Design, Human Factors and Safety

Thomas B. Sheridan, ScD
Massachusetts Institute of Technology

Definitions

DESIGN - is the synthesis of a means to serve a human need
- is an art that makes use of science and technology

ERROR - is an unwanted, unwonted exchange of energy

RISK of an event - is some function of undesired consequences that might occur and the probability of their occurrence. Two common definitions of risk are:

- (consequences x probability) = expected value, and
- (worst possible outcome)

but risk could be defined in more complex ways

SAFETY - is *acceptable risk*

The Usual Steps in System Design

1. Problem identification, based on
- errors
- inefficiencies
- complaints

2. Task analysis
- observation
- analysis of mental workload
- interviews and focus groups
- activity recording
- analysis of information flows and situation awareness
- simulations

3. Mathematical modeling
- statistical models
- dynamic models
- decision theoretical models
- event trees
- logic trees
- cause-consequence models

4. Detailed design/redesign, with help of all actors involved

5. Controlled experiments and simulations to refine and validate

6. Pilot testing in-situ

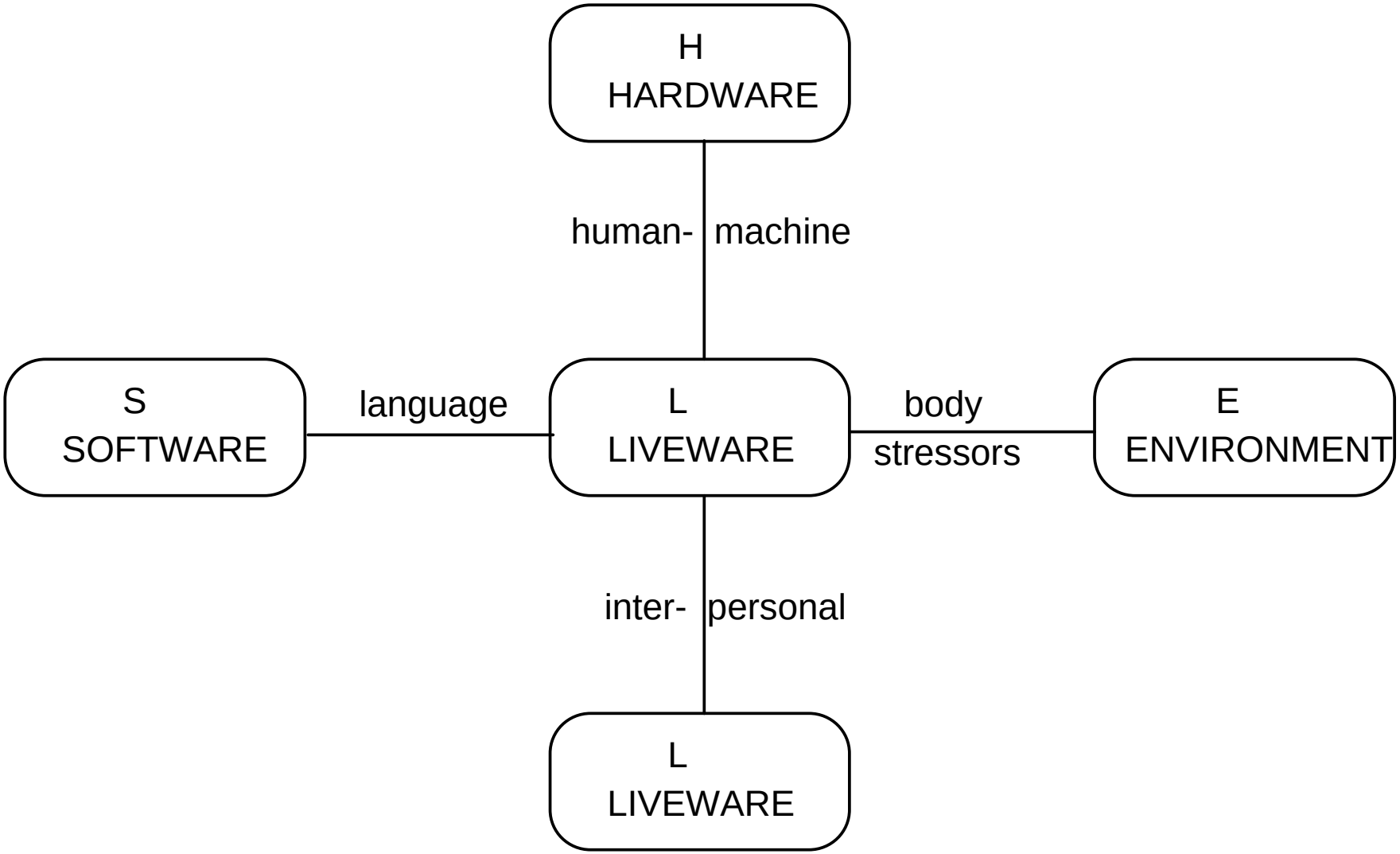
What is Human Factors Engineering?

Psychology and systems engineering disciplines applied to human tasks and human-system interaction :

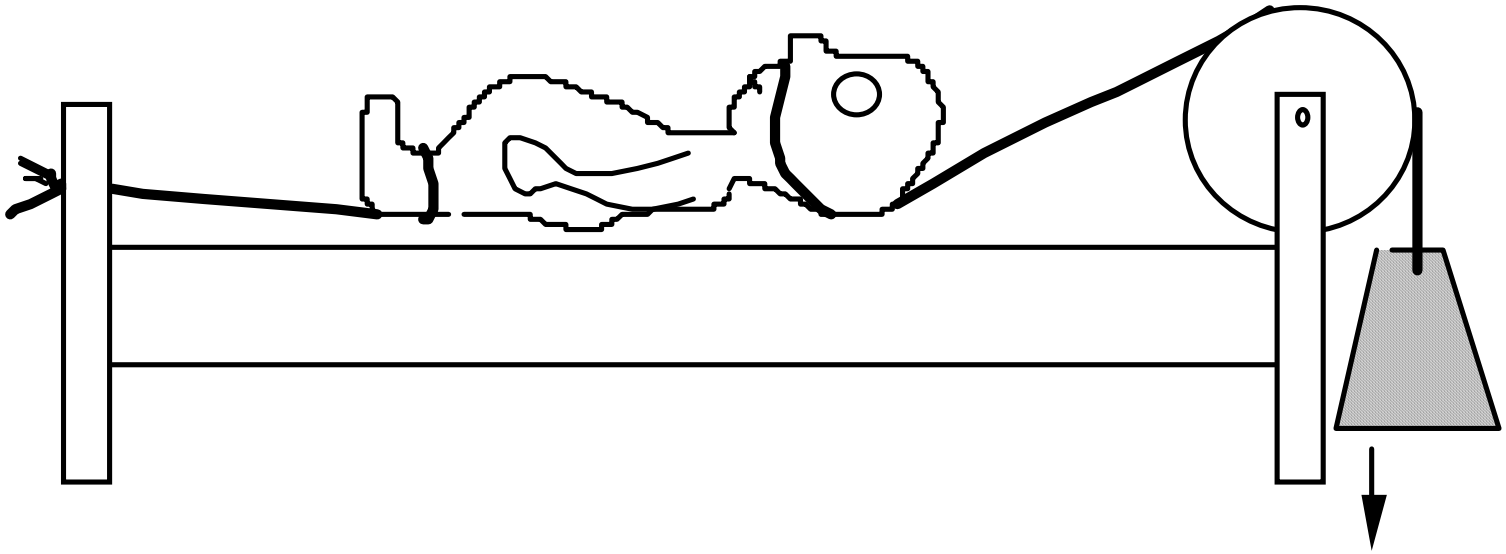
to
- understand error causation, inefficiency
- redesign physical environment, technology
- redesign task and administrative procedures
- improve training

(The subset of HFE called ergonomics, which is biomechanics and physiology applied to spatial arrangements and physical work, is of diminishing importance as automation takes over physical work and human tasks become more cognitive.)

SHEL MODEL OF HUMAN INTERFACES

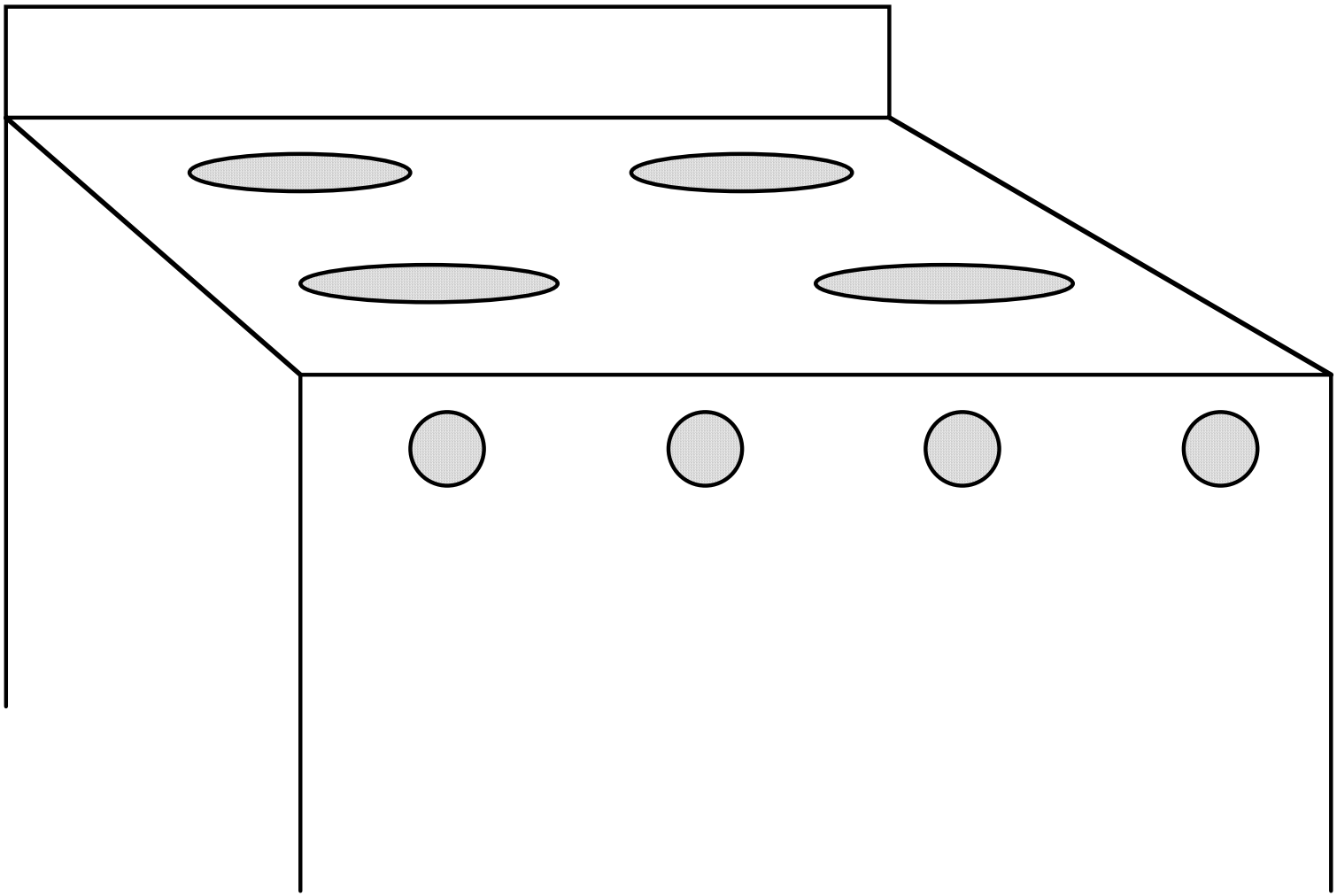


The Procrustean bed:
forcing the human to fit the technology

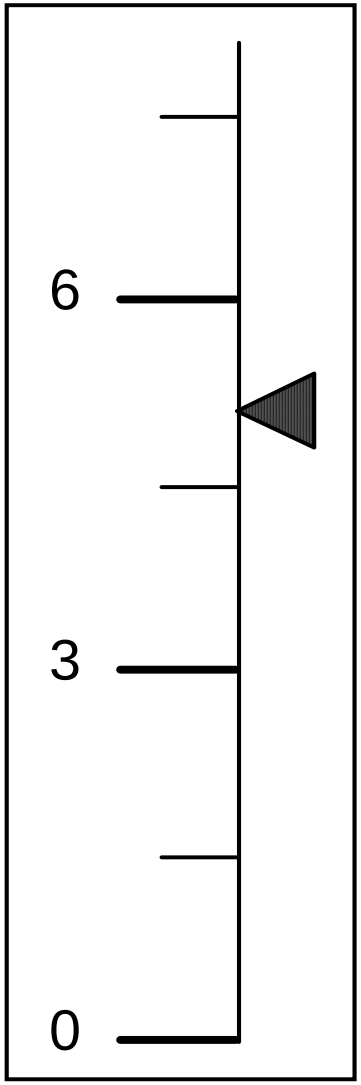


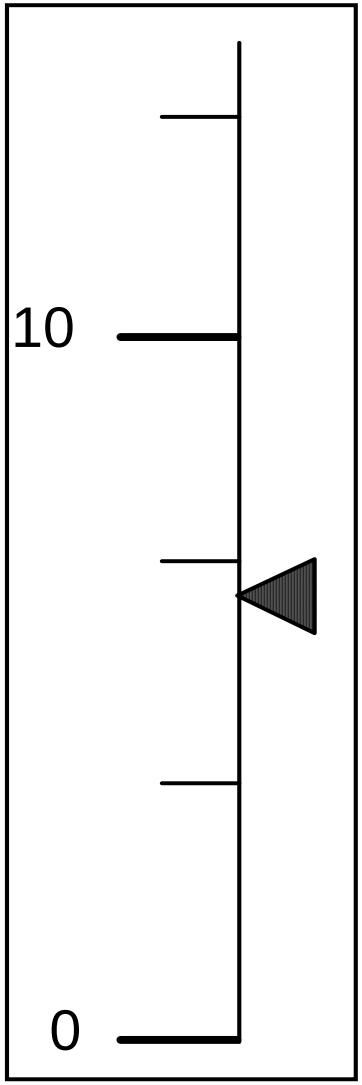
DISPLAY-CONTROL COMPATIBILITY

(E.G., THE STOVE BURNER CONTROL PROBLEM)

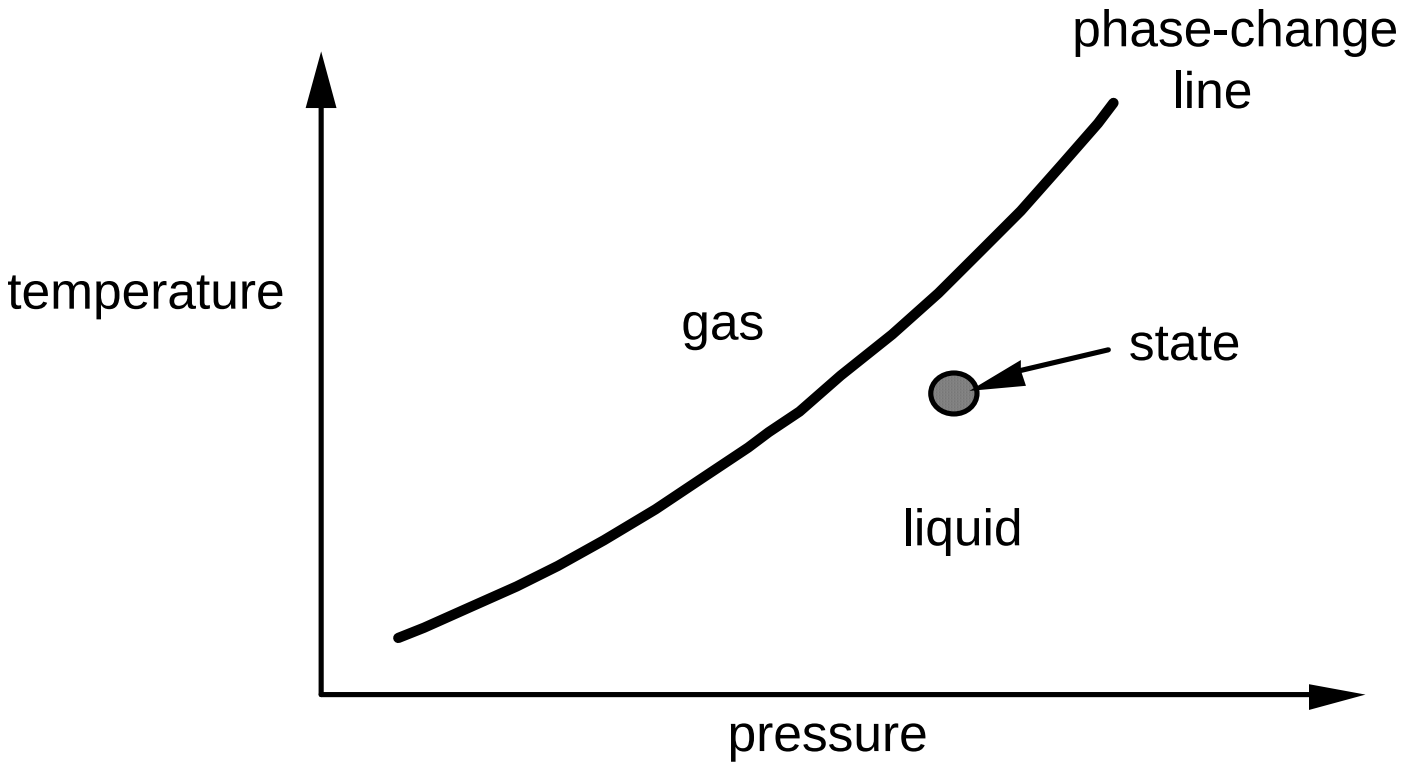


DESIGN OF SCALES AND NUMBERING

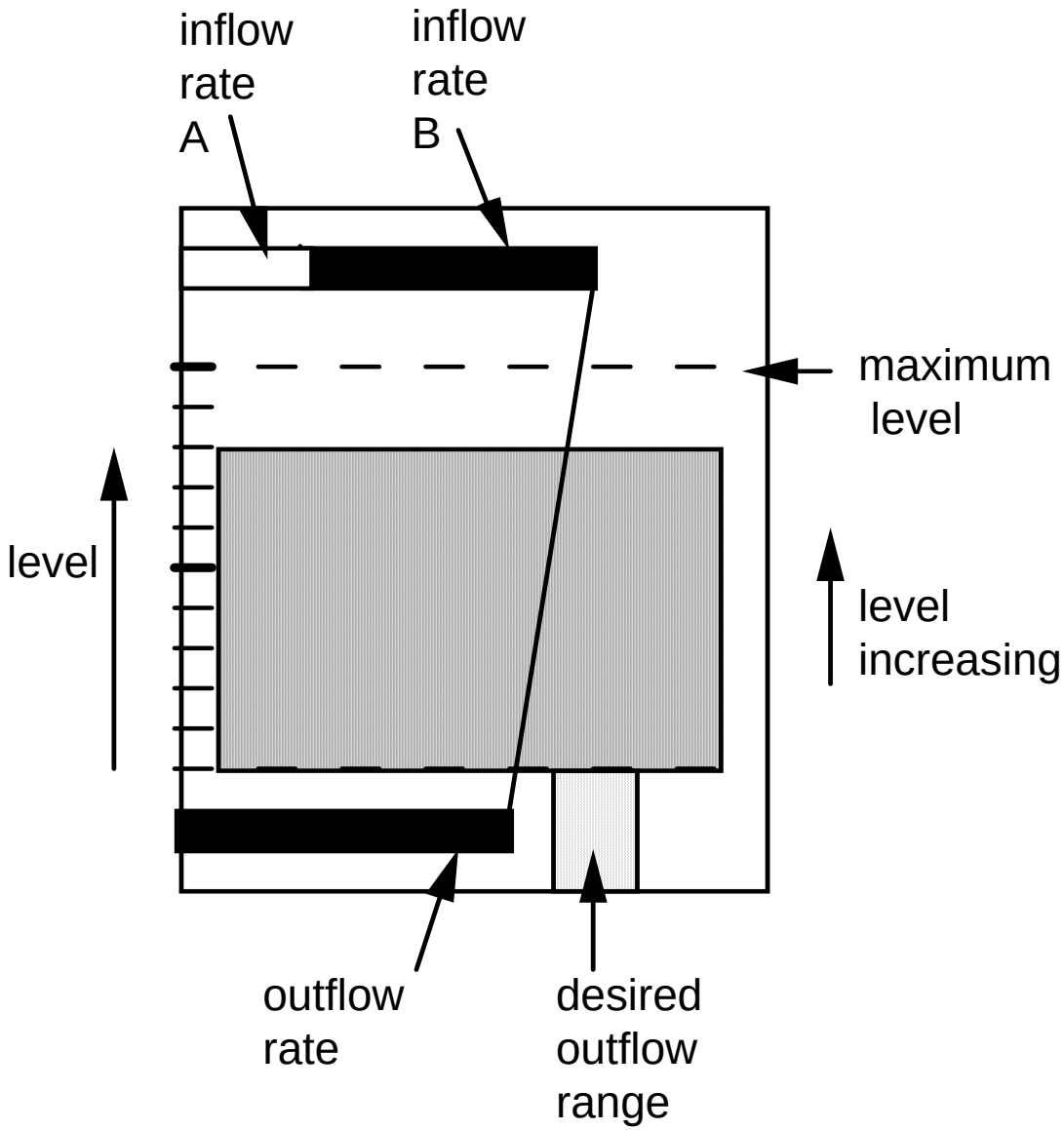




Combining two related variables into one integrated display



Ecological display in process control



Temporal Analysis of Nurse Tasks (in Surgical Procedure)

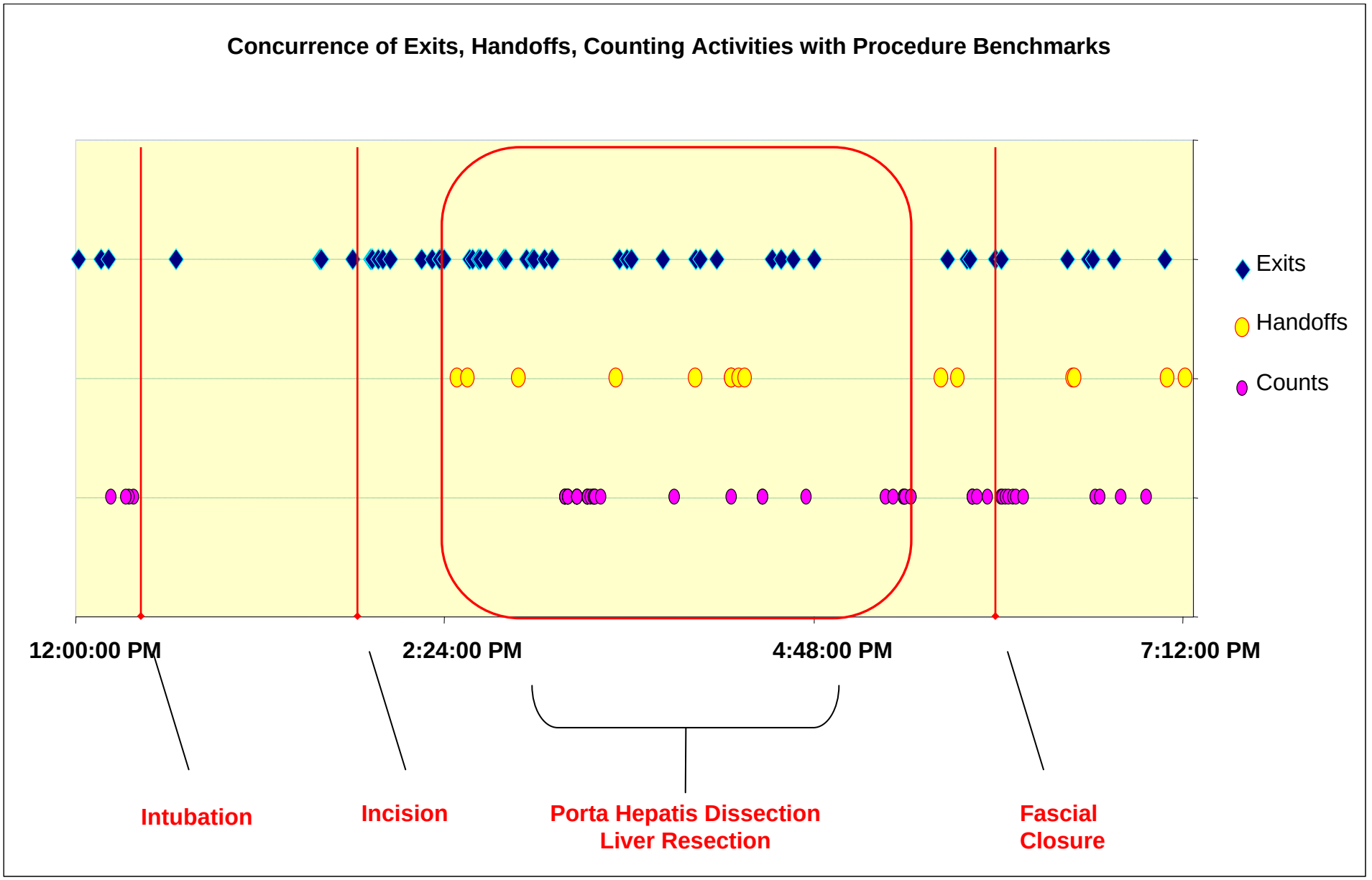
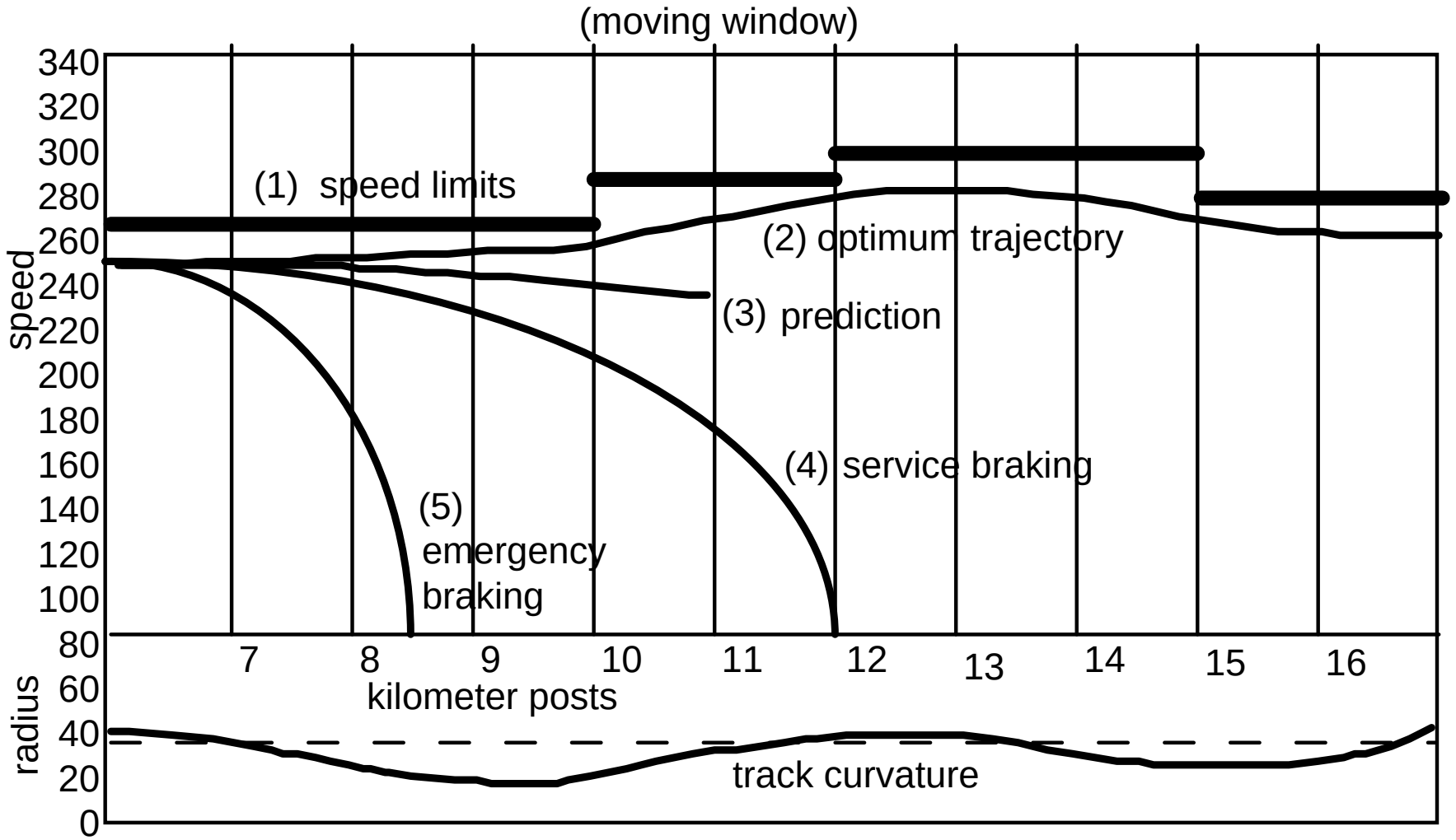


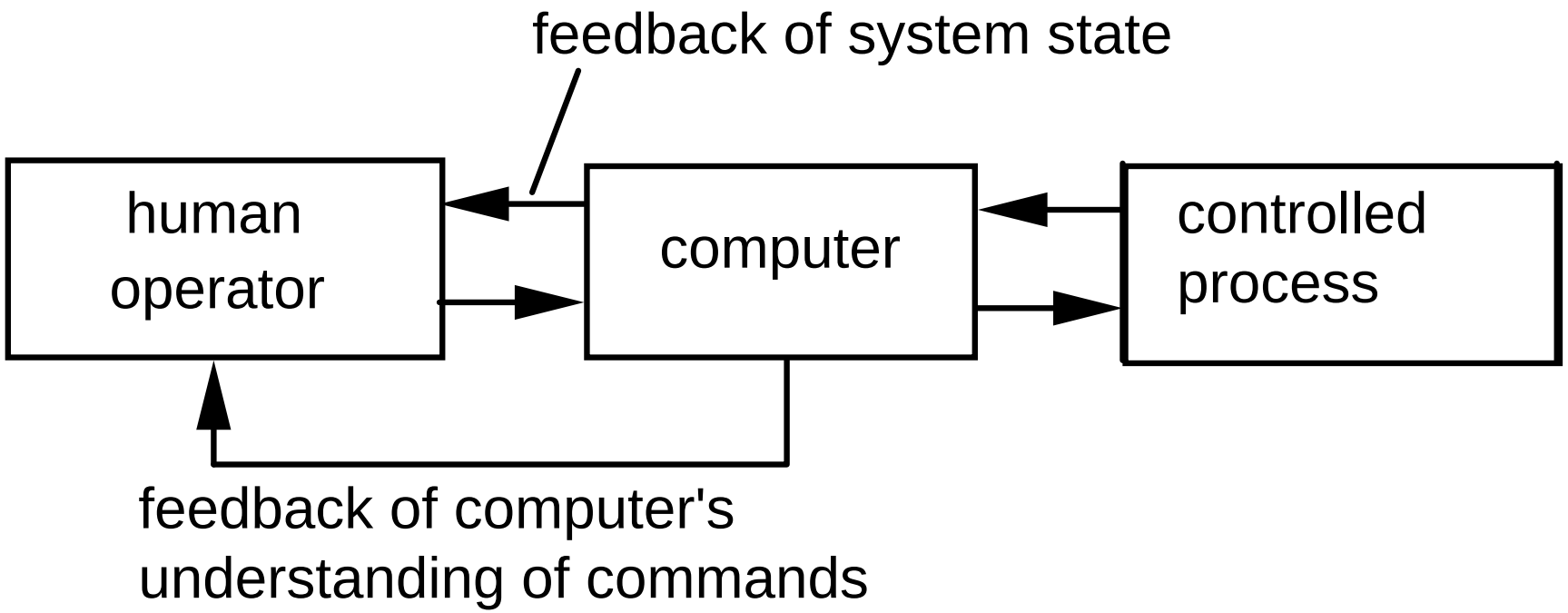
Table 3: Safety Compromising Events and Contributing and Compensatory Factors

Event	Contributing Factors*												Compensatory Factors*					Event Detection**		
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	ND	Self	Other
Wound dehiscence	♦								♦											✓
Intra-operative tissue injury requiring surgical revision # 1	♦								♦	♦									✓	
Intra-operative tissue injury requiring surgical revision # 2	♦								♦	♦									✓	
Medication administration error # 1				♦		♦	♦					♦						✓		
Medication administration error # 2				♦			♦	♦					⊕						✓	
Adverse drug reaction	♦		♦					♦							⊕	⊕	⊕		✓	
Wound contamination # 1			♦	♦	♦													✓		
Wound contamination # 2			♦	♦	♦									⊕					✓	
Hypothermia											♦	♦			⊕	⊕	⊕			✓
Inadequate pre-operative preparation		♦											⊕	⊕					✓	
Near-injury to inexperienced assistant					♦								⊕						✓	

Predictor display (for train)



Supervisory control

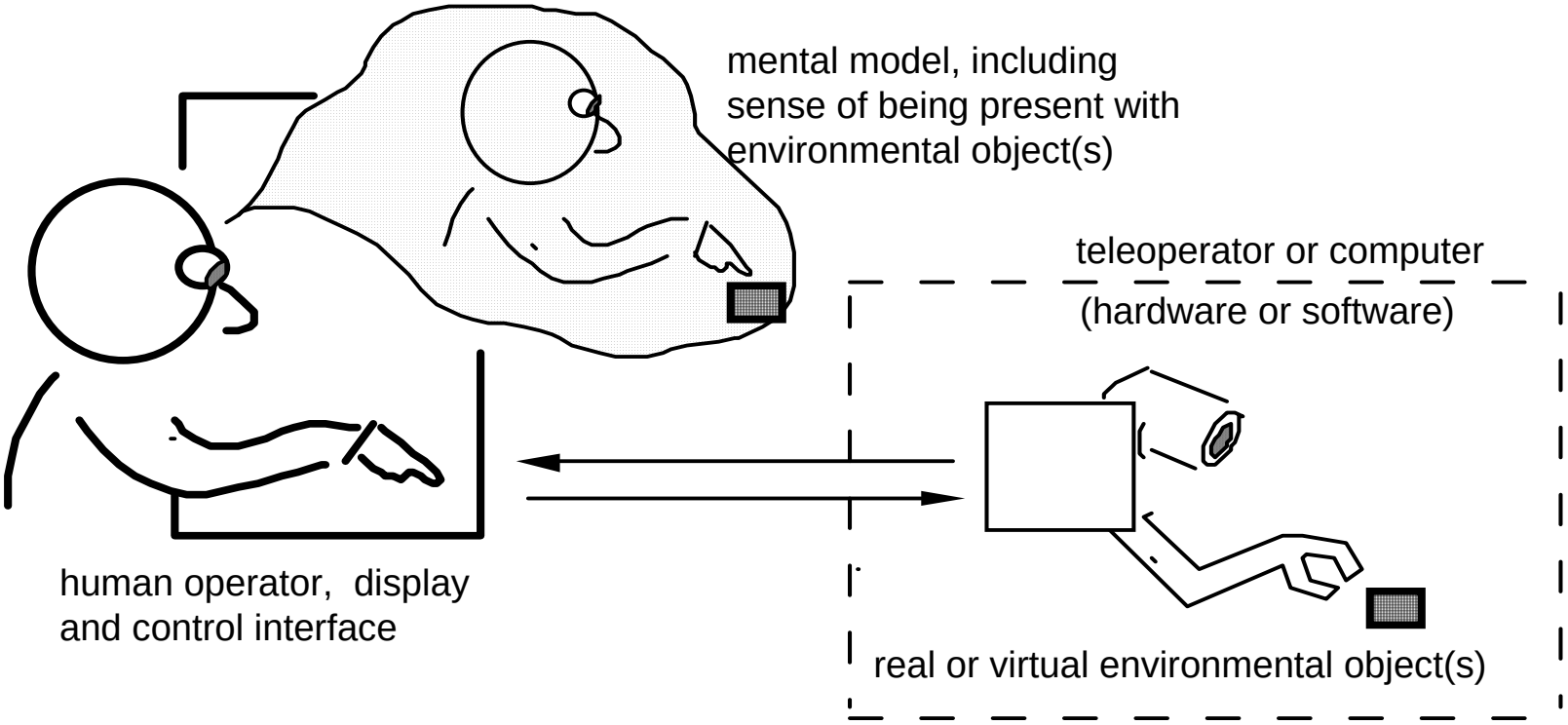


Levels of automation

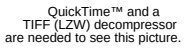
Table 1. A Scale of Degrees of Automation

1.	The computer offers no assistance; the human must do it all.
2.	The computer suggests alternative ways to do the task.
3.	The computer selects one way to do the task and
4.	executes that suggestion if the human approves, or
5.	allows the human a restricted time to veto before automatic execution, or
6.	executes the suggestion automatically, then necessarily informs the human, or
7.	executes the suggestion automatically, then informs the human only if asked.
8.	The computer selects the method, executes the task, and ignores the human.

Telepresence (e.g, in materials handling)



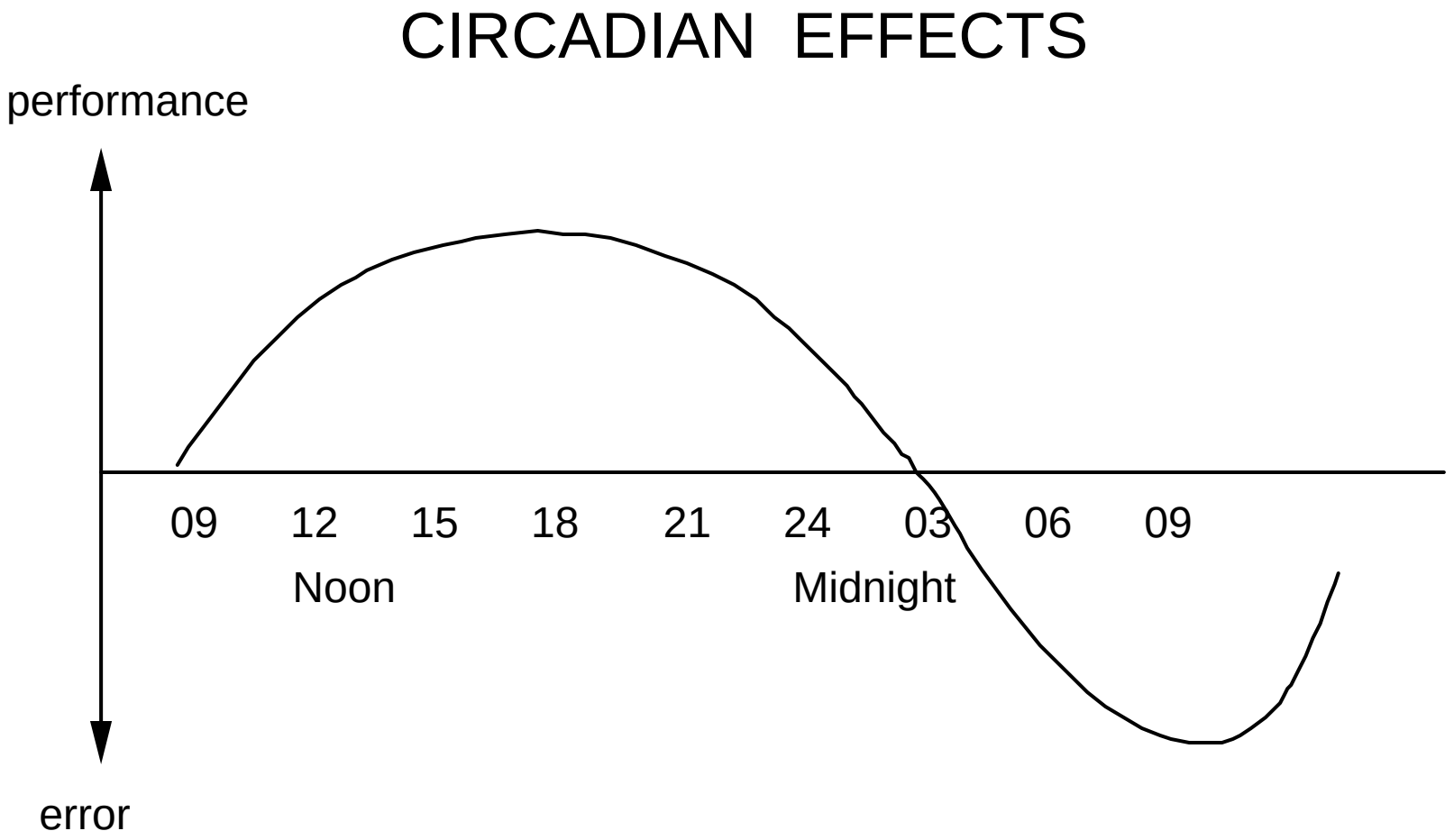
Reason’s model of an accident: penetration of multiple barriers



SOME CAUSES OF HUMAN ERROR

- Lack of feedback
- Capture
- Invalid mental models
- Wrong track of hypothesis verification
- Stress and perceptual narrowing
- Risk homeostasis
- State of the nervous system

Shift work: fitness for duty



ERROR THERAPIES

- Design for ease of use
- Education and training
- Prevention or inhibition of exposure
- Computer-based decision aids
- Alarms
- Posted warnings

Metaphor of Organizational Resilience

to unpredictable incidents and anomolous events