



The Hidden Vulnerabilities in Critical Power Supply Protection

Your building may be protected by redundant generators but that's only part of the power protection story. For business-critical power supplies, even if available generator power is N+1 or better, two risks are always present:-

- 1) In the event of a mains power outage, the control system may fail to operate the change over to generators, This may be due to either a component fault or an auxiliary supply fault.
- 2) Alternatively, in the event of such a fault occurring in the control system, the building may be instead, changed over to generators when there is no real mains failure at all.

The consequences of the first risk are usually disastrous, because it is extremely unlikely that a problem can be diagnosed and solved by site staff before the UPS batteries expire, and so all vital power is then lost. Although it would appear to be an obvious vulnerability, it is often overlooked by business continuity managers.

Occurrence of the second item is a lot more common than may be supposed, and is often caused by the failure of a PFR costing only some £50. Although all power is not lost, unnecessarily running on generators is insecure for the business, and correcting the cause requires the inconvenience of a shutdown in most cases.

Also, depending on the circuitry used, in many buildings a third risk is also present; that not only can a control fault disconnect the mains without reason as in (2) above, but no generator power can be possibly connected either, creating a disaster as great as for the first item, but without the need for a real mains failure to cause it. This particular scenario is totally unacceptable, but many buildings are still liable to it, even though it can be readily diagnosed and eliminated.

The solution:

The three fundamental methods that can be used to obtain reliability of any control circuitry are:-

- 1) High build quality and regular checks in normal (single) circuits to increase reliability. However, the risk caused by the many possible single points of failure is unchanged
- 2) Use of duplicated, or 'back-up' systems, which can in some cases eliminate a possible disaster caused by a single item failure
- 3) Use of triplicated systems, as is common in aircraft, to give total fault tolerance



1. Normal single circuits

It is often supposed that if a control system is regularly put to the test, then its correct operation when required is assured.

Not true.

The correct operation may be proven hundreds of times, but of course many items must operate correctly each time for the system to operate at all. These are the classic single points of failure. They include PFRs, relays, operating coils, and of course, most of all, the control circuit power supply. Here, the loss of a small fuse or a just one bad connection can cause total failure, not only of the change-over operation when required, but also in many cases can black out the entire building even when the supply is healthy.

None of these items is any more reliable after a proving test than it was before, so no real assurance at all is gained by regular testing. Indeed it could even be argued that to some extent repeated testing actually lowers the overall reliability since it stresses components and potentially reduces their life span.

Single points of failure are always a disaster waiting to happen.

2. Duplicated Systems

Suppose that every day you walked under a ten ton weight suspended by a stout rope. The rope is of course a classic single point of failure.

To reduce the risk to you

- The rope was tested carefully when the weight was first attached
- It is checked regularly for damage

You feel fairly confident ... But you would be much more confident if another rope was attached, capable of holding the weight if the first one broke. This sounds like the most sensible solution to single points of failure, because like using two ropes, if a control system element fails, then no problem; the back-up control system can be automatically switched in.

Unfortunately the comparison does not hold true because, when using a back-up electrical control, a fault in the first system must be detected before the back-up is switched in. This is a simple matter if the first system fails completely, but if a fault occurs such as an incorrect signal to the PLC from a faulty contact, (which is far more likely) then the first system will simply respond to that signal and therefore operate incorrectly, and the back-up will not be used at all, making the dual system totally ineffective.

If attempts are made to solve this by using the two systems at the same time, then a fault in one will produce a situation where one control system requires a switch to open, when the other will require it to be closed, and there is no way to identify automatically which one is correct.

In the 1960's during the early development of Aircraft Blind Landing Systems, many attempts were made to automatically tolerate faults in a dual system, by identifying the incorrect 'channel', and operate only on the correct one, but no satisfactory solution was found.

Only when a full triplex system was used to replace a dual channel system, was the problem solved, and triplicated systems are still used in all commercial aircraft today.

3. The triplicated power protection method - Triplex

The triplex method is the simplest way to tolerate faults, yet maintain correct operation, and as mentioned is usually associated with complex aircraft landing systems. My company's adaptation of the triplex system for buildings comprises of three small control units, (in this case PLCs, all programmed similarly), each being given the same information individually. They will then of course normally give the same output commands. These three commands are routed to the item to be operated, and there they enter a 'voting unit'. This, as the name implies, will operate according to a majority; so an incorrect command, regardless of how it is caused, is not acted upon. In practice this is not as elaborate as it sounds, nor as costly.

However, to utilise triplex in buildings effectively requires special techniques, which we have developed over a period of some eight years. Some of these are:-

- 1) Special software to enable a whole series of faults to be tolerated, including failure of busways. All of these techniques have been well proven. With a true triplex system, all single points of failure in the control are eliminated
- 2) An in-depth monitoring system to warn of, and identify faults. The identification is highly detailed, allowing maintenance staff to go directly to the problem, and correct confidently, safely, and at a convenient time
- 3) All items are designed to enable subsequent correction of faults without any shutdown at any time of any part of the building power distribution system

The present growth of triplex control systems in buildings with critical supplies is expanding rapidly, as the advantages for the operator are huge. Also, triplex systems can be designed not just for new applications, but also used to effect a massive upgrade of reliability in an existing building.