00 52 34 04 11 07

Control System Design and Diagnostic Techniques for Improving Total System Availability

M A Keyes IV
President & C E O
Bailey Controls Company
Wickliffe, Ohio U S A

D. J. Dziubakowski,
Sr. Control Systems
Consultant
Bailey Controls Company
Wickliffe, Ohio

M P Lukas,
Manager,
Applications
Wisdom Systems
McDermott, Inc
Chagrin Falls, Ohio

Presented at
15th Annual Advanced Control Conference
Purdue University
West LaFayette, Indiana
September 11-13, 1989

Bailey®

Technical Paper

TP89-6

00 52 36 04 11 07

CONTROL SYSTEM DESIGN AND DIAGNOSTIC TECHNIQUES FOR IMPROVING TOTAL SYSTEM AVAILABILITY

by

M A Keyes V
Pres dent & C E O
Ba ey Contro s Company
W ck ffe OH

D J Dz ubakowsk
Sr Contro Systems
Consu tant
Ba ey Contro s Company
W ck ffe OH

M P Lukas
Manager
App cat ons
W sdom Systems
McDermott nc
Chagrin Fal s OH

0 INTRODUCTION

Tota systems availab ity of an industria plant s a function of process equipment reliability contro system equ pment reliabi ity, and the t me needed to repair both categories of equipment The design and application cf control systems in an industria plant can have a ma or mpact on total availab ity of the p ant in severa ways This paper describes this mpact in the fo low ng areas and provides examples or a part cu ar class of distributed control systems

- o Use of redundancy to max mize control system availab lity
- o Se ecting control and safety strategies that are appropriate for the process con iguration
- o The role of control systems n se ecting and implementing the best maintenance strategy for the plant
- o The use of expert systems n detecting inc pient failures and diagnosing those that have already occurred

) SIGN OF I GH RELIABILITY CONTROL SYSTEMS

Ove ie past several years tiere has been ic c sec iterest in h ig contro a id monitor ng cc t ic it w t h gh re ab ty a id c ava lability It gc ic cc g ized id ag eed that gh c l ty id availab ty are des rable qual ties, but iv e g ice s do not know specifica y what c l ty id ava ab ty are Webster defines c) ty is t to be re ed on a id ava l bility as c c ng a be ic a e lec

M c lc na v rel ab l ty re ates to its c ty the p bab ty that the system w c n s tisfactorily for t east a given period c t c en used under stated cond tions (See c ence) Stated mathematically

Re ty c MTBF

w ie c t mission (or operat ona) t me MTBF Mean c Between Fai ures

The mission t me is se ected to be either the cc e l t (5 to 20 years or more) or the t ie between sc edu ed equ pment outages (genera ly once every or once every two years) The value c se c epends on the purpose o the ana ysis For t c n sons we w l use a two year period

Ava ab l ty relates to whether the device (or devices) w be operational at any given instant of t c t e prob l ty t iat t ie system s operat ng c t y at a iy po it n t me when used under st c c ic t o is w iere the tota t me cons dered gc ic v i ic udes operat ng time and active repa r ne id some cases adm nistrative time and g s c t me (See Reference 1) Kececiog u urther de ies d n strat ve time as that portion of down ie not ic uded under act ve repair t me and g st c t ine and og stic t me as that portion o dow t ne du ng which repa r is de ayed sole y bec use of t ie necessity for waiting for a ep c ne it part or ot ier subd v s on o the system Mathematically

$$\text{Availabil ty} = \frac{\text{MTBF}}{\text{MTBF + MTTR}}$$

where MTBF Mean Time Between Fa lures
MTTR Mean T me To Repair

Control systems can be categorized nto two major groups those that operate continuously (cont nuous systems) and those required to operate nter n ttent y (as batch systems) Batch systems genera ly have a mission t me that encompasses t ie batc i durat on p us charging, discharging, and f necessary clean ng or purg ng t me We wi l discuss on y continuous systems

A simp e control system m ght be composed of o ie or two control loops requiring I/O (input/output) modules, processor modules, mounting racks, and power supp es A pictor al diagram for this system is shown in Figure 1 1 The success diagrams are shown Figures 1 2A & 1 2B This system wil prov de the basis for al compariso is that fo low ns such t is ass gned a relative (availability, reliab l ty, & cost) value of unity

To e ihance the rel ab lity, a second power modu e can be added, as shown in F gure 1 3 When computing the rel ability, repair is permitted so ong as the loop can continue to perform its intended function. The next steps include adding redundant processors (Figure 14) and redundant I/O modules (Figure 15). The redundant processors include a high reliability (700+ year MTBF) link between them. The data transfer includes CRC (cyclic redundancy checks) and error checking.

Two other approaches should be considered first: a 1 out of 2 system with selection logic (Figure 16). This approach is configured to provide a higher reliability than a simplistic two channel system with selection logic, because the normal approach has the selection logic as a single point of failure. The system evaluated here includes independent operating channels with only a high reliability (100+ year MTBF) selection logic between them. The output values can be checked for validity before being sent to the final control device. The second approach to be considered is a 2 out of 3 system with selection logic (Figure 17). The 2 out of 3 system features three independent channels which compute their own control outputs and [illegible] other channels' values before selecting a [illegible] output. The proposed output is verified with [illegible] channels before being output.

A comparison of the MTBF, normalized to the simple loop (Figure 12B), is shown in Figure 18. A [illegible] of the configurations [illegible] new [illegible] modular power system [illegible] available (purchased) [illegible] used previously. Figure 19 shows the [illegible] and the impact of the new [illegible] new power system is 2.4 times [illegible] and 1.75 times more efficient) than [illegible] system. This is a direct result of design [illegible] data reporting system which [illegible] components for the equipment repaired in [illegible] Figure 10 lists [illegible] capabilities.

Today's microprocessor based controllers can handle vastly greater numbers of loops than earlier [illegible]. To increase the size of our original system [illegible] adding I/O modules (one for every two outputs) up to a total of 64 I/O modules (128 outputs). Assume, for example, that there are 5[illegible] in the process segment and no more than 2 [illegible] I/O card. This results in a system, [illegible] Figure 12B consisting of 25 I/O cards [illegible] processor card. To ease comparisons, we will assume that inputs & outputs must be operational for [illegible] to be operational. Figure 11 shows a [illegible] for the various cases.

Several other configurations or adaptations are possible, but, in most cases, they result in little, [illegible] even negative, improvements in reliability/availability. Some reliability gains can be [illegible]. For example, the use of [illegible] in which the bottom of a bus is connected to the head end with additional wiring is sometimes [illegible] used. The additional connections and wiring can offset the reliability gain from the installation of the [illegible]. The base (single) communication bus has a [illegible] 0.999333 (2,998 year MTBF), whereas [illegible] communication bus with a bus loop has a [illegible] 0.99937[illegible] (2,940 year MTBF), a net [illegible] were added, redundancy [illegible] would increase to 0.99[illegible]555 (4,497 year MTBF).

An area often discussed by manufacturers or purchasers of microprocessor based control equipment is that of software reliability. One approach (used in the space shuttle, for example) is to use several processors all running different software independently designed to solve the same problem, and doing this it is felt that an undiscovered fault in any one version of the software will affect only one processor. The system [illegible] specialized applications, but is not cost effective for most industrial applications.

[illegible] to generate a library of [illegible] which can be easily linked together to [illegible] the required control action. In this way the library can be verified to be error free. It is commonly accepted that even supposedly error free software can result in a failure situation. The next best thing is to continuously test the software in various configurations to determine problems. [illegible] software that is operating in 1000 [illegible] applications for a one year period (1000 application years) has demonstrated higher reliability than software having 100 application years of operation. Similarly, 1000 application years would be better than 100 application years, and so forth.

[illegible] STRATEGIES TO MAXIMIZE PLANT AVAILABILITY

PLANT REDUNDANCY STRUCTURE

A typical industrial plant takes several inputs or feedstock streams and converts these raw materials into one or more outputs or product streams. For example, a power generation plant converts a fuel such as coal or oil into electricity and waste solids and gases. Each plant is composed of a combination of parallel and series sets of equipment such as the simplified power plant shown in Figure 2. The plant is considered to be available from a reliability point of view if it is successfully fulfilling its design objective, which is to convert its inputs to outputs at an acceptable level of throughput and cost.

The degree of redundancy in the plant equipment and the way in which this equipment is [illegible] that a [illegible] plant [illegible] equipment is duplicated if multiple units are required for capacity purposes or the equipment is inherently unreliable. Plant equipment is not duplicated if it has a large enough capacity to meet plant throughput requirements, especially if it is very expensive. In this case it must also be designed and operated for high [illegible]. In the example given in Figure 2, the pulverizers that grind the coal into a powder that can burn in the boiler are duplicated for both capacity and reliability purposes; however, the [illegible] generator [illegible] not duplicated because they can handle the desired plant capacity and they are very expensive.

IMPACT ON CONTROL AND MONITORING STRATEGY

The proper strategy for monitoring and controlling each piece of plant equipment varies, depending on its impact on overall plant availability. In the case of duplicated equipment, the best approach generally is to monitor and control each piece of equipment in such a way that it does not malfunction and (possibly) cause the failure of other plant equipment. A good strategy in this case is to simplify the structure of the control and monitoring systems and to design them so that they shut the plant equipment down in case of an actual or impending failure. There is probably no need for redundant controls or complex failure monitoring or prediction systems. Since the plant can run despite a single failure, when in doubt shut it down!

In the case of a major piece of plant equipment that is not duplicated and must work for the plant to continue operation, the best approach is to try to keep the equipment running at all costs, even at reduced capacity. Highly redundant control systems and more complex and extensive monitoring, may be justified to minimize downtime of this critical piece of equipment.

Of course, more extensive control and monitoring strategies may also be justified if the failure of even a duplicated piece of process equipment can have a major effect on other plant equipment or plant personnel. For example, it may be wise to monitor and control a coal pulverizer very carefully, since if it explodes it can kill people and damage a major portion of a power plant.

As the control system becomes increasingly complex, several attributes of modern microprocessor based, distributed control systems can be exploited. These relate to the physical and functional separation capabilities. It is no longer necessary to concentrate the computing power in a central location. Processors or I/O can be located remotely at the field junction boxes or marshalling cabinets. *This not only reduces the wiring costs but* also the cost of the central control building (fewer control enclosures need to be housed and wired). It also adds an incremental increase in reliability, *because fewer connections and pre processors are* required. In addition, a loss of the plant's communication system will not affect a node's ability to communicate with its own I/O, nor its ability to *provide control (execute its control algorithms).*

The functional distribution capabilities provide the ability to dedicate a processor to a single *process unit or group of units. As a result, the* impact of the failure of a processor or power system can be restricted to a known subset of equipment. This partitioning, as it is called, permits a subgroup of control hardware with perhaps, *a higher level of* redundancy to be dedicated to a process unit to provide the required reliability. Control for multiple, parallel auxiliary units (such as pumps, heat exchangers, valves, etc.) *can benefit from the* reduced cost of reduced reliability control hardware configurations (less redundancy). Conversely, it is more cost effective to increase the reliability of the control portion of the control/auxiliary equipment combination, if by doing so will permit the reduction by one (or more) of the required quantity of auxiliary units. For example, if three parallel pump trains are required to meet reliability criteria, it may be possible to increase the reliability of the control hardware (and perhaps the pumps themselves) sufficiently to permit 2 pump trains to satisfy the original reliability criteria. The resulting savings of the third pump train in terms of capital cost, replacement parts, and maintenance (manpower) cost over the life of the plant can be significant.

PARTITIONING FOR ADVANCED CONTROL

Substantial improvements in reliability (and security) result from performing a function or control algorithm at the lowest possible level in the hierarchy to minimize the number of elements between the process and the controller. Using a mini computer in combination with the control system to perform advanced control strategies can only achieve reliabilities of approximately 7 percent (MTBF 6700 hours), whereas a separate control processor operating with the same control system has a reliability of over 85% (MTBF > 100,000 hours). Therefore, advanced control algorithms and supervisory set point calculations should always be done at the processor level, or at very least at the process control unit level. (See Keyes, 1982)

PREVENTIVE AND PREDICTIVE MAINTENANCE TECHNIQUES

Most industrial plants have put in place a preventive maintenance program, in which items of plant equipment are checked and repaired regularly, usually on the basis of elapsed calendar or operating time for the item of equipment. In theory, this approach should increase the availability of plant equipment because the maintenance operations should catch many potential problems before they occur. Unfortunately preventive maintenance programs in practice often fall victim to budget cuts or are not managed properly (e.g., due to poor record keeping on the work done on the equipment). Even when implemented according to plan, preventive maintenance programs can be inefficient due to over conservative schedules and repair plans. The actual wearout cycle of equipment never matches the theoretical cycle, and therefore unneeded work may be done and perfectly good parts are replaced.

A better approach is one called predictive maintenance. In this approach, a distributed monitoring/control system is used to monitor key parameters that determine the wearout/failure status of a piece of plant equipment. Using past history of the behavior of these parameters, the monitoring system regularly predicts the future time at which that piece of equipment is likely to fail. Well in advance of that time, the monitoring system warns plant personnel that a failure is imminent, and provides the plant maintenance personnel with two options: a) take that piece of equipment off line and perform maintenance now, or b) wait until the next scheduled outage to make the fix. In both cases the monitoring system can provide some estimates of the economic consequences of the options and let the plant personnel make the best choice on an informed basis.

Some of the techniques from the field of SPC (Statistical Process Control), such as trend rules or pattern tests, can be used to make failure predictions. Statistical Process Control is based on the fundamental principle that there is a normal, predictable level of variation in every process measurement. This variation includes both random variation and variation which can be attributed to specific causes. Any significant change in normal variation may be the result of process changes or equipment changes. Two parameters are evaluated by the distributed control and monitoring system: X-BAR is the moving average and R is the range of the individual values (of X) in a subgroup (R = Maximum X minus Minimum X). From these the system establishes the boundaries of the normal variance of the parameter (X). Zone C is defined as the area from the mean to plus (or minus) one sigma level. Zone B is the area from plus (or minus) one sigma to plus (or minus respectively) two sigma. Zone A is the area from plus (or minus) two sigma to plus (or minus respectively) three sigma. Seven commonly used pattern tests are shown in Figure [illegible]. See Reference [illegible] for further details on SPC. When one of these patterns is detected the system normally alerts the Operations department to the alarm in order to determine the cause: a change in the process or the equipment. The alarm may also be passed to the expert system for further evaluation as discussed in Section 4.

It should be noted that adding more redundant equipment (either process equipment or control hardware) will increase plant availability. However this approach will also increase the overall number of failures or potential failures of plant equipment since there is simply more equipment to fail and maintain. As a result not only will the capital cost of the plant increase, but so will the cost of maintenance and the required spare parts inventory. The plant designer must make the proper economic trade-offs to maximize the plant's overall return on investment, taking these factors into account.

3 ROLE OF MEASUREMENT & CONTROL SYSTEMS

Increasing the reliability of the control system increases the reliability of the overall system to a point. To continue to achieve reliability improvements the sensors and prime movers must be upgraded also. Generally this involves selecting more reliable sensors or establishing *redundant* sensors or measurements. Redundant sensors should be connected to independent measurement points (such as separate taps for differential pressure measurements). The sensors are connected to independent I/O cards, the processors do a continuous comparison and alarm on significant deviations. On occasion rate of change monitoring is used; high rates of change can be used for alarming but caution should be exercised in using them to trigger alarms or taking action on assuming transmitter failure. Experience has shown that a high rate of change may be the result of an abnormal upset that the process and control engineers hadn't considered in their design analysis. In most cases I/O cards have been specified with high common mode rejection. *Common mode rejection* specifications are actually specifications for input filtering. (High common mode rejection and fast response are opposite ends of the same spectrum.) For a rate of change monitor to be effective it must be set slower than the input filtering (common mode rejection), but faster than the fastest possible transient of that measurement.

Some engineers will transfer the control loop to manual on a large rate of change assuming a transmitter failure will trigger the rate monitor. In this situation, the transmitter failure action may be inappropriate for the existing circumstances. Transferring a loop to manual during a transient can result in major upsets and, in many cases directly result in the loss of a process unit (trip or other safety action). For these reasons rate of change monitoring is generally restricted to (low priority) alarming. When a measurement is critical other techniques are used.

Multiple transmitters are employed (usually three) with an arbitrating method (2 out of 3 voting or median selection) used to establish the correct value. A computed value (using other parameters) is used to validate the transmitter value. In some cases the computed value is substituted for the transmitter value when the transmitter value is known to be invalid (e.g., *out of range*). Multiple transmitters increase reliability and availability but also increase maintenance and repair costs; however, the use of a computed value, using existing measurements, increases reliability and availability at *minimal* cost (thereby saving the expense of extra transmitters).

As we strive for higher reliability, we must be vigilant in monitoring the cost of each increment of reliability. In a few cases the consequences of the loss, for example, require larger capital investment in higher reliability systems. Emergency shutdown and fire (fighting & protection) systems require a commensurate level of reliability which are achieved through partitioning providing single loop integrity or at minimum functional integrity. Single loop integrity is the highest form of partitioning guaranteeing that any one loop cannot and will not affect the operation of any other loop. Similarly, functional integrity provides for separation of functions such as fire pump trains. This allows operation of each pump train independently of the others. Common equipment such as a building halon system is separate and independent from the fire pumps.

A relatively simple method to determine the cost benefit ratio of increased reliability is to determine the dollars per MTBF for each different configuration. A comparison can be made and the incremental cost of the improved reliability can be readily determined. For our purposes the D

Ratio (dollars per MTBF) will be normalized using the single loop system as a base of one. As can be seen in Figure 31, adding a redundant power supply is cost effective because it drives these D Ratio below 1.00. The most cost effective system, based on the figure, is the 1 out of 2 redundancy. Figure 32 shows the similar comparison for the 50 loop system previously described. For the single loop system the most cost effective system is Case V: 1 Out of 2 Redundancy whereas, for the 50 loop system it is Case IV: Redundant Power Processor & I/O Modules.

AUTOMATION OF RELIABILITY ENGINEERING PROCESS

Today, the proposal, design and implementation of distributed measurement and control systems to meet a required level of availability is a tedious, time consuming process. Generally, the engineer responsible for these systems must first lay out a trial configuration, then do the reliability and cost analysis to see if that configuration is acceptable. The analysis is usually done by hand, or at best with a spreadsheet program. If the configuration is not acceptable from either a reliability or cost point of view, the engineer must try another configuration and redo the analysis. Needless to say, once the engineer finds a configuration that meets the availability specs, he or she will not usually bother to look further even though there may be another solution that has a lower cost. There simply isn't time to find an optimal configuration.

Fortunately, engineering automation tools based on artificial intelligence technology have been developed to allow automation of the equipment design and configuration process. One such tool, the Concept Modeler, is an object oriented programming system that is described in Reference 3. The Concept Modeler represents knowledge about a particular product or family of products in the form of a part subpart hierarchy of objects. An example of this approach for the case of automobile design is shown in Figure 33. The top level object is the automobile and the first level of subparts consists of the chassis, the drive train, the suspension system, the braking system, and the electrical system. In turn, the drive train consists of other subparts, such as the engine, transmission, drive shaft, and differential. Associated with each of these objects in the hierarchy is a set of attributes, such as size, weight, location, material type, and manufacturing cost. The value of each attribute can be a fixed quantity (such as a number or symbolic descriptor) or can be a function of the values of other attributes in the design. For example, the length of a connecting rod in the engine might be determined from a table lookup function that depends on the configuration of the engine block, the size of the engine, and the type of [illegible] used. Once these relationships have been set up for a certain class of automobiles (for example), the design of a specific automobile can be generated automatically by triggering the relationships with a set of customer specifications for that automobile (e.g. size, acceleration and braking capability, and handling properties).

This object oriented approach to representing an engineering design also can include reliability and maintainability information. Associated with each object in the design hierarchy would be a set of attributes that define the part's possible failure modes, the reliability figure associated with each failure mode, and the mean repair time needed to correct that failure mode. Then, the availability of each object in the hierarchy would be a function of the availabilities of each of its subparts, or at least of those subparts that are critical to the functionality of that object. Since both availability and cost information are included in the description of the engineered product, the designer can make the appropriate tradeoffs during the design process. Various alternative designs can be analyzed very quickly for their impact on total cost vs reliability vs performance, and the appropriate choice can be made immediately.

The use of the Concept Modeler to determine control hardware requirements from a set of specifications is nothing new and such a system is currently being installed. This system not only determines the best hardware complement for a given application, it outputs the physical requirements (size, power, heat dissipation, etc) for the chosen application. A natural extension of its capabilities is to provide reliability criteria and have it generate an equipment configuration meeting those criteria. The engineer could compare the two configurations to determine if he/she wants to pay the price for the reliability that is specified.

4 DIAGNOSTIC TECHNIQUES TO MINIMIZE REPAIR TIME

Most of the emphasis in designing for availability is placed on the MTBF component of the equation, that is, in minimizing the failure rate of the part being designed. However, the time needed to repair or replace a failed part (MTTR) also has a major impact on plant and control system availability. Part repair time has these components: 1) the time needed to determine which part has failed, 2) the time needed to obtain a repair or replacement part and obtain the required tools, and 3) the time needed to actually fix the failed part or replace it with a new one. The third factor can be minimized by following good product design rules, such as making the part accessible for repair, making it easy to remove without special equipment, and providing clear markings so it is clear how to reinstall the part (or better yet, designing it so that it can only be installed one way). Anyone who has worked on automobiles or home appliances, let alone process control equipment, knows that these product design rules are rarely followed to the letter.

Modern process measurement and control systems can be of great help in minimizing the first factor in the repair time equation — the time needed to identify the failed part. Most well designed distributed control systems have self diagnostic capabilities that detect failures in modules and other elements of the control system. These self diagnostic capabilities include the following:

1) Internal diagnostic procedures within each module that shut the module down or puts it in a safe state of operation if misoperation is detected. For example, the CPU in a microprocessor based module may be required to reset a watchdog timer periodically. If the timer is not reset properly, it shuts the module down and/or broadcasts a message that the module has failed.

2) The operator interface devices in a distributed control system periodically check on the operational status of other elements in the system, such as the communication subsystems, the power system, and the microprocessor based modules in the distributed system. Any detected failures are reported immediately to maintenance personnel.

3) Redundant communication or control devices periodically check on each other to make sure operation is normal. Some systems periodically switch the designation of primary and secondary elements in a redundant pair to make sure that the backup element is always ready to take over in case of a failure in the primary element.

4) Microprocessor based modules run periodic programmatic checks on the operational status of their subsystems, comparing results obtained with known correct results. For example, the module might perform certain memory write and read operations, output and input operations, or arithmetic operations to make sure that the associated hardware is working properly.

A complete description of these self diagnostic capabilities is provided in Chapter 4 of Reference 4. When a failure is detected, the distributed control system immediately reports the location and type of failure to the appropriate operating or maintenance personnel.

Equally important as the ability to diagnose a misoperating or faulty part is the ability to replace it on line and under power. To achieve these benefits, provision must be made to hold an output at its drive at high or low on a processor failure. In special high reliability multiple failures can occur, this hold or output drive capability should be provided even with redundancy. Other capabilities include the ability to use a hard manual backup to provide the output even if the entire system were to fail. This backup adds another level of redundancy. It effectively provides for a backup to an entire control loop. The effect of this backup device has not been included in any of the data presented in this paper.

Each facility has its own (sometime multiple) maintenance and repair philosophy. There is a hierarchy of possible strategies that can be used:

Condition based maintenance
Optimally planned maintenance
Planned maintenance
Periodic maintenance
Fix it when it's broke

As you move down this hierarchy, the overall costs increase due to the increasing costs of lost production and bottlenecking the plant.

A modern distributed monitoring and control system can also be very useful in detecting failures in process equipment. These can be either direct or indirect measurements. Examples of direct measurements are vibration and temperature monitoring to predict bearing failures. Indirect measurements include computing the frictional losses, determining the rod distribution, and monitoring for changes in the mean and variances in excess of the two sigma limit.

Another method is to use the AI capabilities in resolving causes of outages through the use of Ishikawa Diagrams (also called Cause and Effect Diagrams or Fishbone Plots). Some systems have embedded expert system capabilities that allow the user to program and run IF THEN diagnostic logic within the control system without any special computer equipment.

Another technique is the use of Optimal Production Control (OPC) to improve availability and reduce operating costs. The OPC system can be either computer or processor resident. The Preventive Maintenance Opportunity Prediction capability of OPC can optimize the production rate of bottleneck process units in a manner that will recover lost production resulting from (or accelerate production in anticipation of) maintenance outages at minimum cost.

5. CONCLUSIONS

Due to the complex nature of the availability question, there is more to improving total system availability than simply adding redundant elements to the process or its control system. If not done carefully, adding redundancy will simply add to the capital cost and maintenance requirements on the system without improving availability in a cost effective manner. There is a clear need to design the process, the control and monitoring systems and the diagnostic and repair philosophy to maximize system availability while keeping the capital and maintenance costs at an acceptable level.

In evaluating these tradeoffs, the systems engineer of ten will find that the design of the process is pretty well fixed by throughput and p... constraints. However, it is possible to take advantage of the powerful capabilities of the process control and monitoring systems to maximize the availability of the total process at a reasonable cost, through the following techniques

- o Redundancy. Use redundancy only where it has a positive impact on total system availability based on the cost benefit ratios involved in using redundancy
- o *Matching control system design to the process.* Remember that the goal is to keep the process operating, so select and configure control equipment accordingly (*don't overkill*: use only the amount and type needed)
- o Maintenance strategy. Use the power of modern distributed control systems to monitor current behavior of plant equipment and perform optimized maintenance based on total economic considerations
- o Expert systems. Take advantage of expert systems that are embedded in the control system to diagnose equipment failures and minimize the time needed for repair

REFERENCES

1. Kececiog u, Dr Demitri, Lecture Notes on Maintainability, Availability and Operational Readiness Engineering 1989

2. On Line Tools For Statistical Process Control (SPC) Application Guide AG 0000 911 11 Bailey Controls Company 1988

3. M P Lukas and R B Pollock, Automated Design Through Artificial Intelligence Techniques *Artificial Intelligence and Advanced Computer Technology Conference*, Long Beach, CA, May 4 6, 1988

4. M P Lukas Distributed Control Systems: Their Evaluation and Design, Van Nostrand Reinhold New York, 1986

5. Wadsworth, Harrison M, Stephens, Kenneth S, and Godfrey, A Blanton, Modern Methods For Quality Control and Improvement, John Wiley & Sons 1986

6. ...son, W Grant and Coombs, Clyde F Jr, editors Handbook of Reliability Engineering and Management, McGraw Hill 1988

7. SAMA Handbook PMC32 1981, A Guide For Process Measurement And Control Instrumentation Reliability Techniques, Scientific Apparatus Makers Association, 198

8. Reliability Guide For Design, Management, And Procurement Personnel Avco Corporation

9. Keyes M A & Kennedy, Dr J P, Application of a Modern Distributed Digital System to Energy Efficient Control of Distillation Columns, Second Conference on Control Engineering Newcastle, N S W, Australia, 1982

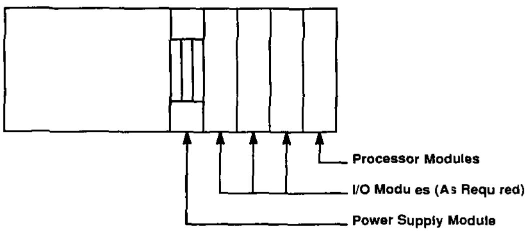


FIGURE 1 1

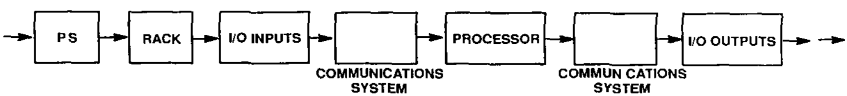


FIGURE 1 2A Detailed Success Diagram

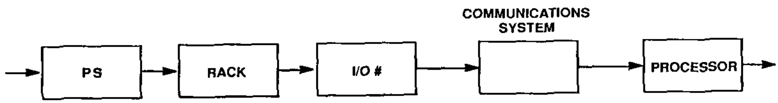


FIGURE 1 2B Simplified Success Diagram

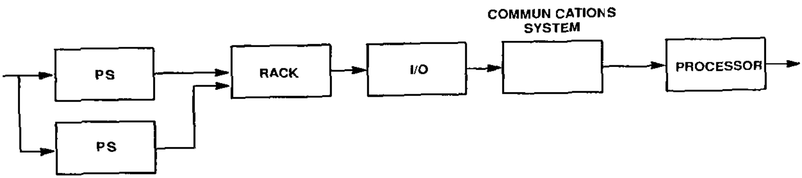


FIGURE 1 3 Redundant Power Modules

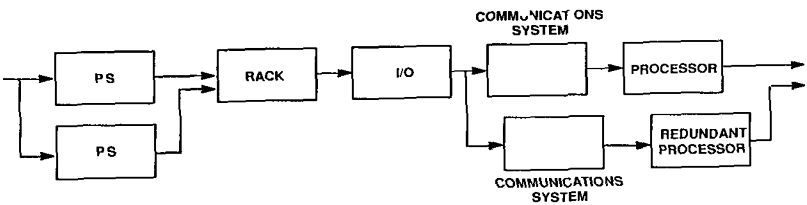


FIGURE 1 4 Redundant Power and Processors

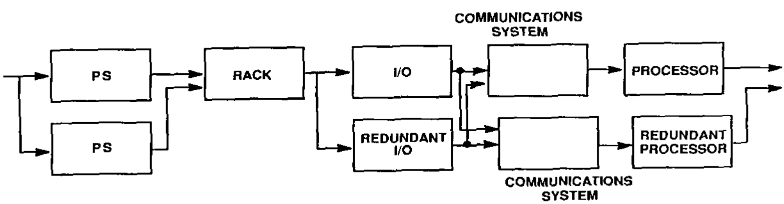


FIGURE 1 5 Redundant Power Processors and I/O

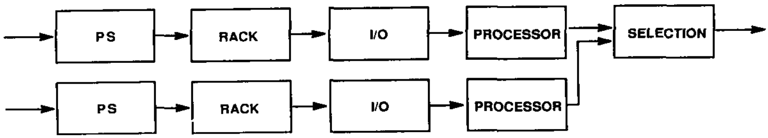


FIGURE 1 6 1 of 2 Redundancy

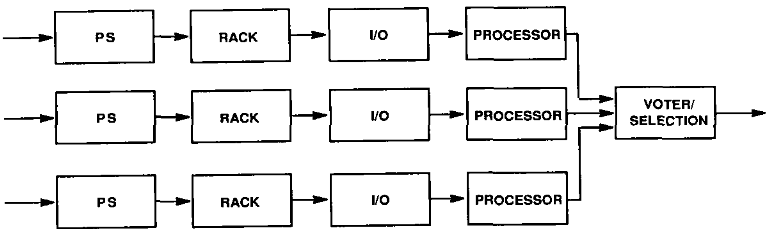


FIGURE 1 7 2 of 3 Redundancy

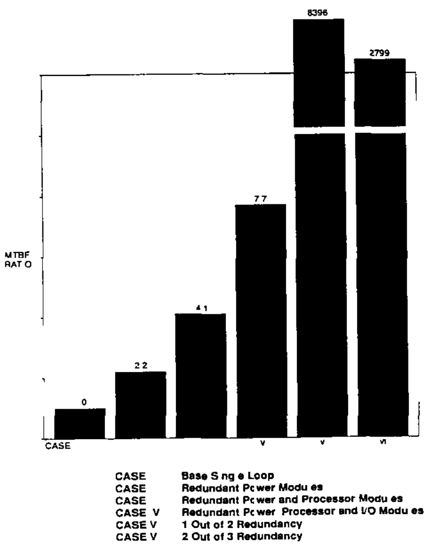


FIGURE 1 8

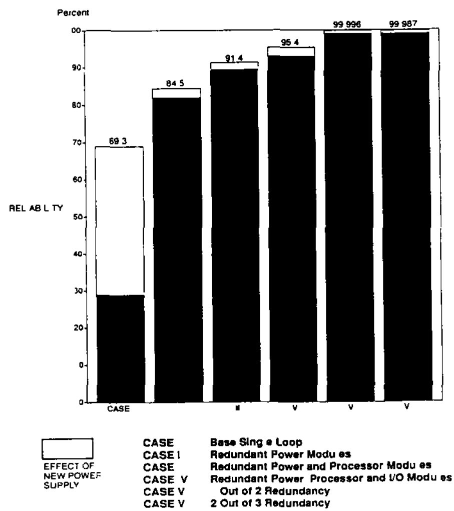


FIGURE 1 9

AVAILABILITY COMPARISONS

	AVAILABILITY
CASE Base S ng e Loop	99 99947693°o
CASE Redundant Power Modu es	99 99975929%
CASE Redundant Power & Processor Modu es	99 99987202%o
CASE V Redundant Power Processor & /O Modu es	99 99993231%o
CASE V 1 Out Of 2 Redundancy	99 99999000%o
CASE V 2 Out Of 3 Redundancy	99 99998000%o

FIGURE 1 10

RELIABILITY/AVAILABILITY COMPARISONS – 50 LOOP CASE

	MTFB RATIO	RELIABILITY	AVA LAB LITY
CASE Base S ng e Loop	1 0	0 2284224072	99 997759 3°o
CASE Redundant Powe Modu es	1 2	0 2784435265	99 99817687°o
CASE Redundant Powe & Processor Modu es	1 2	0 3013482181	99 99828959°o
CASE V Redundant Powe Processor & /O Modu es	43762	0 9999662595	99 99999998°o
CASE V 1 Out Of 2 Redundancy	209 2	0 99296834467	99 99999000%o
CASE VI 2 Out Of 3 Redundancy	11265	0 9998689377	99 99998000%o

FIGURE 1 11

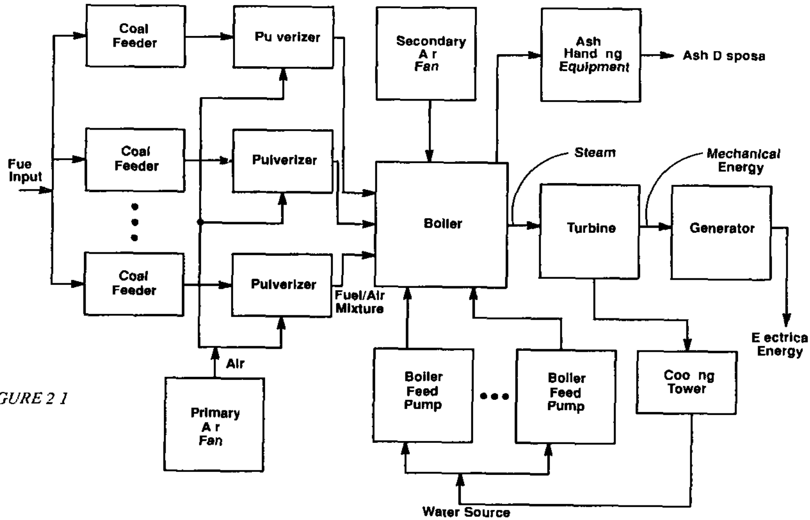


FIGURE 2 1

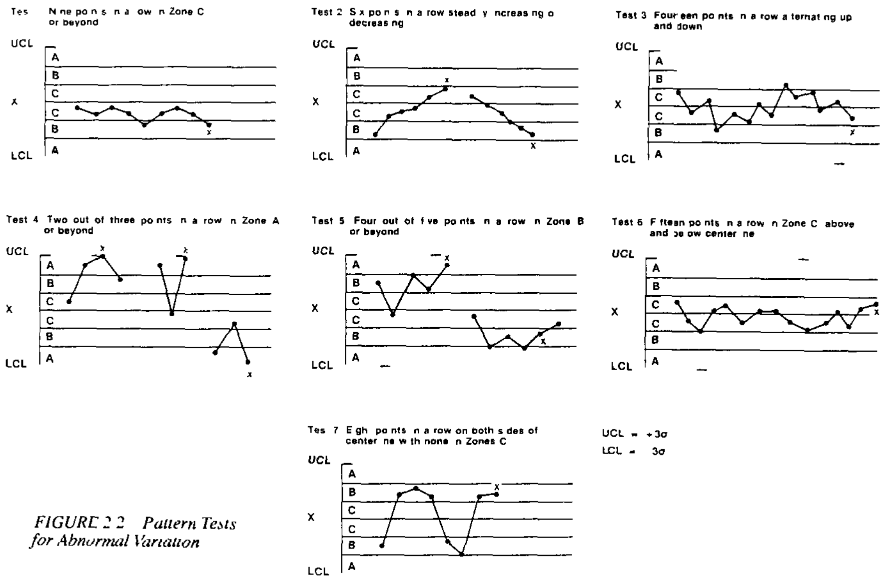
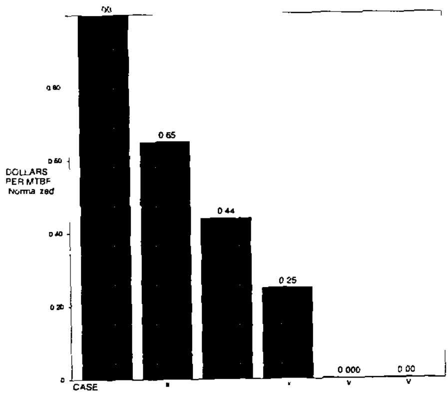


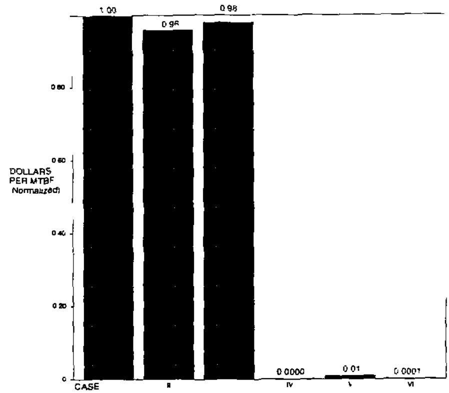
FIGURE 2 2 Pattern Tests for Abnormal Variation



CASE Base S ng e Loop
CASE I Redundant Power Modu es
CASE I Redundant Power and Processor Modu es
CASE IV Redundant Power Processor and I/O Modu es
CASE V 1 Out of 2 Redundancy
CASE V 2 Out of 3 Redundancy

COST FOR MTBF FOR S NGLE LOOP SYSTEM
(DESCR BED N F GURE 1 8)

FIGURE 3 1



CASE I Base S ng e Loop
CASE I Redundant Power Modu es
CASE I Redundant Power and Processor Modu es
CASE V Redundant Power Processor and I O Modu es
CASE V 1 Out of 2 Redundancy
CASE VI 2 Out of 3 Redundancy

COST FOR MTBF FOR 50 LOOP SYSTEM
(DESCR BED N F GURE 1 11)

FIGURE 3 2

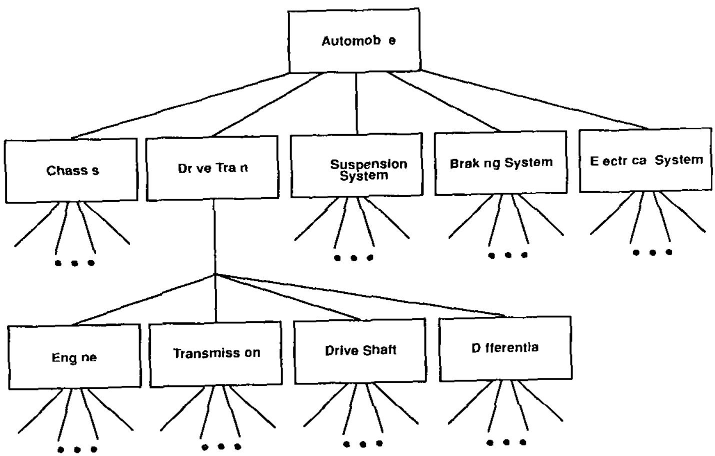


FIGURE 3 3

00 52 47 04 11 07

For additional copies, contact

Bailey Controls Company

29801 Euclid Avenue Wickliffe Ohio 44092 U.S.A. • (216) 585 8500
Telex 980621 • Telefax (216) 585 8756 or (216) 943 4609

Litho in U.S.A. 290