni e dell'esperienza tende a modificare il compito assegnatogli;
- svolge molte funzioni contemporaneamente, per cui può spostare l'attenzione da una funzione ad un'altra;
- è un'elaboratore di informazioni "olistico", cioè vede l'insieme, distingue forme (l'uomo è profondamente diverso, come elaboratore di informazioni, da un computer);
- in relazione alla ripetitività delle azioni e allo stato di stress agisce in base a procedure psicologiche basate sulle abilità memorizzate (skill-based), su regole programmate (rule-based) o sulla conoscenza (knowledge based).



Relationship of **Stress and Performance (based on Figure 17-1** in Reference 7)

Managers must recognize *that most PSFs (including many* ***internal PSFs) are within their control. By designing*** *work* ***situations*** *that are compatible* ***with human needs, capabilities, and limitations,*** *and* ***carefully*** *matching workers* ***with the job requirements, managers can create conditions*** *that* ***optimize*** *worker performance* ***and minimize*** *human errors.*

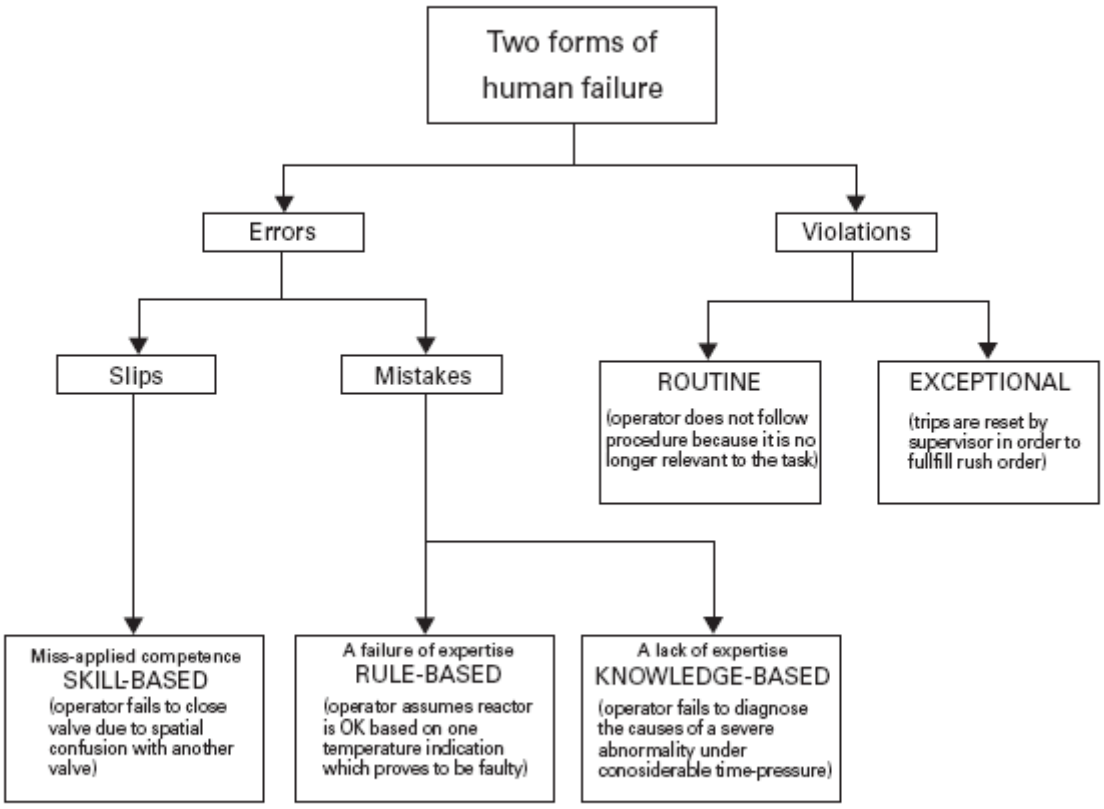


Figure 14.1: Reason, Classification of human errors.

Accident sequence risk analysis-based classification:

If a risk analysis is performed by using the accident sequence approach (initiating events, event trees and fault trees), a classification scheme can be used which is in accordance with this approach. In this approach an initiating event is defined as an event that creates a disturbance in the plant and has the potential to lead to undesired consequences, depending on the successful operation of the various safety systems. The following types of failures can be defined:

Pre-initiator failures: (Latent error)
Testing and maintenance actions prior to an initiating event

Human-induced initiators:
Actions which might cause initiating events

Post-initiator failures: (Dynamic operator action failure)
Emergency-procedure-driven actions taken to deal with and mitigate the consequences of accident sequences and actions which aggravate accident sequences

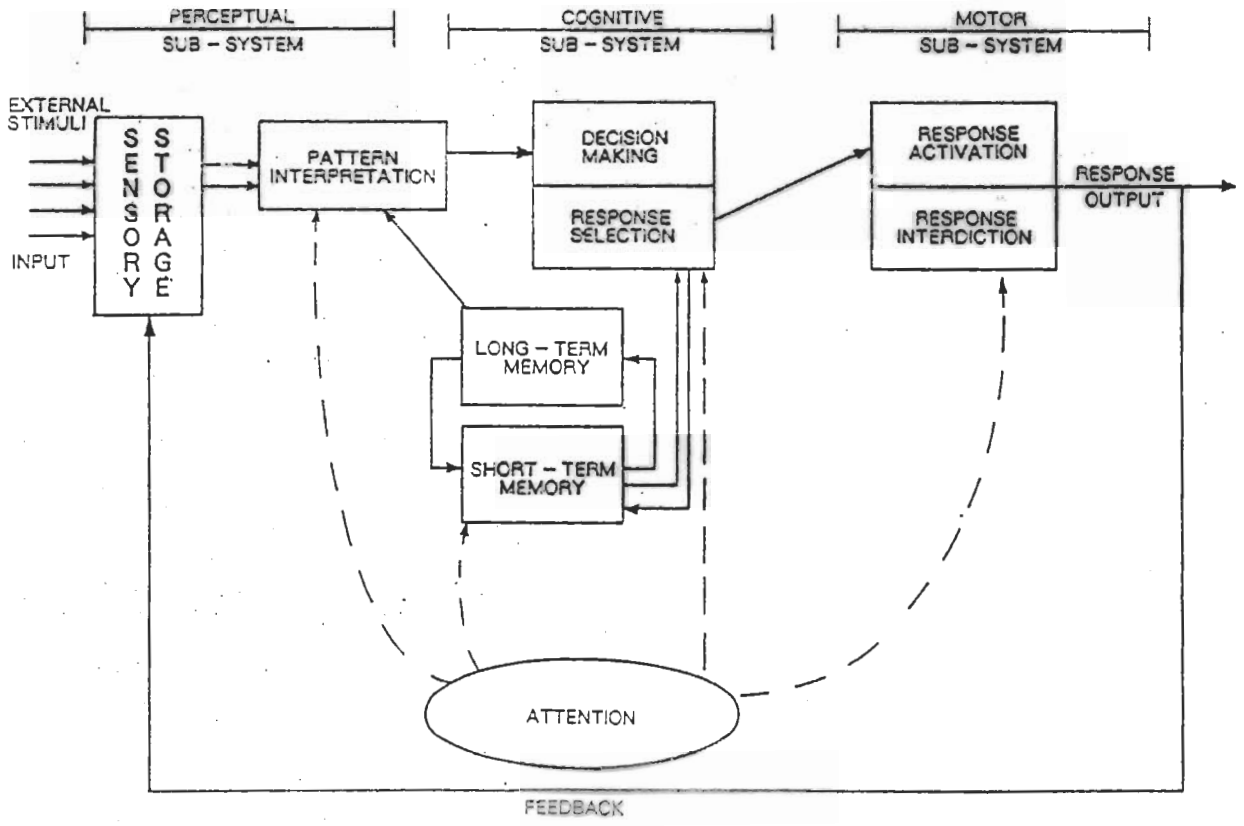
Recovery actions:
Actions to restore failed equipment by repair or by alternative equipment.

Organizational models are reviewed as a distinct category because of the importance of group processes in determining system performance.

6.1 Survey on Cognition/Action Modeling of the Individual

(1) Human Information Processing Framework

Figure 4 shows the general framework adopted for this project. Human information processing is divided into four main subsystems: perceptual, cognitive, motor, and attention. While there is vigorous theoretical debate about how each of these subsystems operate, almost all experimental psychologists agree that this general framework is highly satisfactory. This general framework allows us to organize many different models of specific kinds of human information processing into a coherent structure. Such a general structure is absolutely essential for planning a long-term program of research.



Total model

Figure 4. Human Information Processing

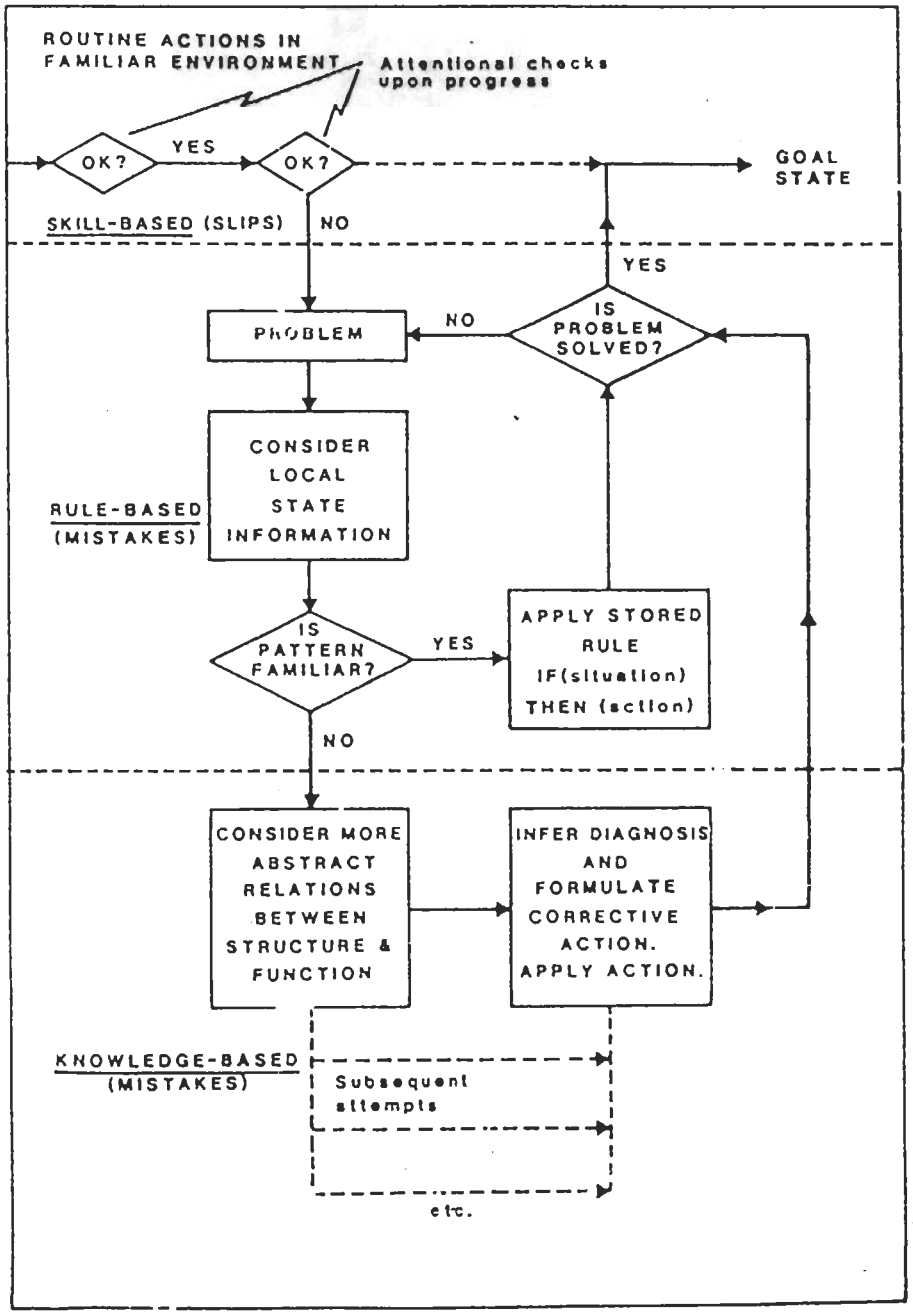


FIG. 1. Classification of human error types.

SAIC's HRA approach analyzes human actions occurring both before initiation of an accident and following the onset of an accident sequence. Figure 2 shows a breakdown of human events, how they are classified and which quantification methods are used. This classification is compatible with most PRA requirements. Slips can be errors of omission (e.g. omitting a step in a procedure) or errors of commission (e.g. mistakenly selecting a switch located adjacent to the intended switch). Errors of cognition are one kind of mistake, based on the classification proposed by Reason. Mistakes also include use of procedures or other rules that are inadequate; with older plants, these are not expected to be very significant compared with a new plant, for example.

elaborate schemes involving inspection and auditing to check for the achievement of certain safety objectives, which are rewarded with prizes.

The question of the effectiveness of motivational campaigns is not easy to answer. The obvious method would be to look at accident rates. However, recorded accident rates vary widely according to the propensity to report or not report events.

A safety campaign may only reduce the willingness of the workforce to report an accident rather than significantly reducing the underlying accident occurrences and hazards.

This is a problem that is not unique to motivational campaigns but is common to all approaches involving the monitoring of accidents or human error, as will be discussed in Chapter 6.

An indirect way to evaluate the effectiveness of safety campaigns is to look at some other observable "performance indicator" such as the use of personal protection equipment (PPE). Many campaigns are targeted at increasing the use of different types of PPE. Monitoring the results of such campaigns is done by establishing a baseline level of use of the equipment prior to the campaign and then looking at the percentage change in this use by the same workforce shortly after the campaign and then after some months have passed. Table 2.2 gives some summary results from a study by Pirani and Reynolds (1976) showing the effects of different types of motivational schemes on the use of PPE for head, hands, eyes, and feet. The first column shows the change from the baseline measurement 2 weeks after the campaign. The second column records the change from the baseline 4 months after the campaign.

In Table 2.2 the results from the use of posters and films are shown in the first three rows. Two points should be noted. First, all three measures show only short term gains. After four months the change in the pattern of use of

TABLE 2.2
Effect of Different Motivational Schemes on Use of PPE (adapted from Pirani and Reynolds, 1976)

MEASURE	PERCENT CHANGE AFTER 2 WEEKS	PERCENT CHANGE AFTER 4 MONTHS
General safety posters	+51%	+11%
Appropriate films	+40%	+11%
Fear posters	+18%	− 2%
Disciplinary measures	+39%	− 7%
Discussion + opinion leaders	+ 9%	+ 2%
Role playing	+71%	+68%

KNOWLEDGE-BASED MODE CONSCIOUS	SKILL-BASED MODE AUTOMATIC
Unskilled or occasional user	Skilled, regular user
Novel environment	Familiar environment
Slow	Fast
Effortful	Effortless
Requires considerable feedback	Requires little feedback
Causes of error: • Overload • Manual variability • Lack of knowledge of modes of use • Lack of awareness of consequences	Causes of error: • Strong habit intrusions • Frequently invoked rule used inappropriately • Changes in the situation do not trigger the need to change habits

FIGURE 2.3. **Modes of Interacting with the World (Reason, 1990).**

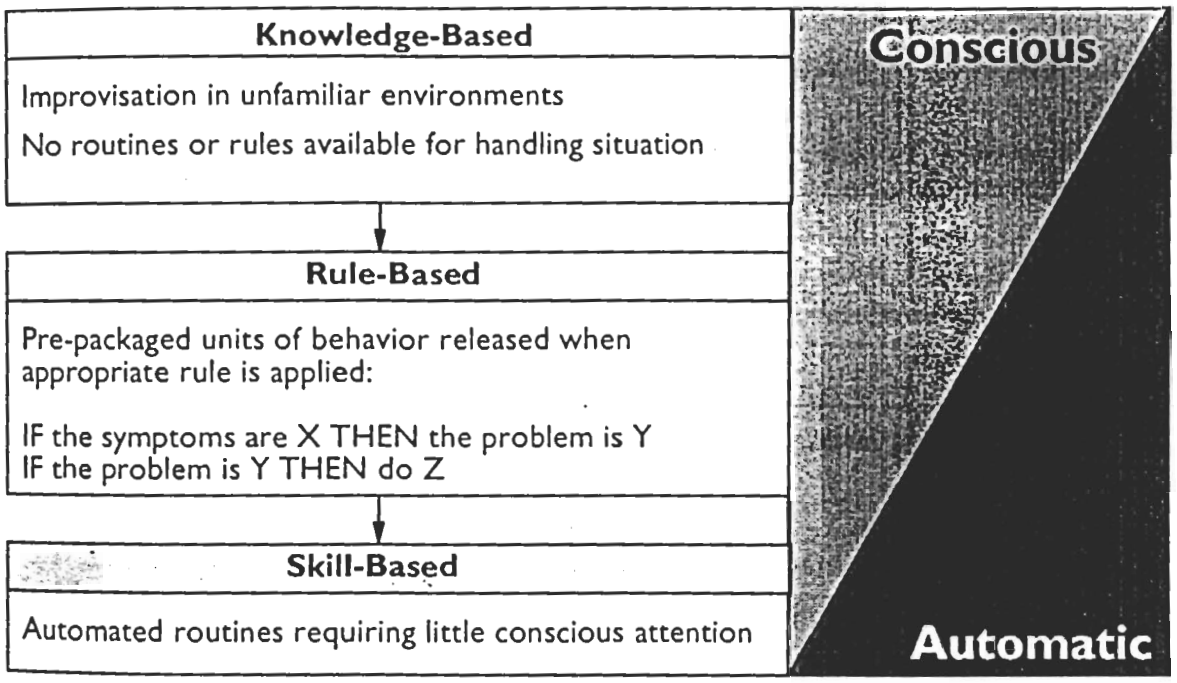


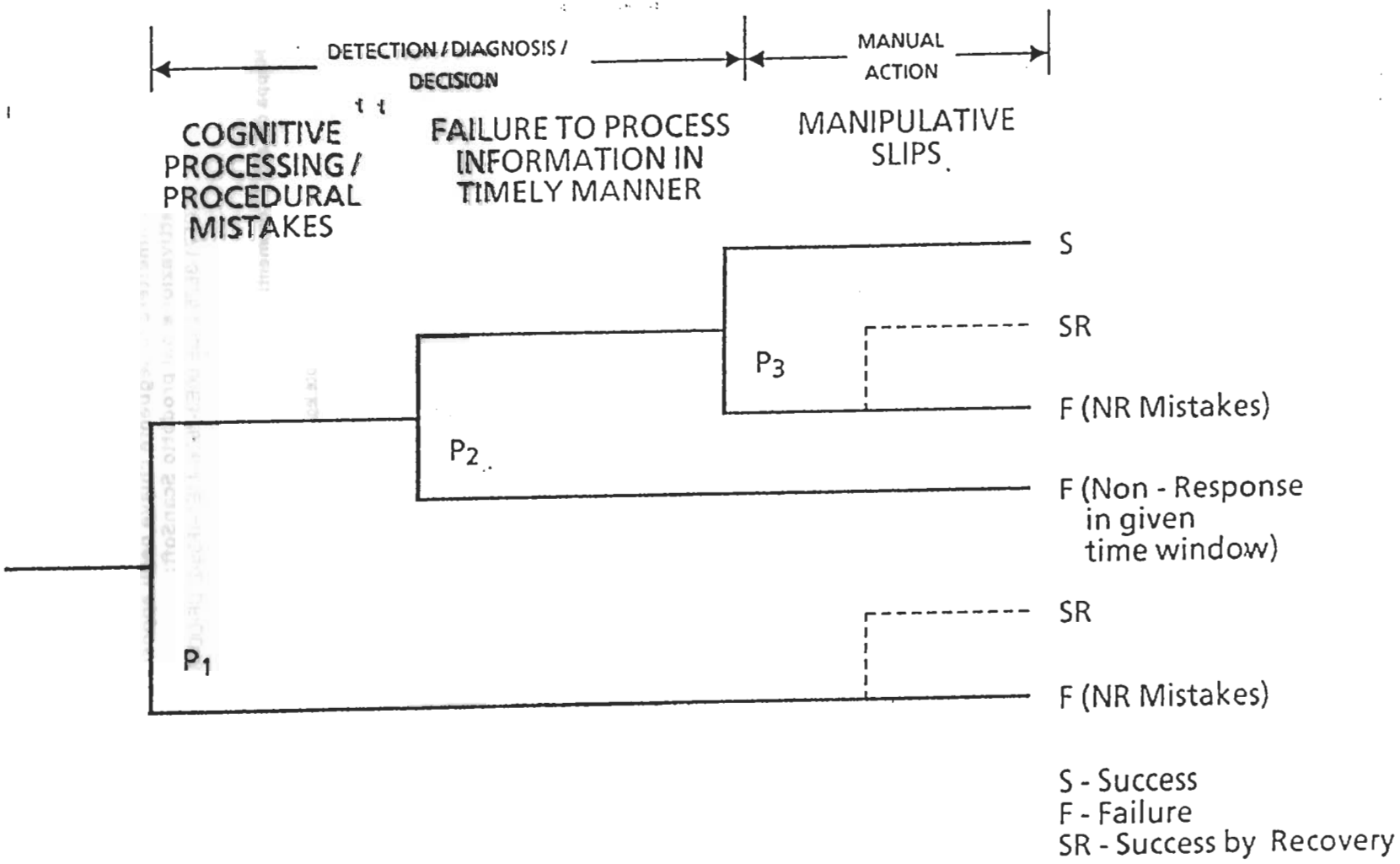
FIGURE 2.4. **The Continuum between Conscious and Automatic Behavior (based on Reason, 1990).**

determine the nature of the problem. This may involve gathering information from various sources such as dials, chart recorders and VDU screens, which is then used as input to a diagnostic rule of the following form:

<IF> symptoms are X <THEN> cause of the problem is Y

TIPI DI ERRORI UMANI

- **errori random**: corrispondono alla naturale fluttuazione di prestazioni dell'uomo di fronte ad azioni ripetute;
- **errori sistematici**: possono appartenere alle due categorie prima indicate, cioè possono essere dovuti ad una errata progettazione dell'interfaccia uomo-macchina o possono essere dovuti ad un comportamento errato, dovuto per esempio alla "selettività" dell'uomo, alla sua tendenza a farsi un proprio "modello di impianto" ed in particolare a ipotizzare situazioni già sperimentate (stereotipi), ecc.;
- **errori sporadici**: sono legati alla grande variabilità del comportamento umano; sono eccezionali e per la loro natura poco trattabili.



General Action Tree Representation of Type C Actions

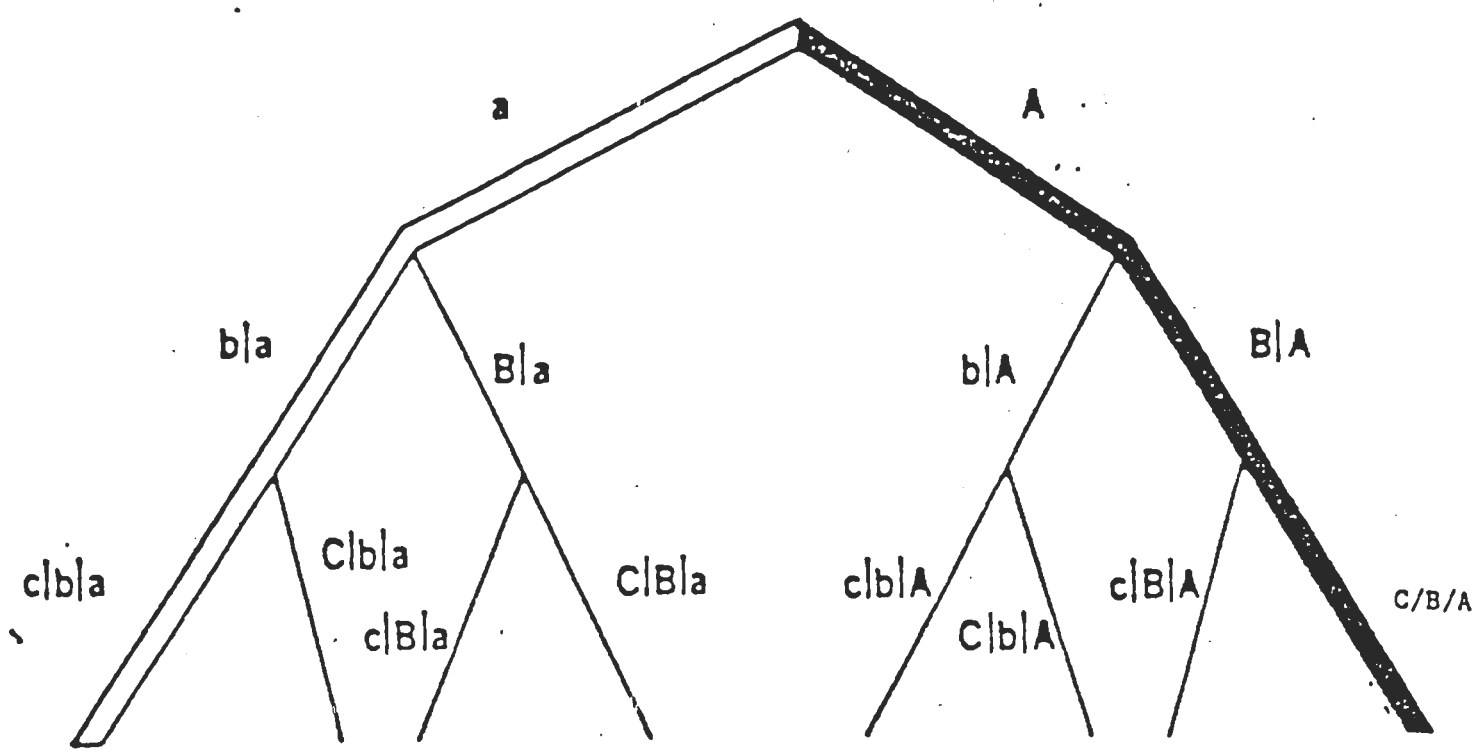
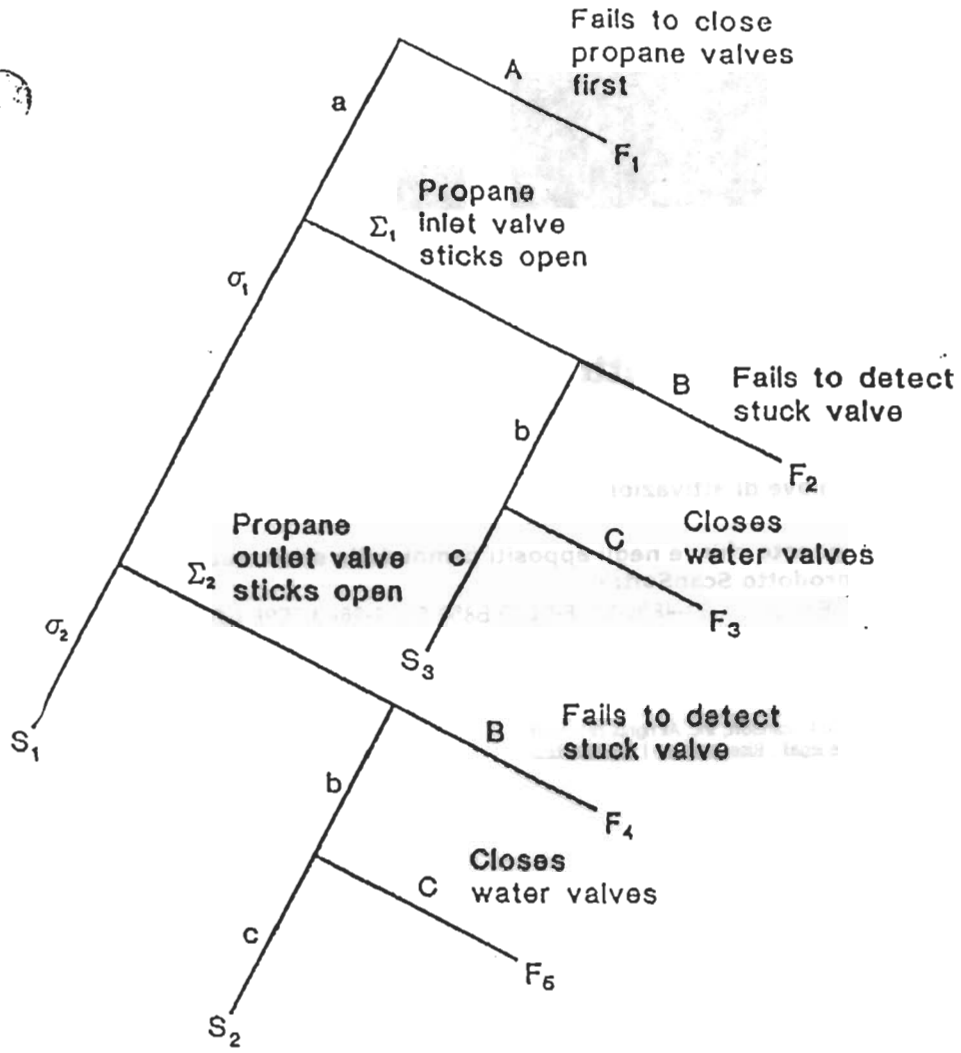


Fig.3.11.a – Albero delle probabilità mostrante cammini di completo successo (doppia linea) e di completo insuccesso (linea solida)

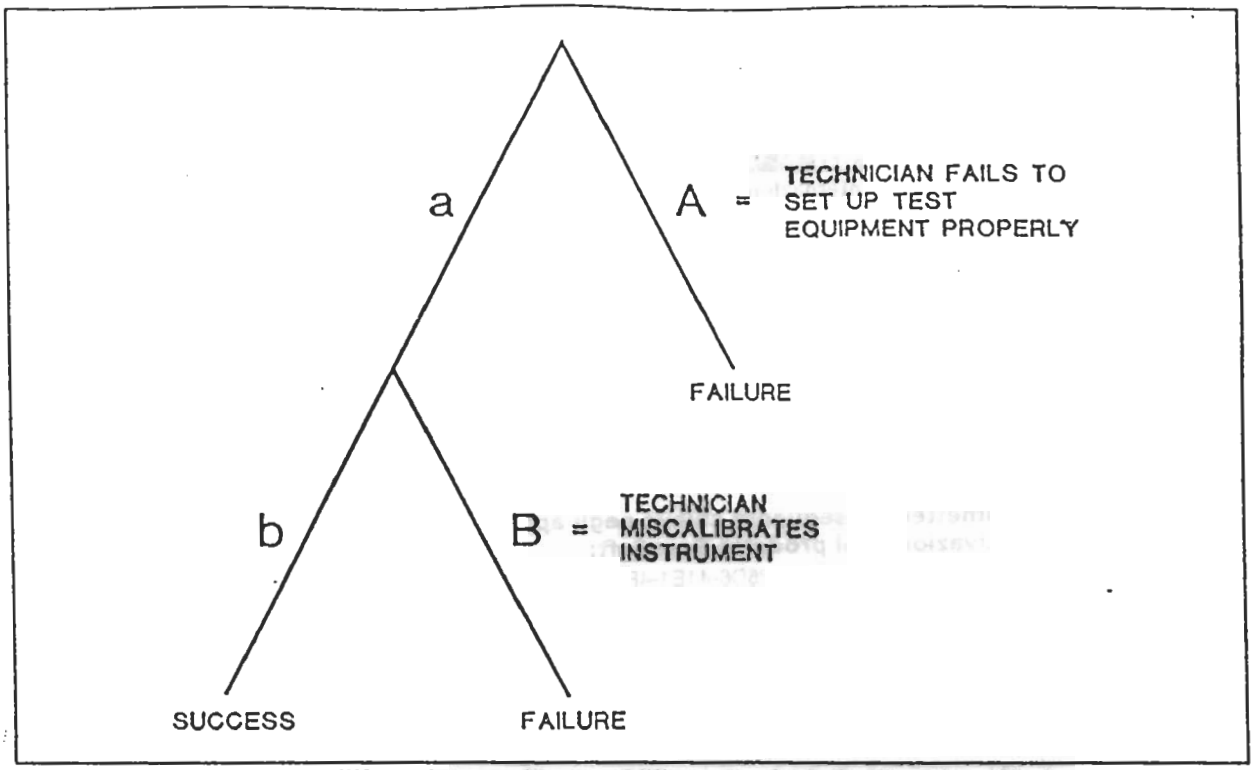


HRA Event Tree for Improper Condenser Isolation

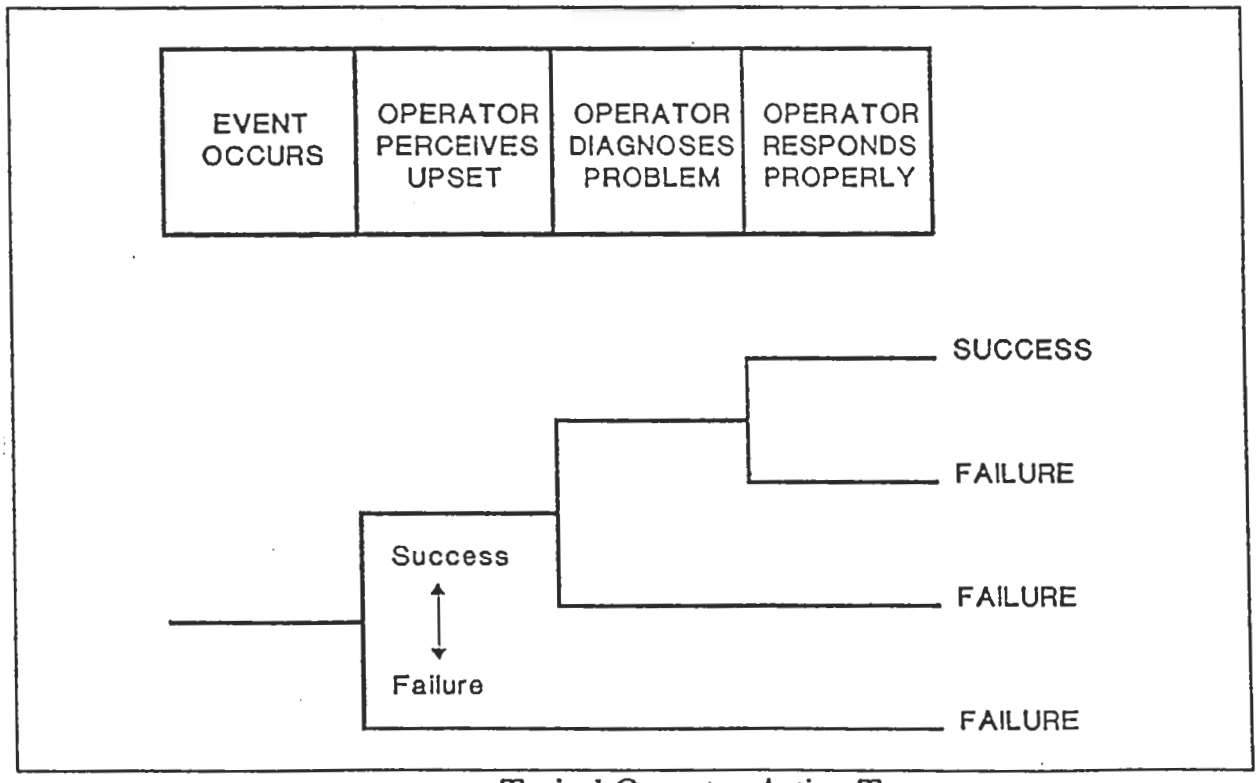
Failure Symbol	Failure Description	Estimated Probability	Data Source
A	Operator fails to close the propane valves first	0.05	T20-7 #5 footnote x 5, per T20-16 #6a
Σ_1	Propane inlet valve sticks open	0.001	T20-14 footnote
Σ_2	Propane outlet valve sticks open	0.001	T20-14 footnote
B	Operator fails to detect a stuck valve	0.025	T20-14 #3 x 5, per T20-16 #6a
C	Operator chooses to close the cooling water valves to stop the propane release	0.25	T20-16 #7a

HRA Results

$F_1 = A$	$= 5.0 \times 10^{-2}$
$F_2 = a\Sigma_1 B$	$= 2.4 \times 10^{-5}$
$F_3 = a\Sigma_1 bC$	$= 2.3 \times 10^{-4}$
$F_4 = a\sigma_1\Sigma_2 B$	$= 2.4 \times 10^{-5}$
$F_5 = a\sigma_1\Sigma_2 bC$	$= 2.3 \times 10^{-4}$
$F_T = F_1 + ... + F_5$	≈ 0.05



HRA Event Tree of Hypothetical Calibration Tasks



Typical Operator Action Tree

Il campo di dipendenza è variabile con continuità; per ragioni pratiche, esso è reso usualmente discretizzato e diviso in 5 parti uguali: completamente indipendenti, a bassa, media, alta dipendenza ed infine completamente dipendenti. Indicando con p_x la probabilità di errore umano in una certa incombenza (operazione x), si ammette che la probabilità p_{X+1} che fallisca anche la successiva operazione sia:

$p_{X+1} = p_X$ in caso di assoluta indipendenza

$p_{X+1} = \frac{1+3p_X}{4}$ in caso di bassa dipendenza

$p_{X+1} = \frac{2+2p_X}{4}$ in caso di media dipendenza

$p_{X+1} = \frac{3+p_X}{4}$ in caso di alta dipendenza

$p_{X+1} = 1$ in caso di assoluta indipendenza

DESCRIZIONE EVENTO	I
OPERATORE NON SEGUE LE ISTRUZIONI RICEVUTE	5E-2
ERRORE DI LETTURA STRUMENTO	5E-3
OMISSIONE DI AZIONE PREVISTA DALLE PROCEDURE	2E-3
OMISSIONE DI AZIONE NON PREVISTA ESPLICITAMENTE DALLE PROCEDURE	1E-2
ERRORE DI CONNESSIONE PARTI MOBILI	3E-3
ERRORE DI CALCOLO ARITMETICO	3E-2
ERRORE IN AZIONE MANUALE	5E-3
ALLARME ACUSTICO E VISIVO IGNORATO	3E-4
INTERVENTO MANUALE OPERATORE, SENZA INDICAZIONI, ALLARMI E TELECOMANDI	1E-1
INTERVENTO MANUALE OPERATORE, CON INDICAZIONI, SENZA ALLARMI E TELECOMANDI	5E-2
INTERVENTO MANUALE OPERATORE, CON INDICAZIONI E ALLARMI, SENZA TELECOMANDI	1E-2
INTERVENTO MANUALE OPERATORE, CON INDICAZIONI, ALLARMI E TELECOMANDI	1E-3

Tab. 3.1 - Dati sulla probabilità di errore umano (ripresi dal Manuale di Dossier Ambiente citato nel testo)

MODELLO TESEO

(Tecnica Empirica per la Stima degli Errori Operatori) per operatori in sala di controllo di un impianto chimico) (Bello e Colombari 1980)

La probabilità di insuccesso (a causa dell. operatore Poper è:

$$P_{oper} = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5$$

K1 tipo di attività

K2 tempo a disposizione per l'operazione
K3 caratteristiche comportamentali dell'operatore
K4 stato emozionale
K5 caratteristiche ergonometriche dell'ambiente di lavoro.

I valori numerici forniti da Pello sono riportati nella Tav. 10.5.

Si noti che la probabilità di insuccesso passa da un valore del tutto trascurabile nelle condizioni migliori tabulate ad un valore prossimo al 100% nelle condizioni peggiori.

L'applicazione della espressione, che fornisce solo un ordine di grandezza, è immediata.

Per esempio se operatore debba inserire un fluido inibitore entro 45 secondi dall'istante in cui la temperatura raggiunge i

Tav. 10.5 - FATTORI DEL MODELLO TESEO

Fattore	Caratteristica		Valore numerico
K1: tipo d'attività	routine semplice		0,001
	routine complessa		0,01
	non routine		0,1
K2: tempo a disposizione	routine	20 s o più	0,5
		10 s	1
		2 s	10
	non routine	60 s o più	0,1
		45 s	0,3
		30 s	1
		3 s	10
K3: caratteristiche operatore	molto esperto		0,5
	mediamente esperto		1
	poco esperto		3
K4: situazione operativa	normale		1
	potenzialmente di emergenza		2
	di emergenza		3
K5: condizioni ambientali	ottime		0,7
	buone		1
	discrete		3
	cattive		7
	pessime		11

400°C, se la pressi
damento non è su
La situazione è
L'operatore ha
(K3 = 1), l'ambi
strumentazione a
In relazione al ti
tempo a disposizi
probabilità di insu
Per migliorare la
una migliore strum
leggibile più facil
acustico e visivo);
tempo a disposizio
è meglio selezionat
probabilità d'insuc
di grandezza.

10.8 Ridondanza s

La ridondanza se
vantaggi.
Nella Fig. 10.5 m
sistemi con unità
ridondanze (vedi
L'andamento de
due in parallelo co
della Sez. 7.
È stato messo i
risulta del tutto fi
(detta *causa comu*
parallelo (Bourne e
possono essere:
– condizioni am
umidità, vibrazione
– eventi eccezio
allagamento, sabo
– guasti a rete d

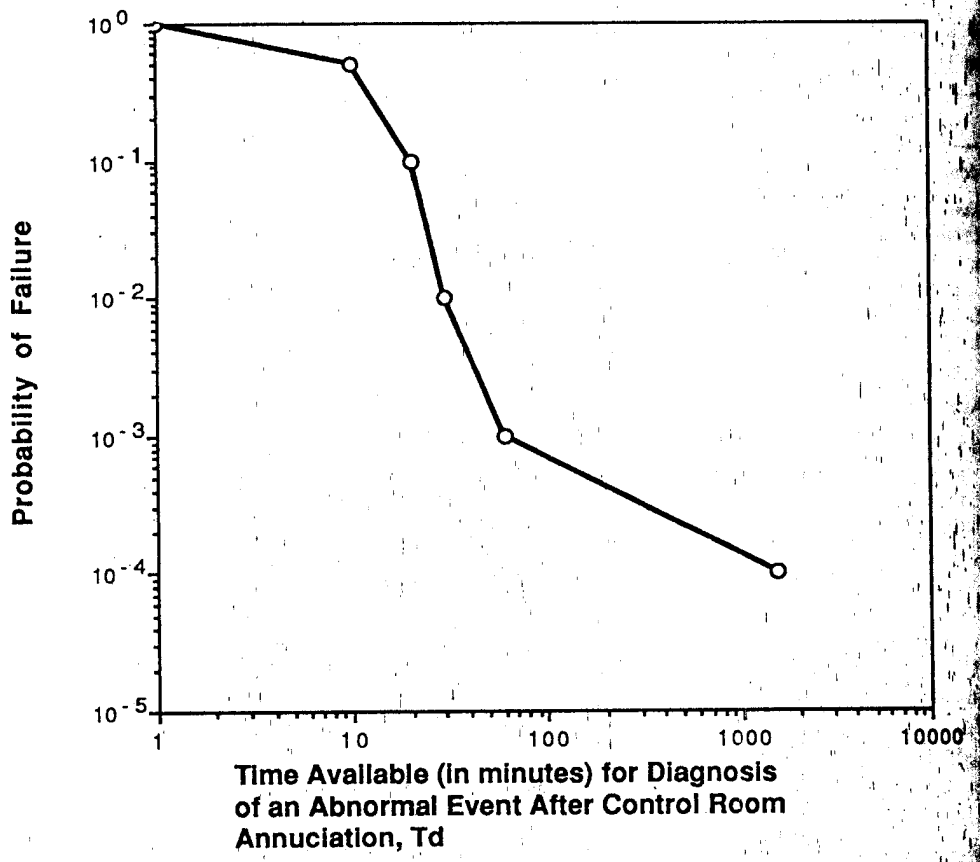


Figure 3.18. Probability of failure by control room personnel to correctly diagnose an abnormal event.

$T_d = T_m - T_a$

where T_d = time available for control room operators to diagnose that an abnormal event has occurred
T_m = the maximum time available to correctly diagnose that an abnormal event has occurred and to have completed all corrective actions necessary to prevent the resulting incident
T_a = the time required to complete all post-diagnosis required actions to bring the system under control

The maximum time to diagnose and correct a problem (T_m) must be determined by a detailed analysis of each accident sequence. An analysis of the time delays created by such factors as the rate of heat transfer, chemical reaction kinetics, or flow rates may be required. This analysis normally requires process engineering support.

The time required to correct the problem (T_a) is next determined. A list is made of the operator tasks that must be completed to correct the problem created in each accident sequence. The times required to complete each of the operator tasks (including travel time) are determined using Table 3.10. For each