Design for Error Tolerance

Rasmussen, Jens

Published in:
American Nuclear Society. Transactions

Publication date:
1983

Document Version
Peer reviewed version

American Nuclear Society. Transactions, Vol. 45,
October-November, 1983. pp 358-59

DESIGN FOR ERROR TOLERANCE

Jens Rasmussen
Riso National Laboratory, DK 4000 Roskilde, Denmark

An important aspect of the optimal design of computer-based operator support systems is the sensitivity of such systems to operator errors.

Faults and errors cannot be defined objectively by considering the performance of humans or equipment in isolation. They can only be defined with reference to human intentions or expectations; they depend upon somebody's judgement of the specific situation. If system performance is judged below the accepted, present standard, somebody will typically try to-back-track the causal chain to find the causes. How far back to seek is a rather open question; generally, the search will stop when one or more changes are found which are familiar and therefore acceptable as explanations, and to which something can be done for correction.

A more fruitful point of view than to look for human errors as causes of system failures is to consider "human errors" as instances-, of man-machine or man-task misfits. In case of systematic or frequent misfits, the cause can then typically be considered a design error. Occasional misfits are typically caused by variability on the part of the system or the man.

Human variability may excee(i the tolerance limits at the tails of its normal distribution; occurrences which may very well have causes external to the person such as troubles at home, a colleague who asks for a match, or general work pressure. Inappropriate acts during attempts to adapt behaviour to the demands of a failed system may be due to lack of training, inappropriate knowledge etc., but may very well be acts to test reasonable but, as it turns out, incorrect working hypotheses.

In general, human variability is an important ingredient in adaptation and learning, and the ability to adapt to peculiarities in system performance and optimize interaction is the very reason for having people in a system. In order to optimize performance, to develop smooth and efficient skills, it is very important to have opportunities to "cut corners", to perform trial and error experiments, and human errors can in a way be considered as unsuccessful experiments with unacceptable consequences. Typically they are only classified as human errors because they are performed in an "unkind" work environment. An unkind work environment is then defined by the fact that it is not possible for a man to correct the effects of inappropriate variations in performance before they lead to unacceptable consequences. This typically occurs because he either cannot immediately observe the effects of-his "errors" or because they are irreversible. This is no new wisdom; already in 1905 Ernst Mach said: "Knowledge and error flow from the same mental sources, only success can tell the one from the other".

In consequence, this means that human "errors" cannot be avoided. What can be avoided are the effects of human variability if the systems can be designed so as to make effects-of unacceptable human actions observable and reversible.

Reversibility is largely a question of system properties; whether the effect of an action can be compensated in due time before damage has happened. Observability, however, depends very much on the human interpretation of the available information, and this again depends on the way in which human activity is controlled. From a control point of view, three different levels of human behaviour can be distinguished, the skill-, rule- and knowledge-based levels (Rasmussen, 1983). The manual skill is based on automated, smooth and highly integrated behavioural patterns; rule-based behaviour is goal-oriented, but controlled by know-how and professional rules. Only knowledge-based behaviour is controlled by explicitly formulated goals. During training in a particular task, control moves from the knowledge- or rule-based levels towards the skill-based control, as familiarity with the work scenarios is developed. An important point is that it is not the control processes of the higher levels which are automated. Automated manual skills are developing while they are controlled and supervised at the higher levels. When explicit knowledge or rules are no longer needed for behavioural control during normal work, they may eventually deteriorate. With respect to error observability, it is a problem at the skill- and rule-based levels that the goals are not explicitly control-Ling the activity. This means that errors during performance may only be evident at a very late stage an error in the use of a recipe may not manifest itself until you taste the cake; i.e. when the product is present.

Early detection of the effect of one's own variability (or of changes in system conditions) depends on an ability to monitor the process, i.e. on knowledge-based monitoring based on understanding C)f the underlying processes. For error detection it may therefore be important that interface design serves to maintain knowledge, even though high skill is developed.

Skill-, rule- and knowledge-based behaviour are not alternative human processes; they are categories of behavioural control which are probably all active at all times. During familiar work situations, when immediate activity is controlled **by** know-how and automated subroutines, the conscious mind has time left for other business which may be to plan the future, to monitor the effects of past activities, or to speculate on private troubles. The degree to which people tend to use knowledge-based functional reasoning to monitor their activities during familiar work situations probably depends very much on one's individual disposition, but the opportunity to do so certainly also depends on the man-machine interface design. It may support an operator during an abnormal risky plant disturbance to have a symptom-based, computer-supported procedure, as long as plant performance adheres to the designer's predictions and the operator makes no mistakes. However, these conditions may not always be present, and then quite different kinds of interface design are needed for knowledge-based monitoring and "error" observation.

The conclusion of this discussion is that it is important to make the process transparent for the operator and to design for knowledge-based monitoring, even when rule-based, proceduralized operator performance is intended. This is particularly the case when modern information technology is used for decision support. @he operator then cooperates in his decision making with the computer and the designer, and in order to be able to perform a knowledge-based monitoring of the plant response during the steps of a decision and control sequence, the operator will need not only to understand the processes of the plant, but also to know the intentions and design decisions of the control system designer.

References

Mach, E. (1905): Erkenntnis und Trrtum. English translation: Knowledge and Error. Reidel Publishing Company, Dordrecht, 1976.

Rasmussen, J. (1983): Skills, Rules & Knowledge; Signals, Signs & Symbols and Other Distinctions in. Human Performance Models. IEEE, Trans. S.M.C., May-June 1983.