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
CONTROL SYSTEM DESIGN AND DIAGNOSTIC TECHNIQUES
FOR IMPROVING TOTAL SYSTEM AVAILABILITY

by
M A Keyes V
Presdent & C E O
Ba ey Contro s Company
Wck ffe OH

D J Dzubakowsk
Sr Contro Systems
Consulant
Ba ey Contro s Company
Wck ffe OH

M P Lukas
Manager
App catons
Wisdom Systems
McDermott nc
Chagrin Falls OH

0 INTRODUCTION

Total systems availability of an industrial plant is a function of process equipment reliability, control system equipment reliability, and the time needed to repair both categories of equipment. The design and application of control systems in an industrial plant can have a major impact on total availability of the plant in several ways. This paper describes this impact in the following areas and provides examples or a particular class of distributed control systems

- Use of redundancy to maximize control system availability
- Selecting control and safety strategies that are appropriate for the process configuration
- The role of control systems in selecting and implementing the best maintenance strategy for the plant
- The use of expert systems in detecting incipient failures and diagnosing those that have already occurred

1 REVIEW OF CONTROL RELIABILITY

In the past several years there has been increased interest in having control and monitoring systems with high reliability and availability. It is recognized that high reliability, availability, and maintainability are desirable qualities, but we do not know specifically what is necessary and available as we proceed on a best case basis.

Many improvements reliability relates to its assessment time period. The system is assessed over a specific period of time. Stated another way (See Table 1), a mission time is defined, and that time is divided into periods (See MTBF). The mission time is the period between failures.

The mission time is selected to be either the expected life time (5 to 20 years or more) or the time between reduced equipment outages (general 1 to 2 times a year or once every two years). The value chosen depends on the purpose of the analysis. For this discussion, we will use a two year period.

Availability relates to whether the device or system is operational at any given instant of time. Problems that the system is operating at any point in time when used under specified circumstances where the total time considered is the sum of the times operating and not operating, and time periods where the system is not operating. Availability is defined as the portion of down time during which repair is delayed solely by the necessity for waiting for another part or other subassemblies. The system is said to be available if it is operational and able to operate.

Availability = MTBF

where

MTBF = Mean Time Between Failures
MTTR = Mean Time To Repair

Control systems can be categorized into two major groups that operate continuously (continuous systems) and those required to operate intermittently (batch systems). Batch systems generally have a mission time that encompasses the batch duration plus charging, discharging, and necessary cleaning or purging time. We will discuss on continuous systems.

A simple control system might be composed of one or two control loops requiring I/O (input/output) modules, power supplies, and power failure A pictorial diagram for this system is shown in Figure 11. The subsystems are shown in Figures 12A and 12B. This system will provide the basis for all comparisons that follow as such it is assigned a relative availability, reliability, and cost value of unity.

To enhance the reliability, a second power module can be added, as shown in Figure 13. When computing the reliability, repair is permitted so one
as the crop continues to perform at intended levels. The next step in installing redundant processes (Figure 14) and reducing MILAce to Figure 6). The redundant processors include a hardware by (4.497 year MTBF), or a method of system with 66% less.(2.940 year MTBF) a net result of the space shuttle example is to use a different process or to run the system separately until it is clear that an MBF will test only one after the other. The system will be fabricated for all applications, but it will not replace existing industrial applications.

A typical process is described for the second approach to be considered, that is, a two-out-of-three system (Figure 7). The two-out-of-three system requires only the same amount of service as a single system. In this case, the redundant version is checked before selecting a point that is on a plot. The proposed output is verified when the error is less before the final output.

A two-out-of-three, the MTBF, normalized to 100 is shown in Figure 18. A two-out-of-three system is a configuration between 1,000 and 4,000 hours depending on purchased parts, cables, and the impact of the new power system. The new power system is 24 times more efficient than the old system. This is a direct result of design changes. After a data reporting system which will be a part of the equipment is required in this application. Figure 10 lists the outstanding properties.
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 tip off generally is to monitor and control each piece of equipment in such a way that it does not interact 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 fast-acting monitoring or protection systems. Since the plant can run despite a single unit failure, it is unlikely to shut 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 it 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 systems may also be justified if the addition of a duplication of plant 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 I/O junction boxes or marshalling cabinets. This does not reduce the wiring costs but also in the central control building (fewer control enclosures need to be housed and wired). It also adds an increased reliability, because fewer connections and pre-processors are required. In addition, there is a loss of the central communication system, which not only requires the ability to communicate with its own I/O, nor is it ability to provide control actions to other systems.

A better approach is a so-called predictive maintenance approach. 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 predicts the failure time with which that piece of equipment is likely to fail. Well in advance of the failure time, the monitoring system may take appropriate actions to prevent the failure from occurring. This can be done in one of two ways: either by reducing the reliability or by reducing the cost of equipment failure. Conversely, it is

...
s rated output to make the \( f(x) \). In both cases the controller can provide some estimates of the occurrence probabilities of the options and the percentages of best choice on an interval basis.

Some of the questions from the front end of SPC (Statistical Process Control), such as trend rules or p-values, tests can be used to make the system decisions. Statistical Process Control is based on a fundamental principle that there are significant changes in normal process changes or change in two parameters are evaluated by the control and monitoring system. The range of the individual values of the subgroup is the range of the data obtained by the unit. A common pattern is to use the moving range of the subgroup data. This is used to calculate the control limits for a process. The process is considered to be out of control if the data points fall outside the control limits.

It should be noted that adding more redundant systems or control devices increase plant availability. However, as the number of sensors or other process equipment or control devices increase, the cost of the system's reliability also increases, which is a critical factor in determining the cost and the lifetime of the system. As a result, the cost of the system's reliability must be balanced with the cost of the system's availability and the required spare parts inventory. The plant designer must make the proper economic decision to maximize the plant's overall return on investment by considering these factors.

ROLE OF MEASUREMENT & CONTROL SYSTEMS

Increasing the reliability of the control system increases the reliability of the overall system to a large extent. It is necessary to select the sensors or mechanisms that must be redundant in general, this involves selecting one of the redundant sensors or establishing redundancy. Redundant sensors are connected to independent measurement points (e.g., separate inputs or different pressure measurement heads). The sensors are connected to the control systems, and a decision must be made about which sensors or sensors should be used in a change of monitoring system. The change can be evaluated to determine whether it could be exercised in using measuring sensors or taking action or...
Ratio (do ars per MTBF) w1 be normalized using the single loop system as a base of one. As can be seen in Figure 3, adding a redundant power supply system has a positive effect because it drives these D Ratios to 100. The most cost-effective system, based on the gure, is the out of 2 redundancy. Figure 4 shows the system comparison for the 20 loop system previously described. For the single loop system, the most cost-effective system is Case V1 Out of 2 Redundancy whereas, for the 20 loop system, it is Case IV Redundant Power Processor & TDMs.

4 DIAGNOSTIC TECHNIQUES TO MINIMIZE REPAIR TIME

Most of the emphasis in designing for maintainability is placed on the MTBF component of the equation, that is, minimizing the failure rate of the part being designed. However, the time needed to replace a failed part (MTTR) also has a major impact on plant and control system reliability. Part replacement time is determined from the components of the system. Assumptions are made regarding the age, condition, and type of maintenance required, and the time needed to perform the task. Example: How long does it take to replace a motor? If the motor is located in a remote area, the time needed to get to the motor may be significant. The time needed to replace a part can be determined by summing the time needed to perform the task and the time needed to replace the part. The total time is the MTTR.
A complete discussion 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 a failure to the appropriate operating or maintenance personnel.

It is very important to diagnose a failure or fault in part so the ability to replace or repair under power can be achieved. This provision must be made to hold an output drive high or low on a processor failure. In some high reliability multiple failures can occur, so a dedicated redundant power system is required. Other capabilities include the ability to use a hard manual backup to prevent the output even if the entire system were to fail. A hard backup adds another level of redundancy. A dedicated power source for a backup to an entire control loop is often a necessity. This backup device has not been needed in many of the data presented in this text.

Each facility has its own (some are multiple) maintenance and repair philosophy. There are a variety of possible strategies that can be used:

- Condition-based maintenance
- Routine maintenance
- Total maintenance
- Shutdown when it's broke

As you move down this hierarchy, the overall costs decrease due to increased costs of lost production and downtime per 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 instrument and temperature monitoring to detect bearing failures. Indirect measurements include computing the fractional losses determining the distribution, and monitoring changes in the net and rates excess over the two

Another method is to use the AI capabilities to analyze causes of outages through test set analysis diagrams (so-called Cause and Effect Diagrams or Fishbone Plots). Some systems have embedded expert system capabilities that allow the user to program and run an IF THEN diagnostic code within the control system without any system computer software.

Another technique is the use of Optima Production Control (OPC) to improve availability and reduce operating costs. The OPC system can be either a computer or processor resident. The process is to minimize the opportunity to predict an out-of-control situation. The OPC optimizes the production rate of bottleneck process units in a manner that never results in production resulting from its decision. This is a philosophy of maintenance action at a minimum cost.

5. CONCLUSIONS

Due to the complex nature of the available test programs, the emphasis on adding redundant elements to a process control system if not done carefully adds redundancy without simply adding 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 control and monitoring system and design the layout and repair philosophy to maximizes zee system availability and to keep the capital and maintenance costs at an acceptable level.
In evaluating these tradeoffs, the systems engineer 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 power to capitalize on the process control and monitoring systems to maximize the availability of the total process at a reasonable cost, through the following techniques:

- **Redundancy**: Use redundancy only where it has a positive impact on total system availability based on the cost benefit ratio involved in using redundancy.

- **Matching control system design to the process**: Remember that the goal is to keep the process operating, so select and stage control equipment accordingly instead of using only the amount and type needed.

- **Maintenance strategy**: Use the power of modern distributed control systems to monitor current-behavior o plant equipment and perform optimized maintenance based on total economic cost calculations.

- **Expert systems**: Take advantage of expert systems that are included in the control system to diagnose equipment failures and minimize the time needed for repair.

---

Kececin u, D. Demitr. , Lecture Notes on Maintainability, Availability and Operational Readiness Engineering 1989

---

FIGURE 11

![Processor Modules](image)

![I/O Modules (As Required)](image)

![Power Supply Module](image)

**FIGURE 12A Detailed System 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
AVAILABILITY COMPARISONS

CASE
Base S-ng-e Loop

CASE
Redundant Power Modus

CASE
Redundant Power & Processor Modus

CASE V
Redundant Power Processor & I/O Modus

CASE V
1 Out Of 2 Redundancy

CASE V
2 Out Of 3 Redundancy

AVAILABILITY
99 99947693%
99 99975929%
99 99967202%
99 99993231%
99 99999000%

FIGURE 110

RELIABILITY/AVAILABILITY COMPARISONS – 50 LOOP CASE

<table>
<thead>
<tr>
<th>CASE</th>
<th>MTFB RATIO</th>
<th>RELIABILITY</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base S-ng-e Loop</td>
<td>1 0</td>
<td>0.2284224072</td>
<td>99 997759.3%</td>
</tr>
<tr>
<td>Redundant Power Modus</td>
<td>1 2</td>
<td>0.2784435265</td>
<td>99 99817667%</td>
</tr>
<tr>
<td>Redundant Power &amp; Processor Modus</td>
<td>1 2</td>
<td>0.3013482181</td>
<td>99 99825959%</td>
</tr>
<tr>
<td>Redundant Power Processor &amp; I/O Modus</td>
<td>43762</td>
<td>0.9999652595</td>
<td>99 99999996%</td>
</tr>
<tr>
<td>1 Out Of 2 Redundancy</td>
<td>209 2</td>
<td>0.9929634467</td>
<td>99 99999000%</td>
</tr>
<tr>
<td>2 Out Of 3 Redundancy</td>
<td>11265</td>
<td>0.9998689377</td>
<td>99 99998000%</td>
</tr>
</tbody>
</table>

FIGURE 111
FIGURE 2.1

FIGURE 2.2 Pattern Tests for Abnormal Variation