On the reliability of process plants and instrumentation systems

Rasmussen, Jens

Publication date:
1968

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

DANISH ATOMIC ENERGY COMMISSION **February 1968**
Research Establishment Risö **R-7-68**
Electronics Department **Risö-M-706**

ON THE RELIABILITY OF PROCESS PLANTS AND INSTRUMENTATION SYSTEMS

BY Jens Rasmussen

A. E. K. Risø

Risø - M - 706

Risø - M - 706

Title and author(s)

On the Reliability of Process Plants and Instrumentation Systems.

By Jens Rasmussen

Date February 1968

Department or group
Electronics Department

Group's own registration number(s)
R-7-68

28 pages + tables + 4 illustrations

Abstract

The reliability of an instrumentation system is often regarded as a property that may be evaluated when the system has been designed on the basis of purely functional criteria. In this report, elementary reliability properties of an instrumented system are discussed in an attempt to incorporate the reliability as a fundamental specification for the process control system proper as well as for monitoring and safety systems.

Copies to

Abstract to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, Roskilde, Denmark.
Telephone: (03) 35 51 01, ext. 334, telex: 5072.

FI 25-204

TABLE OF CONTENTS:

INTRODUCTION

The problems connected with the reliability of large, complex electronic systems have been the subject of much interest of late years and have been dealt with in a large number of publications reporting theoretical investigations as well as conclusions based upon empirical failure data. As these studies are aimed at elucidating widely different problems, it is often very difficult to judge whether the methods and results reported ar,e adequate for the assessment of a particular actual system.

The first thorough investigations had their starting point in reliability problems connected with military installations, and this origin and the military capability aspects and mission-oriented tasks still leave their impress on the terminology and definitions in common use for the reliability of electronic systems.

On acount of the tremendous development of electronic systems and their use in industrial automatization, a need has arisen for increasingly efficient methods of predicting the reliability of a large-scale electronic system at an early stage of the development and design phase of the process plant as a whole; for not only does automatization involve the possibility of expensive consequences of failures in the electronic equipment, but the rapid development of the numerous special applications makes operating experience from existing plants an insufficient basis for evaluation. The reliability of industrial plants - apart from such in which failures may result in injury to human beings - must be estimated from an economic analysis of normal and abnormal operation, while the operational reliability standards developed for military installations are not directly applicable. As to industrial process plants the problem is to create a plant performing the desired function in the most economic way for a long period; in such plants maintenance and repairs are usually possible. Therefore the economic penalties of the different failure types determine, what precautions are economically justifiable, and so a detailed analysis of the various possible failures is required. Also in this respect industrial plants differ from military installations, missile and aircraft equipment, which are desired to perform a particular function faultlessly for a given - often rather short - period during which repairs are out of the question. Here a, more detailed classification of failure possibilities is often of no interest.

For the reliability of a plant to be estimated in advance, regard must be paid both to gradual changes in the components and the influence of the environment and to radical changes of a statistical nature caused by component faults. This requires mathematical descriptions of the failure mechanisms as well as information about the nature and frequency of the

failures, and much work is done all over the world to develop suitable models and collect failure statistics. In the preparation of mathematical descriptions of actual plants it is necessary to make a great number of simplifying assumptions, and existing failure statistics are usually most imperfect; therefore endeauvours to evaluate the reliability in advance often give rise to great scepticism.

Although it is not possible with any great certainty to calculate the reliability of a plant beforehand, and is not likely to become possible in a period seeing a rapid development of components and plants, the value of a systematic assessment based on simplified models and inadequate failure statistics should not be underestimated; for such assessment may often efficiently call attention to weak points in the system and its mode of operation and may further present a reasonable choice between alternative designs and countermeasures against the more important sources of failure.

SYSTEM

In the following we shall consider a system, mechanical, chemical, electrical or economic, which produces an output (a product or state) from an input (raw materials, power forms, etc.) under the influence of a control signal. These three quantities may all be multidimensional.

The output will be subject to quantitative or qualitative specifications, and the system is considered reliable when the specifications are met in an economically satisfactory way. Thus the system may sometimes fail to meet the specifications and still be reliable if countermeasures against failures are feasible and the economic losses are of minor importance compared with the total process economy and balanced with the cost of gaining a lower failure rate by a more conservative design.

The output is related to the input by a law, the transfer function of the system, whose parameters may be varied by means of a control signal.

Of course it is only possible to estimate the economic consequences of failures for an actual plant, and even for that often in coarse outline only since such estimation must be largely based on an evaluation of the probability of occurrence and the duration of failures. However, it will normally be necessary to establish limits to the consequences one is willing to tolerate in the case of failures, and these limits provide an important basis for the design of the system.

In the present discussion, failures can therefore only be divided into certain characteristic classes.

A class apart is constituted by failures that may cause injury to persons.

An economic evaluation of this class of failures and of expedient countermeasures has been attempted by several investigators 1), but is unrealistic for so small an economic unit as a single plant or enterprise. An evaluation should ensure that the risks connected with the plant do not contribute to the general hazards of the operators, but it must be taken into account that excessive protection against the factors that are under control may increase the unknown risk from factors not under control.

An important type of failure from an economic point of view is plant failures resulting in large once-for-all expenses every time they occur, for instance costs of repairs for damage to the plant. Such failures most often interfere abruptly and radically with the operation of the plant, and in estimating the extent of countermeasures the frequency of the failures is clearly the decisive factor. This type of failure is evidently characterized by manifesting itself to the operating staff, when it occurs.

Other failures cause increased working expenses, depending mainly on their duration, e. g. in connection with losses due to less economical production, products of poor quality or increased possibility of more comprehensive damage to the plant during thc-, period in which the failures are present. These failures do not always manifest themselves when the occur; they may be due to minor and gradual changes in the plant, and what matters is not their frequency, but their integrated duration.

Thus, for a reliability assessment it does not suffice to add up the failure frequencies of the various components; the influence of the individual failures on the overall economy must be estimated. The principal difficulty is that such estimates in most cases necessitate component failure statistics showing a far more detailed distribution on failure types than those made to-day. An open circuit fault in a simple component such as an electric resistor may have an effect on the total plant essentially different from that of a short circuit, and while it is possible to find applicable figures for the total failure frequency of the resistor, it may be necessary to resort to pure conjecture as far as the distribution is concerned.

According to their effects on the performance of the plant, failures may be divided into three categories:

The first category comprises failures caused by an input to the system of false information which, being treated in the same way as the genuine information, causes deviations from the specifications of the output. This group may include influences from the environment of the plant in the form of e. g. heat, induced noise voltages and variations in supply as well as component failures.

The second category consists of failures that bring about parametric changes in the transfer function of the system, such as variations in gain and wear phenomena. Like those of the first type, these failures may be due to outside influences as well as component changes.

The third category is constituted by failures that give rise to structural changes in the system involving an alteration of the form of the transfer function, for instance interruption of information channels or establishment of new false couplings; mechanical ruptures, and saturation phenomena. This category comprises a number of failure types that may be regarded as excessive parameter variations. On the whole, the limits between the categories are undefined.

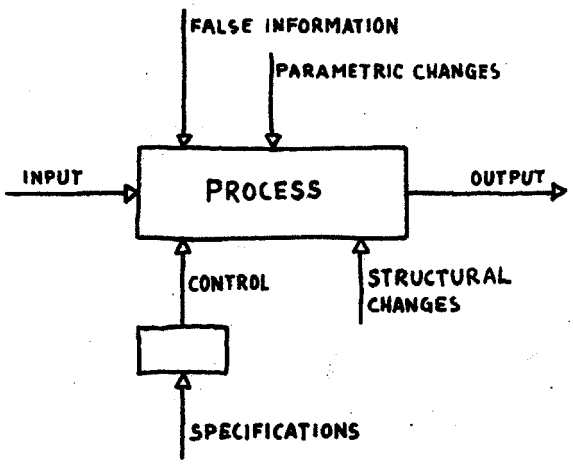
One and the same component failure may give rise to - possibly simultaneous - system failures within two or more of these categories.

This, however does not affect the fundamental classification as applied in the following considerations.

The discussion of countermeasures will only comprise the technical possibilities of obtaining a reliable process in spite of unreliable components and disturbances from the surroundings; the trivial possibility of improving reliability by choosing better components and surroundings is left out of consideration.

DIRECT CONTROL

In its simple form the process system may be depicted by the block diagram below:



The diagram illustrates a process that converts an input (often multidimensional) to the desired output under a controlling influence based on the desired specifications. A condition for the practical applicability of this sim-

ple scheme, which shows the directly controlled process, is that the relation specification - control - output is sufficiently unique - so that the designer may predetermine the entire process in every detail. This will only be so when the process is based on simple fundamental laws unaffected by disturbances.

In designing a process plant one naturally endeavours to base the process on an inherently reliable law, but the fact that the choice of process depends very much on operation economy will greatly influence the range of selection.

Since a process permitting direct control must be governed by simple and stable laws, the control possibilities are often very limited and the specifications of the output therefore incorporated in the system itself by the designer.

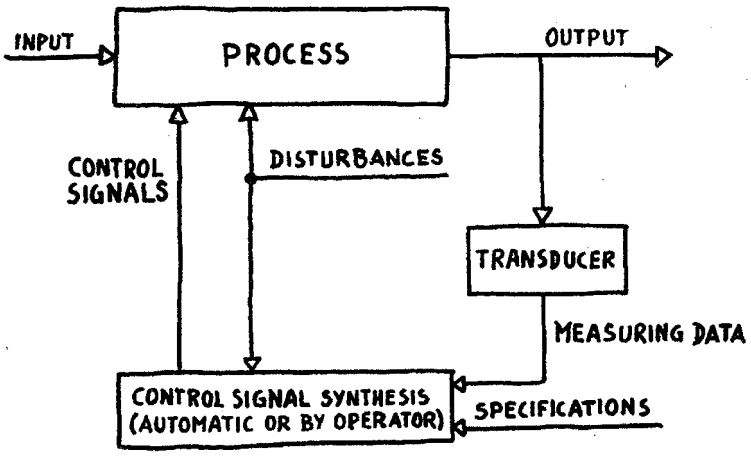
By way of example may be mentioned machine tools, with automatic stamping machines as an extreme.

Where the process cannot be based on a law so unfailing that the desired output can be obtained by direct control, compliance with the specifications must be ensured by continous measurement of the output.

FEEDBACK

For measurements to make any sense, the result,-, must be compared with the specifications, and on the basis of this comparison the process must be controlled by means of suitable signals.

The synthesis of control signals may take place in an automatic control device or through the action of an operator in manually controlled plants. Either case may be illustrated by a block diagram of a feedback system:



For the purpose of the fundamental discussion we shall here impose the restriction that we look upon the static properties, i. e, that the speeds of variation are so low that the operation is not influenced by the dynamics of the system.

Obviously a satisfactory reliability depends upon a reliable measurement of the specified properties of the output, that is a reliable conversion from a property of the output to a signal, a representation in the instrument system and conversion from the specification to a representation. If it is possible, by means of the control input, to counteract all changes of the output signal due to false signals and parametric changes throughout the variation range, the influence of such changes on the output may be kept within the specified limits provided the sensitivity of the control input is adjusted to the signal level obtained by the comparison between measured value and specification. In other words, the gain and the dynamic range must be sufficiently large. (Systems utilizing this technique thoroughly in practice are referred to in parts of the modern literature 2) as "high-gain adaptive systems"). Thus instrumentation improves the reliability where the process relation 'specification → control signal → output' is less unique and reliable than the opposite relation that may be utilized in a control system: 'output → specification → control signal'.

The great possibilities of improving the reliability of complex processes by the use of instrumentation are due to the fact that in the instrumentation there is a very considerable liberty of choice both of the physical system used as instrumentation and of a variable as representation in this system that physically deviates substantially from possible disturbances. One may choose among electrical, pneumatic and mechanical systems; in electrical systems the representation may be D. C. or A. C. signals, pulse-modulated voltages, etc.; and the representation may be analogue - or digital-coded.

As appears from the above, planning of process plant and instrumentation as a whole may be decisive for the reliability as a comparison is required between the possibilities of choosing inherently reliable laws in the process and in the measuring equipment. Minor changes in the specification may often decide the choice of system.

To illustrate this we may take a simple system designed to keep a temperature constant . Looking for E. simple law that ensures a constant temperature, we may naturally think of 0 and 100^0 in the centigrade scale. if 100 0 C is a useful temperature, and the variations in the boiling point of water at normal barometric variations are within the specifications, simple

direct control is possible in the form of an open water bath, the only purpose of the control being to ensure a sufficient supply of power.

Even a minor alteration of the specifications may lead to difficulties. If e.g. 90^0 C is desired constant temperature, it cannot be immediately ensured by any simple law. The temperature is here directly dependent on the power supply, the temperature of the surroundings, etc., and it is necessary to investigate whether measurement and regulation are the most advantageous method.

This necessitates another physical system that permits a unique conversion of the temperature and the reference to a new variable, suited to control the power supply, in this system. It is well known both that such a system can be provided and that an expedient representation is possible in both electrical, pneumatic and mechanical systems.

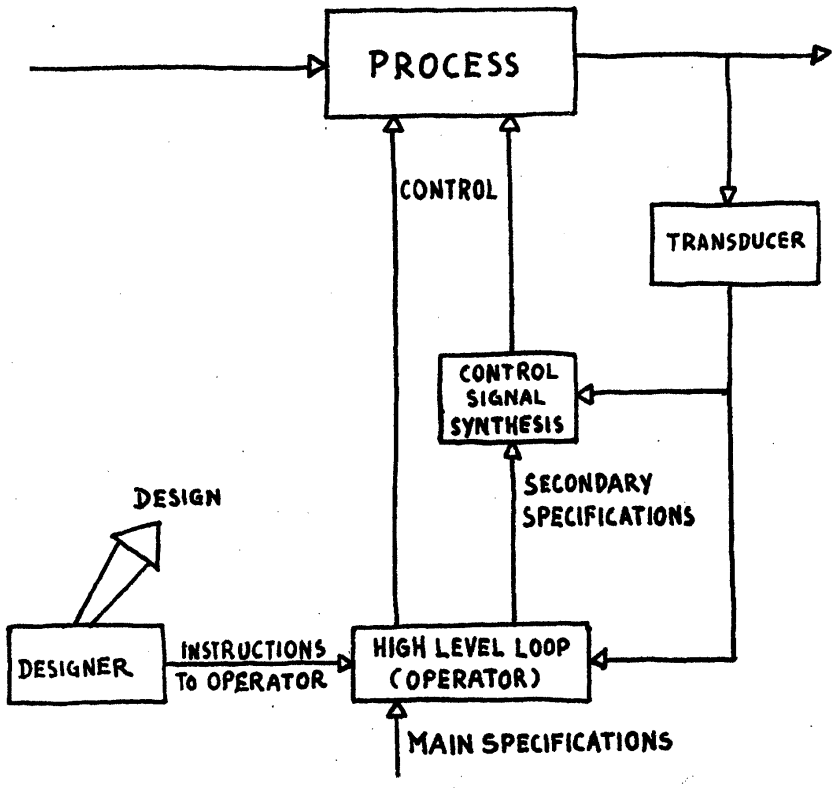
The specification and the output are usually multidimensional, the output being characterized by several specified parameters, which may be mutually related by their dependence on a superior specification. If the individual specified parameter can be measured directly, and if they can be controlled independently of the others by a suitable signal, the system may be regarded as a number of independent elementary control loops.

However, this is usually not the case. Often the specified property cannot be measured directly by sufficiently simple method.-,; instead a calculation must be made, based on measurement of secondary properties. Moreover, a close coupling may exist between the effects of the various control signals on the output parameters. In these and other cases the control signals must be based on a more complicated combination of the representations of measured data and specifications in the instrumentation. It is important to emphasize again, from the point of view of reliability, that any law utilized for the conversion of measured data and specifications into representations in the system and for calculations on these representations until the comparison is made must be qualitatively and quantitatively reliable, while laws utilized for operation on the signals after the comparison are only subject to qualitative requirements.

The reliability demands on -the functions of measuring and specification do not immediately apply to subsystems that measure and formulate secondary specifications if the final main specification is controlled by a higher-level feedback loop. As control input such a loop may often advantageously use the specification or reference input of a lower-level loop, whereby the demands on the reliability of the functions of measuring and specification in the lower-level loop are eased. In many actual plants this superior control is carried out by the operator.

Such division into lower-and higher-level loops may be necessary, both because the state of operation of the plant depends on a number of technical factors not directly related to the primary output specifications, and because these specifications may necessitate evaluation of the output during a longer period , for instance for the purpose of economic optimalization, and thus give no information about the required immediate control signals.

The block diagram of the system is now as follows:



In large plants the designer is ofted presented with a choice between automatizing the superior control function, which requires clear, objective and detailed specifications, and leaving this control to an operator; in the latter case the control may be based on more loosely defined specifications formulated during the training and instruction of the operator.

Under normal operation conditions the operator is thus part of a feedback loop and may continually correct his controlling actions on the basis of the result. After the training period the designer's instruction - apart from the continuous up-dating of the operation specifications - will therefore be of negligible importance and be replaced by the operator's experience. The operator's role in the system will be well defined, and his properties may be established on the basis of experiments and experience from other plants with human operators,

As discussed later, this does not apply to the operator's sole under abnormal conditions.

It is as true of the measuring and specification equipment in the instrumentation as of the process itself that if it is not possible to utilize a simple and reliable law for the conversion one way, e. g. from measured value to representation, the possibility may exist of utilizing a simple law describing the opposite conversion. If the function of amplification is sensitive to the parameters, the more stable attenuation may be utilized in a feedback; where measurements are more sensitive than direct control, the latter is used in a compensating measurement.,

Outside the measurement/specification function the reliability problem is thus eased by the fact that only a qualitative relation is required between control signals and output. This means, however, that in this simple system the instrumentation does not compensate for structural failures, which disturb just the qualitative relation. Failures manifesting themselves as parametric variations ("multiplicative failures") are counteracted regardless of their location in the system (still provided it is outside the measurement/ specification function in a higher-level loop), and it is well known that their effect depends only on the "loop gain". False information is an "additive failure", whose effect may be assessed by conversion into an equivalent error in the specification. The effect of the feedback on this failure type is implied in the possibility of altering the conversion factor in the design of the system and the positioning of the it gain" in the loop.

On the above-mentioned static assumptions, all failures resulting in parametric changes outside the measurement/ specification system may thus be counteracted by a sufficiently high gain. The only demand on the process is that it is possible to control the specified properties of the output through the control input.

DYNAMIC PROPERTIES

The much simplifying static assumption does usually not hold, for the control signals will have no immediate effect on the output because of time constants or delays in the process, and the memory in the system expressed by the time constant ("energy accumulator 11) makes the state of the system dependent on its past history. Therefore the control signals normally depend, not only on the immediate value of the output, but also on the past history of the system.

In some cases, for instance when pure time delays occur, the system may be improved by combining feedback with direct control, the control signals

being calculated on the basis of direct measurements of the input and the other influences. Such direct control is sensitive to disturbances, but any faults in the control signals will be corrected by the feedback.

Thus the control signals normally have to be modified in a compensator dimensioned by the designer to give the necessary time correction. The dimensioning will be based on knowledge of the process and its dynamics and on a specification of the response of the output to transient effects.

The time correction in the compensator is in the nature of direct control, being conditional upon accordance between the dynamic properties of the process and the model of them constituted by the compensator, as well as between the designer's dimensioning criterion and the influences to which the process is exposed. The properties of the output under transient conditions will thus depend on parametric variations in the process as well as the compensator unless a higher-level loop controls the parameters in the compensator and/or the process on the basis of a measurement of the transient properties and a corresponding specification.

In most automatized plants to-day this control is exercised by the operator who adjusts the compensators as required; in this way the need for an objective specification of the transient properties is to a certain degree eliminated. In plants with great parameter variations, and in the case of increasing automatization, the control must be taken over by the higher-level loop; in many cases this will present a problem, at the design stage, of establishing an appropriate specification of the transient properties and a suitable measuring method.

It is the wish to be able to control a process with greatly varying or poorly defined parameters that has given rise to the intensive. studies of adaptive and optimalizing systems carried out of late year,,. In these investigations little attention has been paid to parameter variation.- in the instrumentation itself. From this point of view the most promising systems seem to be those in which the instrumentation does not comprise a model of the process, but information about the I:ast history of the system is gained by extensive direct measurement of the state of the process, and the control signals are made from an optimalization on the basis of constant "experimenting" with the process and of an objective specification of the desired properties.

As mentioned above, the feedback principle as currently applied has no correcting influence on the consequences of such structural failures as decisively change the performance of the plant. On the contrary, the effect of structural failures that open a feedback loop may be aggravated since the high gain characteristic of feedback systems may drive the system to one of the limits of the dynamic range. Structural failures usually manifest themselves in sudden changes of the performance of the system, but may have

widely different physical causes: wear (e. g. mechanical breakdown) gradual change of electric components (e. g. stop of oscillator), noise pulses (change of programme in digital computer), and abrupt failures in electric components.

The normal procedure in the case of a structural failure is to stop the process in response to a failure indication, search for the failure and carry out repairs. In the majority of cases the best countermeasure is therefore the installation of an efficient monitoring system to detect failures, protect the plant and assist the staff in locating failures.

The above-mentioned procedure may be inadequate in plants with a great reaction speed. Here it may be profitable to introduce alternative operation possibilities by duplicating equipment for particular critical operations.

To be efficient such duplication, which may be effected on component subsystem or system level, must be based on a detailed analysis of the plant and its operational and maintenance procedures. Especially it is important that there is no coupling between a unit and its duplicate so that failures may affect them both simultaneously (for instance there must be no possibility of damaging all cables in a doubled information channel at the same time). By failure indication or routine inspections it must be ensured that failures are detected and repaired in the individual doubled units soon after occuring, seeing that the mean interval between failures in a redundant system, where repairs are not made till system failures occur, may be considerably smaller than that for the individual 3) channels constituting the system

In the process plant itself doubling is often an expensive affair as compared with the resulting sawings in costs of repairs and loss of profits; in large process plants doubling of certain critical units in the instrumentation system may be necessary.

In traditional instrument systems, the functioning of each component and unit has been carefully planned by the designer. The system is therefore very sensitive to structural failures, and under normal operating conditions doubled equipment will be superfluous (redundant).

This is true especially of the units connecting the process with the instrumentation via measuring units (transducers) and control units (actuators). As regards the part of the instrumentation that calculates the control signals from the measured data, recent investigations on self-learning data processing systems seem to point to a possibility in principle of building up system of uniform units whose functions and mutual couplings may be influenced by appropriate control signals derived from an -evaluation of the working results of the plant. If the units are sufficiently general in their functions and their number in the system sufficiently large (micro-

electronics), the duplication or redundancy principle may be radically utilized, and rapid repairs to failing units will be unnecessary. An interesting property of such systems will be that the functioning units may at any time be utilized in the best possible way so that gradually accumulating failures do not lead to a radical change of the functioning, but to a slow degradation of its quality (graceful degradation). Of course this principle is of most interest in systems that cannot be repaired; the preliminary investigations reported therefore naturally deal with missile and satellite equipment.

Some reported investigations of self-learning control systems for process plants have been concerned with the control of processes with poorly defined properties and influences. In the nature of things such systems are well adapted to face failures and unintended variations in the process plant, but in their design little attention has, as mentioned been paid to failures in the control equipment.

Instrument systems based on a great number of uniform units are clearly decentralized, the necessary functioning types being distributed over the system. A structural failure will therefore affect only a very limited part of the total functioning (in self-learning systems even only during the retraining period). In greatly centralized systems, represented particularly by computer systems, in which all functions of the same kind are performed in the same circuits - all memory is concentrated in the ferrite memory, all decisions are made by the same arithmetic unit,, etc. - the desired functions of the system are specified to the smallest detail in circuits and programme, and failures in a single circuit may greatly affect a large number of operations. This system design is thus fundamentally very sensitive to structural failures - and to parameter variation, and false information leading to structural changes through programme disturbances. That such systems may be very reliable in practice is due to other factors; the digital representation in itself makes the system insensitive to a number of types of false information and to parameter variations in the basic circuits; the high data processing speed makes it possible - with rather little equipment - to solve problems whose solution would otherwise be unrealistic in practice because of the amount - and thus unreliability - of the conventional equipment needed; last, but not least, the fact that the operation required for a special purpose may be based on a programme stored in mass produced equipment means that the risk of unreliability involved in the use of tailored special equipment is avoided.

The self-learning control systems offer an interesting possibility of solving the reliability problems arising where it is difficult to formulate the functional specifications of the plant in a way that may be utilized in a conventional control system. Here it is possible to control the structure and pa-

rameters of the system through a higher-level good-bad comment on its functioning.

The considerations above are concerned with instrumentation systems, but apply to other systems as well, social and economic for instance. In organizational discussions we recognize the concepts specification of purpose, rmasurement of result, choice between ordered and goal determined functions, and choice between centralized and decentralized structures.

MONITORING AND SAFETY SYSTEMS

Only in very few instrumented process plants is it possible in the long run to obtain satisfactory reliability - that is satisfactory, or optimal, operational economy - alone by means of instrumentation and operator in a reversible control function. The sensitivity of the system to structural failures will generally in itself necessitate a monitoring system. The latter here means a system that controls part specifications of the output or internal variables of the process plant, and which - automatically or via the operator - may establish a safe state of operation of the plant when these variables are found to have values indicating a hazardous state of operation.

The functions of the monitoring system differ on essential points from those of the normal process instrumentation. The purpose of the latter is to control - continuously and reversibly, in a closed loop - a process in such a way that measured properties of the output correspond to the specifications. As discussed above, the reliability of this control depends closely on the self -healing effect in a feedback loop; the system, as it were, feels its way and is able reversibly to adjust its effect on the process to its experience with respect to the result.

The monitoring system, on the other hand, is designed to protect the plant against rare events, radical failures in the plant infrequent outer influences, and unusual combinations of minor failures. The system measures selected quantities in the plant and compares the results - or quantities calculated from the results - with the specified limits. Under normal conditions, i. e. when the limits are not exceeded, the system has no influence on the operation of the plant. Only when the limits are exceeded does a signal from the system induce a correcting action (automatic or via the operator). The system has no influence on the further course of this correction, that i,-., it cannot cancel it if it has an inexpedient effect. The characteristic monitoring system is thus a pronounced "open-loop" system, incapable of "feeling its way". On account of its irreversible nature, the intervention of the system will usually have great consequences for the operation, and the problem of reliability will be marked by the resulting high decision level in the system.

Monitoring systems range from simple systems in which just one physical quantity is measured and the system, in the case of exceeding of a fixed limit, gives an alarm signal and automatically stops the process, to complicated plants in which a great number of quantities are measured -and, after advanced processing of the data collected, a choice is made, possibly by an operator, between a number of corrective actions in accordance with the situation.

Because of the discrete nature of the functioning of the system, failures in the system cannot be expediently divided into information, parametric and structural failures; they must be classified solely according to the corresponding corrective action and according to whether they induce this action at the wrong time (Tail to safe") or block it when it ought to set in ("fail to unsafe").

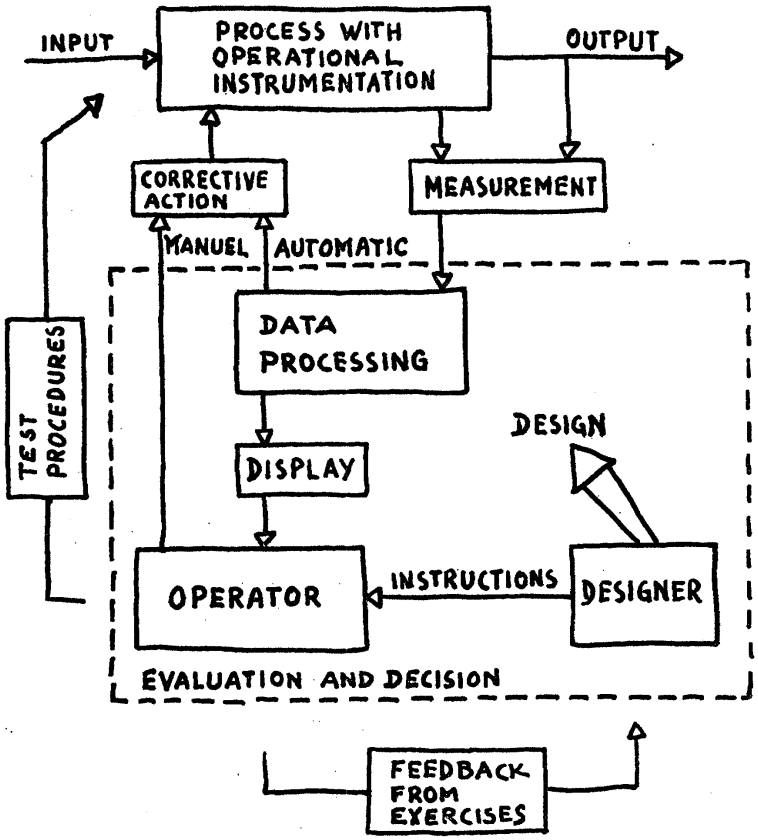
The reliability of the monitoring system is thus characterized by the frequency of unwanted interference with the operation and the corresponding loss of profits caused by failures in the instrumentation, and by the duration of failures blocking its protection of the process plant, measured e.g. by the "dead time" (i. e. the relative integrated time during which it is blocked) and the connected economic risk.

THE FUNCTIONS OF THE MONITORING SYSTEM

By measurement the monitoring system collects information about the state of the plant. Then, by data processing it detects possible failures in the bounds and relations that govern this information in normal operation. If an abnormal situation is detected, the cause of the failure is identified, the failing component is localized, a decision is made about a suitable countermeasure, and the countermeasure is put into effect. For the decision to be made, extensive information i,- required which cannot be obtained by measurement on the plant, but must be incorporated in the functioning of the instrumentation by the designer or imparted to an operator through training and instruction. The functions of the monitoring system may therefore be illustrated by the block diagram below:

In how far it is possible to monitor the operation and identify causes of failures by processing of the measured data is determined by the extent of the measurements. In the choice of measuring parameters regard must be paid to the fact that the measurements are to serve for monitoring not only of the process plant, but of the measuring equipment itself. While continuous measuring channels are currently tested by the normal operation, the same is not true of measuring channels with a threshold value that causes them to function only in certain operational situations. To ensure the functions of these channels, special measures must be taken in the form of

regular testing with a simulated signal, possibly combined with an appropriate kind of duplication.



By doubling a measuring channel that transmits measured data continuously one merely increases the redundancy in the measured information, which is in any case necessary for the detection and localization of failures from the measurements. However, the demand on the duplicated information is so simple - the measured results must be equal - that the identification of failures in these channels requires only simple equipment in the data processing unit.

In doubling discontinuously acting measuring channels one must bear in mind that such doubling will only serve the intended purpose if carefully planned since the design of the system as well as the testing and repair procedures used have a decisive influence on the reliability. At worst, doubling may reduce the reliability of the system. 3)

The normal state of operation of the plant is defined by the designer, and the relations governing the measurement data in normal operation are established during the design and commissioning. In addition to the measured data, information about these relations is necessary for the data processing connected with failure detection. Where an operator is to be responsible for the detection of failures, the designer must make sure, by training and instruction, that the operator has the required knowledge, which he may up-date from his operational experience. In view of the limited ability of

the human operator to remember detailed data accurately and, especially to pay constant attention during long periods of normal operation, it is desirable to exonerate him from this task. Further, as the designer can usually provide a covering definition of the normal state of operation, automatization of the failure detection is a most realistic measure, as indicated by the widespread use of effective alarm systems. The role of the operator will then be that of a supervisory monitor, and with a suitable display system at his disposal he will be well adapted to play it because he can draw on this normal operating experience.

Identification of failures and decisions about action present much more complex problems. What is required here is not only measurement data, but comprehensive information about the reactions of the plant and their consequences in connection with a vast number of different failures and failure combinations in the process plant as well as the instrument system.

Faced with the identification and decision problem, the de signer may either foresee actual failure -ituations and incorporate detailed identification and action procedures in the instrument system, or he may impart the necessary information to the operator at a higher level by giving him, through training and formulated instruction, a thorough understanding of the nature of the plant and its response to abnormal situations. As both possibilities have pronounced advantages and drawbacks, it is natural that we here find the most complicated cooperation between operator and instrumentation.

As the identification and decision function is of a markedly discrete nature, its reliability will depend on the testing procedures used as a safeguard against failures that may block the system (fail to unsafe). As to the instruction system, testing in the form of exercises is as necessary as testing of the automatic functions of the instruments This is so because in well-designed plants it is just the very hazardous failure situations that have a low probability of occurrence, and the corresponding instructions and procedures may therefore degenerate unless they are kept alive by exercises.

FULLY AUTOMATIC MONITORING SYSTEMS

Incorporation into the instrument system of failure identification as well as decision and action may be necessary for plants subject to particularly hazardous situations in which an operator has too long a reaction time and, on the whole, 'too small a reliability.

Where it is possible to define a safe condition to which the plant may be brought in any circumstances through automatic action, the safety action can be automatized. To cover all situations such intervention must usually

be of a radical nature, for instance an emergency stop, and strict reliability demands therefore attach to the decision on which it is based. Consequently the designer must base his classification of the failure situations concerned on a simple criterion so that he can make sure that his classification is correct and can automatize the decision and action by means whose reliability may be assessed beforehand.

For hazardous plants these requirements often lead to safety systems that monitor selected parameters in the plant individually by means of redundant measuring channels and automatically close down the plant when a fixed limit for any of these parameters is exceeded. In such plants the decision is simple; therefore reliability models may be made that allow evaluation in advance of the effects of "fail-safe" dimensioning, of duplication a more advanced redundant couplings and of different maintenance and testing procedures.

To-day such models exist particularly for relay systems and certain types of semiconductor logic in which failures are attributable almost exclusively to faulty information to the decision function, the decision logic being contained in the cabling structure. For the majority of semiconductor logic circuits it is still difficult to work out models because failures in the semiconductor elements lead to often complicated and unforeseeable failures in the decision logic. 3)

It is usually necessary to make a quantitative assessment of safety systems on the basis of failure statistics for the components used since the reliability demands on the total system will correspond to a failure frequency so low that it cannot be verified by testing within a reasonable time.

Because of the radical interference with the operation by such a safety system and the economic consequences, it must only enter into operation when absolutely required. Therefore it is normally necessary to supplement it by a system based on a much more differentiated classification of the failure possibilities and a corresponding group of control actions whose effects on the operation correspond to the importance of the failure types. As the frequency of the more radical control actions may thus be reduced, the operation of the plant will be less affected.

However, the much more complicated decision and action require more comprehensive and hence more vulnerable equipment, which further means that it is more difficult to evaluate the reliability in advance. At the same time the designer will have greater difficulties in giving a covering classification of the relevant possibilities of failure, their operational consequences and their data patterns for use in the desire of an automatic decision function.

The uncertainty of the designer's classification is to some extent counteracted by the fact that a missing or incorrect control action at a low level may give rise to a more effective control action later in the development of the failure situation. For a similar security to be obtained against failures in the more comprehensive data processing required in the decision function there must be a reasonable degree of independence between the equipment used for the different types of action. In the case of a fairly detailed classification such separation is impossible, alone on account of the internal coupling between the individual failure patterns, and the data processing capacity required for large plants is so great that it may pay economically to use a digital computer.

For these reasons a monitoring system with a highly differentiated influence on the operation of the process plant may be so vulnerable as to necessitate an alternative monitoring possibility. It may be obtained either by comb:L-iinl the system with a higher-level, more simple and independent safety system or, in the system itself, by co-operation of several digital computers. The latter choice may soon be made attractive by the price development taking place for small computers. Another possibility, often suggested, is to introduce automatic testing equipment for the monitoring system, which may secure the process when it detects failures in the monitoring function. In many cases, however, this simply means that the reliability problem is transferred to the testing equipment.

For differentiated automatic changes in the state of operation of the process plant - as countermeasures - to be possible, the normal control equipment must in most cases be capable of controlling the plant during changes beyond the normal operational range. The intervention may then take the form of a change of references in the control equipment provided the failures are not located in this equipment. Thus it is expedient also for this reason to have decentralized control equipment.

In view of the problem it is for the designer at the present stage of development of automatization to make in advance a sufficiently detailed analysis of the response of the process plant to possible failure situations, the decision in the monitoring system for the more differentiated kinds of intervention in the operation is usually left to an operator.

Irrespective of the intervention being automatic or manual, rapid and automatic localization of the failure may be an advantage since the localization that is a condition for repairs may be difficult and time consuming once the intervention has altered the state of operation.

MONITORING BY THE OPERATOR

For the reasons indicated in the foregoing, the monitoring of a process plant is usually arranged as follows. A rather simple automatic safety installation controls a few selected parameters and secures the operation by radical intervention such as emergency stop when a few well defined and hazardous situations arise in the plant. As regards the more differentiated monitoring, instrumentation detects the abnormal conditions, and an operator evaluates the situation and decides the action to be taken.

The decisive advantage of an operator is his ability, in a failure situation, of generating detailed information himself by virtue of his understanding of the nature and mode of operation of the plant. His greatest disadvantage is that his reaction speed and information capacity are limited. Further he may be unreliable in his decision., being apt to base it on his everyday operational experience; thus he may, as shown by experience, interpret a complicated failure situation as a coincidence of more trivial and frequent failures, e. g. instrument failures, while serious, but rarely occurring situations ought to be given absolute priority in his assessment.

These drawbacks of the human operator may to a very great extent be off set by the design of the means of communication between operator and instruments and by an appropriate data reduction in the instrumentation. Likewise, the instructions and training, which, as it were, programme the operator for his intended functions, have a great influence on the reliability of his decisions.

The operator's limited input capacity for detailed data must be efficiently utilized. This means that the information to be imparted to him in an abnormal situation must be coded in such a way as to enable him quickly to survey the operational situation. For the decision he is in need of a quick estimate of the relation between sets of data rather than of accurate individual data; in this situation an appropriate coding will be in the analogue form, graphs that show the relevant relation directly. Through a suitable display arrangement, including e. g. display on a picture screen (cathode-ray tube), the resigner may make sure that the operator pays attention, in his evaluation and decision, to selected and covering sets of data. However, the designcr must not prevent the operator from having access to selected and accurate data for the evaluation of unforeseen situations. Such access is immediately possible in conventional instrument systems with simultaneous display on many instruments; in the case of --cmputer-controlled display the operator must have the same easy access to detailed data, for instance by means of a light pen in connection with the survey displays in cathode-ray tubes mentioned above.

In view of the uncertainty of the operators decision the designer will find it attractive to utilize the, data-processing and storage capacity available in digital computers to support the understanding of an abnormal situation which the operator ought to have from his instructions, but which may not be present to his mind. This can be done by an automatic analysis of measured data and a comparison with data patterns for a classification of foreseeable failure situations worked out by the designer.

It is hardly expedient to work out this analysis in the same way as if automatic intervention in the operation were the aim, that is so that it ends in the selection of a detailed failure situation and in a direction to the operator as to the appropriate countermeasure. That the designer wants the operator's assistance and evaluation of the situation may be due to a feeling that his functional analysis in uncertain, and if the automatic analysis is made in such a way as to point selectively at the most probable cause of failure, it may block the awareness and inventiveness of the operator, the very qualities it is desirable to utilize.

If the operator is wanted to make the decision he must feel qualified and responsible, not a mere link in an automatic procedure. Therefore the automatic analysis should support his natural method of work, that is, it should be used for an examination of the more trivial failure possibilities of which, as the most probable, the operator will first think in a given situation. If the results of this analysis are quickly and clearly presented to him in more serious situations, he will the sooner turn his attention towards more complex and hazardous possibilities. It is essential that the communication to the operator is clear and efficient, which is achievable by appropriate design of conventional alarm tableaus. In the case of computer-controlled display, textual information on a screen will be more suitable than information by typewriting or table printing.

In designing instrument systems for complicated process plants the designer is thus faced with the choice of counteracting an abnormal operational situation by incorporating automatic protective intervention in the instrumentation system or by ensuring correct intervention on the part of the operators through training and instruction. This choice is rendered difficult especially by the very limited general knowledge of the reliability of operators' decisions and the possibility of improving it by advanced data processing in the instrument system, and further by the shortage of generally formulated knowledge of the reliability of instruction systems.

Therefore the change in the structure and functions of instrument systems that is made possible by digital computers, with their great flexibility and data capacity, must rely on a realistic formulation of the tasks and properties of systems and operators based on the knowledge implicit in the tradition that has developed for more conventional instrument systems. The

use of the digital computer in automatization must therefore not be in the nature of a break of the more conventional tradition, but must be a harmonious development on a technological basis with greater possibilities.

ACKNOWLEDGEMENTS

This report has been prepared on the basis of material used for the establishment of the general lines of the reliability and system studies in the Electronics Department. The author wants to thank his colleagues P. Timmermann and K. B. Hansen for inspiring discussions and Fl. Steenbuch for translating the report into English.

REFERENCES

1.

An interesting attempt at establishing realistic criteria for safety demands on plants involving the risk of injury to persons is described in E. Sidall, Statistical Analysis of Reactor Safety Standards. Nucleonics 17, No. 2, 64-69 (1959).

2.

Surveys of various types of adaptive control systems, as well as further references, are to be found in a number of textbooks and articles, for instance: Review of Adaptive Control System Theories. C. T. Leondes (editor), Modern Control System Theory (McGraw-Hill, London, 1965).

3.

An elementary introduction to the properties of redundant systems and their dependence on maintenance procedures is given e. g. in J. Rasmussen and P. Timmermann, Safety and Reliability of Reactor Instrumentation with Redundant Instrument Channels. RisZ5 Report No. 34 (1962).

A more thorough treatment, with a comparison between a number of recent publications and a list of references, may be found in P.

Timmcrmann, Improvement of Reactor Safety System Reliability by Means of Redundancy. Nuclear Electronics Conference Proceedings, Bombay 1965 (IA-EA, Vi--nna, 1966).

4.

Learning systems and their properties are dealt with from several angles in a great number of publications. From the reliability point of view the following articles are illustrative:

B. Widrow., W. F. Pierce and J. B. Angell, Birth, Life and Death in Microelectronic Systems. IRE Transactions on Military Electronics, 191-201 (July 1961).

D. R. Moore and A. C. Speake, New Learning Machines for Future Aerospace Systems. New Scientist (10 March, 1966).