DTU Library

The Use of Man-Machine System Design Criteria in Computerized Control Rooms

Goodstein, L. P.; Rasmussen, Jens

Published in:
Automation for Safety in Shipping and Offshore Petroleum Operations

Publication date:
1980

Document Version
Publisher's PDF, also known as Version of record

THE USE OF MAN-MACIIINE SYSTEM DESIGN CRITERIA IN COMPUTEIZIZED CONTROL ROOMS[1]

L.P. Goodstein and Jens Rasmussen
Riso National Laboratory DK-4000 Roskilde, Denmark

Abstract: The advent of advanced computer-based VDU systems in process control rooms has been handicapped by the lack of a sound basis for their incorporation as an improved aid for the operator. This paper attempts to define and illustrate the use of a set of universal criteria for the design of man-machine systems based on the conception of the human as an information processing system with a limited set of resources and methods for coping with the wide spectrum of normal and unexpected situations which can arise.

INTRODUCTION

The advent of computer-based displays as exemplified by the significant increase in use of visual display units (VDU's) such as CRT terminals for use as'the basic means of access to information has also reached the process industry's control rooms. Here a long tradition of one <u>measurement, one indicator</u> has, on the grounds of space savings or other economic considerations, given way (often abruptly) to more concentrated information centers built up around one or more (color and/or graphic) VDU's connected to the plant data base through the on-line computer system. Although such an approach offers considerable freedom to the designer in the way of presentation and of access to information, it is safe to say that the relatively rapid transition from conventional panels to VDU's has not been accompanied by any corresponding radical change in basic display philosophy. Instead, presentations of the individual process variables are typically transferred to the relatively modest working area on the VDU where they are combined in various ways often as alpha-numeric lists, trend curves or as state indicators superimposed on some sort of mimic diagrammatic background.

---

[1] Automation for Safety in Shipping and Offshore Petroleum Operations A.B. Aune and J. Vlietstra (eds.) North-Holland Publishing Company, 1980. The work reported here is part of the inter-Scandinavian proi . ect on control room design and human reliability, sponsored by the Council of Nordic ministers (Report No. NKA/KRU-P2(80)23).

Aside from reasons based on ordinary conservatism and traditional practise, this tendency is in keeping with one of our time's characteristic traits - the fact the tools and techniques made available by technology together with the ensuing rush to incorporate them far outweigh our knowledge of how they best can be utilized - either in the interests of improving system performance and effectiveness or of maintaining/achieving human well-being for the people who have to employ them.

It is probably not far from the truth to say that this will always be so - matters relating to an optimal incorporation of humans into systems can be likened to a little life raft struggling to keep afloat in the wake of the juggernaut of technology - but never catching up. Therefore any attempts to at least minimize the effects of this unfortunate state of affairs must be based on generalizable concepts and theories which can readily be adapted to a changing world.

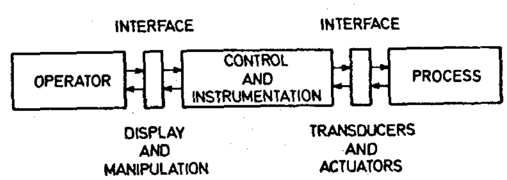
This paper is a modest attempt to define and illustrate the use of a set of (hopefully) universal criteria for the design of man-machine systems based on the conception of the human as an information processing system with a limited set of resources and methods for coping - in this case, with the vagaries of an industrial process complex.

MAN-MACHINE SYSTEM CONSIDERATIONS

To set the stage for the main discussion, it can be useful to use fig. 1 as a reference for identifying and characterizing the basic elements of the man-machine system under consideration.

Process - a system of physical components and substances which together support and sustain combinations of electrical, hydraulic, chemical, mechanical .... processes which can be described, measured, and controlled by means of a set of interrelated variables and parameters.

Control and instrumentation - a system of information processing elements - operating on the one side with transducer-based input data representing the previously mentioned process variables and parameters and generating, on the basis of quantitative calculations and stored decision rules, appropriate output signals for the system actuator interface and/or understandable information to the operator through the display interface - AND operating on the other side with operator messages through the manipulation interface and identifying and inter-



preting these according to stored rules and transformations so as to give appropriate outputs at one or both interface surfaces.

Operator - a complex component describable at many levels but, in the interests of attaining consistency with the instrumentation and control approach, also treatable as an information processing system where terms such as strategies, use of data and models become useful analogies to ordinary data processing concepts such as codes, algorithms, data structures program control, etc. This is not to imply that the operator is a computer per se, but rather that, for system engineers, it can be helpful to consider the human as a kind of computer center in the sense that he or she has access to several types of processing activity in the course of interacting with the surrounding world (1). It is important to identify and describe these in order to make a start, toward being able to move smoothly from one side of the display and manipulation interface to the I other without a drastic and difficult shift in representation.

OPERATOR FUNCTIONING

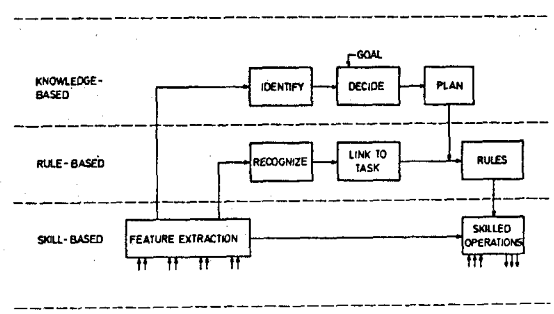
Any attempt at developing and applying criteria for the design of man-machine interfaces must of course rest on a suitable characterisation of human functioning and interaction with the "system". A fundamental concept in any useful characterisation is that the human, in connection with his daily activities, is continually striving to achieve one or another goal - where "goal" reflects a short or long term desire/compulsion to effect some kind of change. This effort is guided and supported in the main by personal expectations and experience. Such a conception thus implies that the human is not merely a passive receiver and processor of information with limited capabilities but rather is an active seeker and doer who constantly tests the state of the environment via a controllable set of samples to check for consistency with the predictions of his/her own dynamic model of the world. It is clear that this formulation has significance for display design.

It will be convenient for the purposes of the following discussion to use three categories of functioning which together broadly encompass the total spectrum of expected operator behaviour:

- skill-based behaviour
- rule-based behaviour
- knowledge-based behaviour.

Fig. 2 indicates the underlying mechanisms as well as the relationships among the three categories.

Skill-ba8ed (automatic sensory-motor) behaviour. - Immediate examples from everyday are riding a bicycle, typing, playing a musical instrument. This type of behaviour occurs typically as the consequence of a consciously expressed intention (ride, type) which is thereafter executed as a subconscious smooth and highly integrated sequence of movements synchronized to certain key features extracted from the "surroundings". The result of highly trained performance, this type of behaviour is relevant in the present context for many tracking and control tasks as well as for manual manipulations in connection with familiar tools and equipment.



Rule-based behaviour - rules take the form of either prescribed @written) work instructions or as remembered procedures from earlier successful applications. Thus, this type of behaviour occurs in situations which arise and are recognized as belonging to the set of previously foreseen or predetermined situations. Rule-based behaviour is typical in the control of complex and/or lengthy activities which form part of relatively familiar job activities.

Ideally - at least in the eyes of management and regulatory authorities - prescribed rule-based behaviour is/should be both task-dependent and operator-independent. However, reports from the field indicate somewhat the contrary (2).

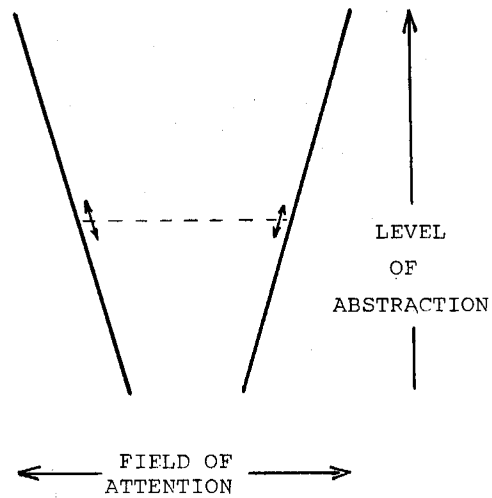
Knowledge-based behaviour - this type of behaviour becomes actual @as a last resort) when skills and rules are neither available nor adequate and the situation therefore calls for problem solving and perhaps improvisation. Elements of data processing thus include observing, identifying, deciding and planning and these involve causal and functional reasoning based on a knowledge of the functional properties of the system including the potential means for and effects of making corrective changes in order to counter an undesirable state or trend.

Under knowledge-based behaviour, there are two important subconcepts which have significance for display design. These are:

- field of attention
- level of abstraction.

Their interrelationship can be seen in fig. 3.

Field or span of attention is a simple yet important concept which can be likened to photographic "zooming" where the amount of system coverage and detail is variable and depends on the desired field of attention which, in turn, depends on the current activity. For example, in the initial phases of a diagnosis, the coverage would be wide and the detail probably restricted to the most critical primary parameters. In the final portion where a corrective action is identified, the coverage would be limited and the detail concentrated on the location and operation of the selected control.



Level of abstraction is a more subtle concept which reflects human ability and tendencies to speculate consciously about the world (or bits of it) in different ways depending on needs and abilities. These ways are best illustrated with examples, starting at the "lowest" level and continuing on to the "highest". Of course the boundaries between levels are not rigid.

1. Physical form: relates to the appearance and location of parts and components; has to do with anatomy and topography.
2. Physical function: how do parts and components work; how are they connected; how do they interact. OR how are variables related; e.g. from empirical data, numerical laws.
3. Functional structure: how are variables related by physical laws; e.g., heat transfer, neutron physics, steam tables. OR in terms of properties of standard functions and their interactions; -e.g. feedback loops, criticality, boiling, computer interfaces.
4. Symbolic function: without direct relation to a given system - expressed in terms of energy, mass, information flows; e.g. logic functions in control and safety systems, computer programs.
5. Functional meaning: what are the purposes and objectives of the systems or functions. What were the designer's intentions with the system.
6. Value structures: what are the relations among goals and values; what is the structure and operation of the goal-setting organisations.

A more detailed description of these with many examples is available (3).

As far as the process operator is concerned, his abstraction range will usually go from (1) to (4) with an occasional visit to (5). When attention has to be paid to the entire system to evaluate the propagation effects of changes, faults, possible counteractions, the operator will/should operate around (4)-(5), i.e., the levels where mass-flow considerations affecting inventories (water, steam, etc.) and energy flows affecting power control need to be related directly to established values and compared with operational limits. Thus a high abstraction level demands usually a large field of attention with limited detail. When attention thereafter is directed to a particular sub-system, the level of abstraction will probably also shift downwards to (2)-(3) where the system-specific physical functions and attributes become important so that more detail within a smaller field of attention will be required.

A fourth behavioural element is equally important and must be included. Common to a response to any situation is the need on the part of the operator for a preliminary <u>identification</u> of the problem followed by the <u>initiation</u> of the proper behavioural category - and this again has special relevance for the display problem. For example, response to unfamiliar and non-stereotyped situations is, according to published event reports, an especially difficult task. This is because operators, instead of integrating all the available information in making their preliminary diagnosis, tend to rely on familiar (individual) indicators as reflecting <u>system</u> state and thus they often can be trapped into making an incomplete and perhaps incorrect identification when their familiar "signs" are insufficient. This is equivalent to saying that, instead of activating a conscious knowledge-based process, the set of signs leads to a premature judgement which can activate either a rule-based or an automatic response or perhaps none. Therefore, coping with this trait in human behaviour is of vital importance.

The above categories describe possible alternate behavioral classes - i.e., they illustrate what an operator can do. However, what an operator will do in a specific situation is difficult if not impossible to predict. For example, operators learn by experience. Thus a task which requires a knowledge-based response at the beginning can later be executed by a set of rules which, even later in time, can evolve into complex automated subroutines. However, the reverse can also occur if, for example, the employed rules degenerate from lack of use and have to be regenerated and reconstructed from the operator's available knowledge base. Thus the boundaries between the classes are ill-defined - both with respect to groups of operators and also as they apply to a single individual as a function of time - since operators will respond in a fashion which is dependent upon the perceived demands of each situation balanced against their currently available resources.

INTRODUCTION OF DESIGN CRITERIA(4)

In general, criteria are expressions implying "value" which are intended to assist the designer in selecting among alternatives and thus reduce the typically high number of degrees of freedom to a manageable few. The importance of criteria as judgement aids increases directly with the variety of solutions available as well as with the degree of difficulty in establishing quantitative specifications for performance - and it is clear that this is exactly the situation existing when incorporating computers and people in a system.

Thus, if a curve of "fit" between man and machine vs. design alternatives could be plotted, then suitable criteria should serve the function - as a minimum - of preventing the resultant design from lying in a deep valley on the curve (which would represent a poor fit) - but more hopefully they would assure a reasonably "good" fit, all factors taken into account (for example, economy, management attitudes, schedule, etc.).

Actually two sets of man-machine system design criteria are necessary:

- those related to man as a system component and thus connected with the characteristics of behaviour described above.
- those related to considerations of the system as man's environment and thus having to do with @a) working life quality and the influence of affective, emotional and socially relevant factors and (b) protection of the population in general and hence the responsibilities of the operator in particular in connection with large, centralized and potentially dangerous system complexes.

This paper deals with the first category with the anticipation that satisfying these will at any rate not worsen the situation with regard to the second category.

The proposed set of criteria will be listed and two discussed in detail here. For each, reference will be made to the appropriate elements of human behaviour as well as to the criterion's general significance for display design. In the concluding section, several of the points regarding displays will be illustrated.

The criteria are listed in Table 1.

Discrimination

Compatibility

Sensitivity

Preparedness

Flexibility

Trustworthiness

Responsibility

Pacing

Reversibility

Error Tolerance

Table 1

DISCRIMINATION

This criterion is directly related to some earlier remarks about the importance in the initial phases of a response to a change in the system of alerting the operator in such a way that the full significance of the change becomes apparent so as to repress normal tendencies to make superficial analyses, premature diagnoses and automatic responses.

A few examples from the field can illustrate the fact that operators adapt quickly to the idiosynchracies of a system and, with experience, begin to rely heavily on individual data elements instead of sets of related. information.

1. Explosion in a chemical plant essentially because the operator's experience led him to interpret the readings on a flow meter as follows:
   - When full scale, the valve is open and the pump is running.
   - When near full scale, adjust the flow.
   - When zero, the valve is closed.
   - When near zero, calibrate the flow meter.

with the results that a dangerous leakage was not detected.

2. Three-Mile Island - because of leakage through a relief valve, temperatures on the outlet side had been high for some time and water had had to be added continuously to make up for the leakage; After a turbine-trip and the resultant primary pressure increase, the relief valve had opened as prescribed but did not close again after the pressure had fallen. Because of their knowledge of the leaking valve, the operators did not revise their interpretation of the continuing high temperature with the result that there occurred a critical loss of inventory through the open valve.

In present day installations, designers attempt to take the discrimination criterion into account in the form of alarm and annunciating systems which are intended to alert the operator about changes in the system. Such aids are usually based on one measurement-one indicator (or line of text) so that complex mental operations are required for scanning and processing when more than one alarm appears as usually occurs in practise. Designers of these systems recognize such limitations and, to a certain extent, attempt to relieve the situation by means of filtering, conditioning, moving thresholds and limits, etc. but while still retaining the basic approach of attempting to capture and display in essentially raw form the behaviour of hundreds, even thousands, of bits of information reflecting system state at many different levels of importance.

The employment of a computer brings with it opportunities for a more sophisticated treatment of plant data as well as for its presentation. For example:

- Data can be arranged in directly perceivable patterns enabling rapid responses to questions like "CHECK THAT....." or "GIVE A NAME TO IT".
- Data can be combined and transformed to depict system behaviour at the universal and fundamental level of mass and energy - in terms of flow and storage. These in principle can be system independent in presentational form.
- Data which normally are connected with a given process parameter can often be converted and combined with other similar data to indicate indirectly the status of a common supply system (electrical, air, etc.).

Such an approach, used as a replacement for traditional alarm systems, could guide the operator through appropriate sets of information, as described above, based on a consistent computer-based analysis of process changes with respect to normal and using the fundamental flow structures in the system. Operators would thus work with integrated sets of information which would give a better basis for discriminating among situations as well as among possible behavioural responses.

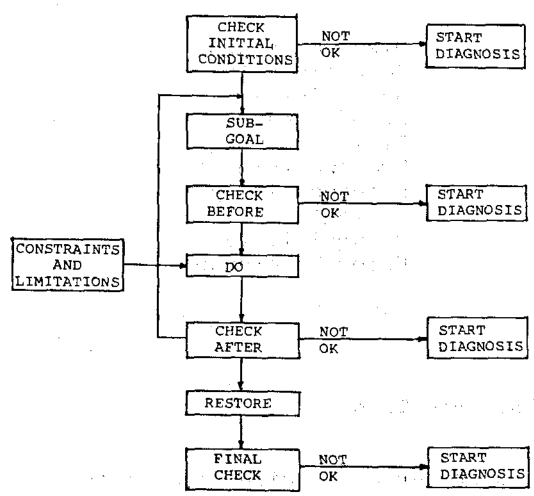
COMPATIBILITY

Previous work on guidelines for interface design (5) has suggested that the concept of "transparency" was of paramount importance in the sense that the operator then would be able to "see the process" through the interface. However, the previous discussion will hopefully have made it clear that the required "view" through the inter-, face is not really so simple. As was pointed out, the operator can indeed speculate at many levels with varying degrees of detail about all or parts of the system. Thus the concept of compatibility would seem to be a more suitable criterion for insuring that the information presented to the operator was transformed into sets of *sym,*bols consistent with his current needs. Therefore it is clear that data presentation must be multifaceted instead of transparent. This will be expanded upon in connection with the behavioural categories discussed previously.

Skill-based behaviour, being automatic, requires a purely graphic / pictorial presentation in time and space in order to support a direct perception of the state of the "world". In more concrete terms with respect to the process plant environment, this would mean, for example, that executing a startup or other change of state could be supported by a two-dimensional time-space display of the major parameters being controlled. Thus orthogonal elements of time (as reflected in the concepts of gain, time constants, reactivity, etc.) and space (parameter XX must not exceed YY) could give rise to a trajectory on the display reflecting the operator's direct control of the evolution through the permitted regions shown on the VDU. Viewed as a driving exercise, this is equivalent to ''keeping the car on the road".

Rule-based behaviour - compatibility of display support with rule-based operations can be related to the following representation of a procedure (work instruction, etc.).

This depicts the sequence of predetermined steps (together with the corresponding pre-established and recognize, able plant states) which must be followed in order to achieve a given goal, - i.e., to move the system or parts of it from one state to another. Thus the situation is known, the steps are preplanned and the operator's response will involve conscious control because of the level of detail and complexity and because of the lack of skilled familiarity with the total sequence. Since reliance on memory is in general inadequate (and indeed can be disastrous), a directly observable/readable form for support is required.

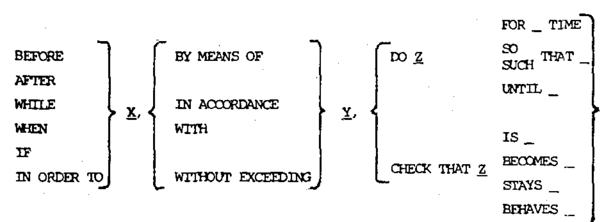


As the diagram indicates, any sequence must start with the plant in a given specified and verifiable state. It is the designer's responsibility to define the "range of applicability" of the procedure and the operator's responsibility to "test for applicability" each time. If the initial conditions are met and the goal is appropriate, then the prescribed set of checks and actions, if carried out correctly on a normal system, should "automatically" achieve the intention of the designer as reflected in the procedure. Displaywise, this means:

- System states and reference states must be able to be compared direct and effectively.
- States and actions should be reliably linked.
- Means for action should be clearly identified.
- Results of actions should be apparent.
- Precautions, restrictions and other constraints must be made clear to the operator -'even if they are built in as automatic features.

Since procedural rules are goal-specific, the corresponding set of displays will also be specific; however, hopefully they can be based on a restricted set of graphic equivalents to the following generic formulation of a (sub)procedure.

<u>Knowledge-based</u> behaviour - compatibility with a knowledge-based approach requires particular attention to aspects of the operator's interaction with a <u>non-normal</u> or unfamiliar system where problem solving and improvisation may be called for. However, novice operators will need similar support under all circumstances so that the display repertoire must be utilizable under all conditions. Instead of basing behaviour on rules or automatic skills, operators here need to plan their responses by using causal reasoning based on the functional properties of the system. This will involve the use of information about:



See (6) for further details.

- Critical system variables - their identification and status with regard to limiting/or other specified values. These variables reflect the state of the various system processes and thus serve as "flags" which warn of current and/or impending trends in system behaviour which can be dangerous (energy pileups,
- Potential means for action-taking on the system in order to change state, structure.

- The "built-in" rules and decisions regarding interlocks, automatic sequencing, etc. employed by the designer for system protection and control.
- Conditioning and supply system status.

Compatibility with knowledge-based behaviour requires also that the associated dimensions of <u>attention field</u> and <u>abstraction</u> level be taken into account.

As was stated earlier, each of these varies with the phase of the problem solving task. In the initial stages aimed at identification of system state, the view must be broad to begin with - while in the later corrective and manipulative phase, the view will be considerably narrower, but will be followed by the need for a wider field of attention when checks for proper response must be made.

Likewise, when attention span is wide in order to evaluate the spread of the effects of changes, disturbances, corrective actions, etc., there is a need for a level of information which is directly related to the state of the overall causal structure of the system as reflected (a) by the previously mentioned critical variables and (b) the system conditioning and supply parameters. A high-level abstract and process-independent form for achieving this can be based on considerations of energy, mass and information flow. Effects of disturbances and changes can then be represented as mass/energy balance disturbances so that depicting system operational states in terms of mass flow structures for inventory control and energy flows for power control can enable a direct comparison with normal and limiting states to be made.

However, when attention span is more limited, the abstraction level will also usually become more specifically concerned with the physical and/or functional properties of particular items of equipment.

Thus shifting field of attention and abstraction level requires some kind of combined <u>windowing</u> and <u>zooming</u> technique so that different portions of the system can be selected at different levels of abstraction. This creates the need for a large set of displays, probably hierarchically structured, which, especially in a VDU-system, will require an efficient accessing time, inflexible chaining of pictures, the need to remember names .... This is not an insignificant problem. Hopefully the use of "hybrid" control rooms where VDU's are supplemented with other computer controlled display dynamic wall mimics, projected presentations, eventual flat panel units, etc.) and the introduction of improved accessing techniques using voice or touch will ease the situation.

The compatibility criterion is relevant as a measure of the degree to which requirements for display support for all categories of behaviour are met. Thus it is usually not sufficient to aim at selected coverage for only rule-based or for only knowledge-base behaviour because, in actual interactions with the plant, the response will not be fixed but subject to the capabilities and experience of each operator. Thus rule-based behaviour needs as an alternative knowledge-based support to permit regeneration of rules; rule-based behaviour may also low inventory ... selection mechanism for the operator without excessive delays because of require skill-based support in cases where procedures are performed so often that automatic skilled responses can be generated.

In any case, sophisticated aids such as computer-based display systems receive better grades for acceptability from their users if the behaviour of the total system is understood and predictable.

DISPLAY CONSIDERATIONS

Considerations of human behaviour as outlined in this paper and summarized in fig. 2 lead to a set of control room activities and thereby corresponding needs for display and other aids which can be classified roughly as follows:

Behaviour	Activity requiring support	In the form of
Skill-based	Manipulate such that ___	Trajectory display
Rule-based	Give a name to situation	Data patterns
	Link to a task	Info retrieval
	Follow task rules	Procedural support
Knowledge-based	Find out about (what, where, how, how to)	Data patterns
		Flow diagrams (see text)
		Info retrieval

Space does not permit a detailed review of these - some are already well known.

For example, data patterns commonly take the form of bar graphs of one type or another, trend curves, alpha-numeric lists. Other possibilities include:

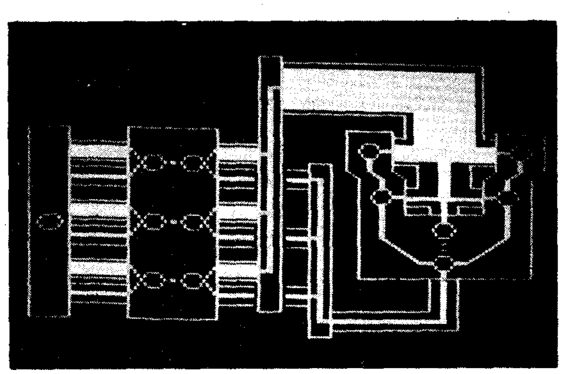
- Deviations from a normal figure such as a circle or other symmetrical shape.
- Other "balance"-based formats.
- Phase-plane plots - especially for control systems.
- Computer-generated faces (used first for geological data).

Surprisingly, control room VDU's are not commonly used for trajectory displays - i.e., the presentation of X vs. Y with time as the third dimension. Nor have computers been utilized very much for supporting procedures. checklists or ' giving operators access to design data bases. Indeed, as stated in the introduction, computers in general do not yet seem to have found their proper niche in control room thinking.

In addition to the display types mentioned above, there emerges from several points in the criteria discussion the need for graphical representations of the plant suitable for monitoring, detection of disturbances and initial identification of problem areas and extent. In this connection, it was suggested that a representation in terms of the flow and storage structures of the various processes based on the fundamental- concepts of mass and energy conservation and also incorporating elements of the system's information and control structure would Five, in principle, the basis for a high-level task-independent description of the system which could be incorporated into a hierarchical display repertoire. The following two display types reflect the main ideas behind the flow concept:

- Power control with display of:
    - Branchings, feedback of energy.
    - Levels of energy "accumulation" via status of critical variables.
    - Means for control and routing.
- Inventory control with display of:
    - Supply and loss.
    - Levels of accumulation.
    - Means for control and routing.

To these can be added important information on conditioning states (vibration, vacuum, bearing status) and common supply systems (el, water, etc.). Flow representations can be either absolute or deviations from normal. An example of an energy flow display taken from a VDU is shown on fig. 5 for a PWR unit with three steam generators and two turbo-generator units.



It should be mentioned that this display approach is part of a broader analytic treatment of systems based on energy and mass flows.

For further details, see (7) and (8). The method has excellent potentials for, among other things, the systematic design of procedures as well as automatic diagnosis.

CONCLUDING REMARKS

This paper has discussed criteria for man-machine system design - with emphasis on information transfer via displays - on the basis of a consideration of the human as a data processing system with identifiable operating modes - skill-based, rule-based and knowledge-based. Needs for display support have been identified; the lack in the past of computer integration into a total display function has been decried and a new computer-based approach using flow structures has been presented.

REFERENCES

(1) Rasmussen, J., Man as a Systems Component. In Smith, H. Green, T. (Eds.), Man-Computer Research, Academic Press (to be published).

(2) Rasmussen, J., What Can Be Learned from Human Error Reports. In: Duncan, K., Gruneberg, M. and Wallis, D. (Eds.), Changes in Working Life, John Wiley & Sons (Proceedings of NATO International Conference on Changes in Nature and Quality of Working Life, Thessaloniki, Greece, 1979) (to be published).

(3) Rasmussen, J., On the Structure of Knowledge - a Morphology of Mental Models in a Man-Machine System Context. Riso-M-2192, 1979.

(4) Rasmussen, J., Notes on Human System Design Criteria. Preprint to IFAC/IFIP Conference in Socio-Technical Aspects of Computerisation 79, Budapest.

(5) International Purdue Workshop Industrial Computer Systems, Guidelines for the Design of Man/Machine Interfaces for Process Control, Purdue Laboratory for Applied Industrial Control-, August 1978.

(6) Goodstein, L.P., Procedures for the Operator - Their Role and Support. Presented at IAEA IWG/NPPCI Specialists' Meeting on Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations, Munich 1979.

(7) Lind, M., Flow Models of Material and Energy Processing Systems. Riso-M-2201, 1980.

(8) Lind, M., The Use of Flow Models for Design of Plant Operating Procedures, see (6).