

REDUNDANCY - ASK THE RIGHT QUESTIONS

Understanding Redundancy

Redundancy Fundamentals

There are two concepts of redundancy when considering process and automation systems. These are:

- Process redundancy, i.e. storage capacity in a system
- Equipment Redundancy

Process Redundancy is the amount of spare capacity built into the resources or manufactured items in a system. Maximum downtime allowance for specific components within a system is often directly related to the process redundancy capacity. Maintenance staff are usually very clear about these requirements and deadlines. Examples include; the storage capacity in a warehouse, amount of water in a reservoir, volume of product contained in a pipeline.

Equipment Redundancy generally includes all of the infrastructure and software systems used for monitoring, controlling and reporting of a process plant or systems. It includes telecommunications and any transportation of resources required to facilitate normal operation, i.e. all non-process redundancy items.

The purpose of this discussion is to review a few key areas when designing equipment redundancy. Although not explored here, process redundancy should be considered at all phases of equipment redundancy as it may negate its need in certain circumstances.

Equipment Redundancy Components on Process Control & Automation Software Systems

Equipment used to monitor, control and provide information could include some or all of the following components:

- Telecommunication Infrastructure (PSTN, Fibre Optic, Radio, Cable)
- Information System Database and Web Servers
- Server and Workstation Equipment, including operating systems
- HMI software systems
- Distributed Control Equipment (DCS, PLC, & RTUs)
- Distributed Control Equipment embedded controller operating systems, configuration software and sequential logic code.

Systems are generally very complex in nature. What appears to be simple in concept in detailed form becomes extremely complex when redundant components are added.

The Basis of Redundancy

When doing detailed design, the level of redundant equipment should be considered for each component in the system. Each single point of failure should be reviewed and the consequences of failure. In addition to reviewing the likelihood of this occurring, the procedure to remediate the condition should be defined whether redundancy is going to be applied or not. The basis of all redundant component decisions determined during design should be documented thoroughly so that the wisdom gained about the system maintainability is trapped for further use.

Product suppliers at the very least should define under what conditions redundant components are actuated and returned to normal. It is worth investigating what parts of the system are compromised when operating in redundancy mode and if there are any performance trade offs.

Common Traps

Generally it is thought that a set of rules must be applied to fail a system over to the backup system. For example, if Condition A occurs, then use backup System. The assumption is often made if Condition A disappears, return the system to normal. This assumption has a number of problems. User interaction and the ability to interact with operational plant is the second dimension to be considered.

When a process moves to a condition that is abnormal, it may not be desirable to return the system to normal by reversing the action it took to get there in the first place. It may also be desirable to stage the return to normal process in time so that too frequent oscillation between primary and standby systems can be avoided.

A further input to management of redundant system is the operators and controllers who intercede or are required to provide input. Often it is mandatory to have users control the process of returning a system to normal after visual checks are made and certification processes completed. Even initially selecting failover to the standby system may require user confirmation. A strong advantage with having operator intervention is it prevents any scenario of systems hunting between primary and standby systems by the redundancy switching logic. Additionally it forces a verification process to occur that the original fault has been cleared or that the primary system offers a better solution than the standby system does. This type of intuition is often very difficult to imitate with logic controllers.

REDUNDANCY - ASK THE RIGHT QUESTIONS

Understanding Redundancy

Complexity

The return to normal process is by far the most complex undertaking in redundant systems. Often this is not understood and is therefore overlooked. The type or degree of redundancy should also be clearly defined by product suppliers and implementers. Sometimes the redundancy offered may not provide an acceptable solution. A few of many examples follow which highlight issues that are never black or white:

- Using dual CPU Modules on a PLC device sharing a common backplane bus. This offers a degree of redundancy for processing etc but under certain circumstances the failure of standby or primary CPUs may shut down the entire system.
- Relational Databases may be synchronised or replicated across the LAN connecting them. This may be prohibitively expensive. The remote gathering devices may be used to provide buffering of field data so that information can be recorded into databases after failures have been rectified. This is an example where the down time of the critical plant (database server and LAN) must be known and performance requirements met to retain system integrity.
- Radio Infrastructure and propagation conditions are often very difficult to duplicate. The optimum physical position for an antenna is normally chosen at the best possible location. A secondary position may not even be available for reliable communications. Therefore alternative communications media may be implemented for selective system components or additional cold swap spares allocated to maintenance staff to facilitate a rapid restoration of services.

Keeping it all together

Sometimes designs must be improved to remove the risk of failure rather than catering for what is considered likely. High quality components and more thorough testing may increase the confidence levels to a point that overrides the requirements to implement redundancy. Whatever the final design includes, it should at least contain the following:

- A description of the philosophy of redundancy for process and equipment.
- A definition of the user interface and the user's authority to change the process.
- Monitoring procedures for operation of redundancy and all component failures.
- Detailed workflow diagrams or descriptions of how standby systems are to be selected and the sequence for returning back to the primary system. This should be done for both automatic and manual operation.

