

Plane thinking

When Chase Manhattan decided it wanted to eliminate all possible points of failure in its power supplies and control circuitry, it turned to solutions developed by the aeronautical industry — triple redundancy.

BY MARK FAITHFULL

Jeff Rodbard is an old-school engineer. The kind of person who likes nothing better than to disappear into his workshop with a defunct hairdrier motor, a couple of bits of scrap metal and the innards of a toaster, only to reappear a few hours later clutching an ingenious contraption and bearing a victorious smile.

You can't help but feel that it was probably from just such a scenario that his mind turned to buildings and power security or rather the lack of it.

Rodbard's contention is that many offices are very vulnerable and should one small part of the power supply go down "the building falls over". Faced with such a tantalising dilemma his solution was to turn to his old stomping ground, aeronautical development at Hawker Siddeley.

Aircraft systems work on the triplex principle; triplicated circuitry that produces a two-out-of-three priority system such that no one failed component can adversely effect the operation of the aircraft. In simple terms, if one circuit fails, or tells the aircraft to do something different from the other two circuits, then the aircraft ignores it.

Rodbard set up his own company, Triplex Power Control (TPC), to devise similar solutions for buildings. He came up with his proprietary TPC control circuit, a system based on conventional hard-wired relays, timers and phase failure relays, but triplicated and powered by three separate dc supplies.

Rodbard had been in discussions with Ove Arup for some time when he discovered that Chase Manhattan was unhappy about its own power security



Flying high with triple-redundancy controls systems at 125 London Wall.

provision in its London Wall offices. Chase called in the consultants to come up with a solution, and Ove Arup proposed Rodbard's idea. The client bought the solution, and in so doing became the first major client to apply triple-redundancy principles to a building's control circuitry.

"Financial institutions are a classic case, says Rodbard. "For them the consequences of any power loss are immense, having to shut down the power at somewhere like Chase Manhattan is going to cost them at least £4 million. All they are interested in is keeping computers up and running."

As you would expect, the offices at 125 London Wall had a full uninterruptible power supply, with around 20 minutes of battery power and standby generators ready

to kick in if necessary. Despite this convention, Rodbard believes that the approach has intrinsic problems.

"Should the changeover circuit fail in any way, generator power cannot be used, however many generators are installed," he says. "And where one generator of a pair or more fails when in use, some predetermined amount of load must be shed quickly. Any problem can cause loss of the remaining generator power through overload."

While on the face of it engineers have 20 minutes to locate the fault, Rodbard says that the actual window is much shorter. At Chase Manhattan it takes a full 15 minutes to complete a shutdown of the computer systems, that means the engineers must decide after just five minutes whether to close down or try and fix the problem.

The offices have an available supply provided by one 2.5 MVA and two 2.35 MVA generators, all located at high level and connected to the five rising busbars, each rated at 3000 A. Normal mains supply is fed into the lower end of the busbars and the top and bottom switches are electrically interlocked.

The new system was initially installed without connection to the main switchboards, the old wiring left in place. "Chase Manhattan wanted to minimise downtime," recalls Rodbard, "They were very clear about that."

The TPC fault diagnosis system monitors each of the three circuits at various points, looking for any differences that may be present at one point compared with two similar points on the other circuits. It also checks the control circuit supplies.

If a fault is diagnosed, an alarm indicates the type and area, allowing it to be corrected without the supply being affected. The use of low voltage dc power for the control circuits means that components can be changed live, with the supply still operational.

Triplex tested the proposal using dummy air circuit-breaker units, which used the same operating coils as the real circuit-breakers. Through demonstration these were shown to operate mechanically and electrically in the same way as the actual units (although the main contacts were represented on each dummy by a microswitch). Thus consultant, contractor and manufacturer were able to prove to Chase Manhattan that the system was ready to run before anyone did anything drastic, like turning the power off.

Not only were three separate circuits specified, but the client proposed that the cabling take three different routes. Should one set of cables be damaged physically the other two sets should remain intact. Although the triplex support would be lost, the circuits would continue to work. Inevitably this meant a lot of complicated cable routings for installer London & Essex and a lot of very careful work in floors occupied by sub-tenants.

A bank holiday weekend was scheduled for the installation, and once the power was off the wiring was transferred from the dummy circuit-breakers into the real units, tested and verified. "Some of the contracting lads stayed until 3am but we got it all done," says Rodbard.

The system allows an additional degree of sophistication, with load shedding based on priority circuits should one or more generators fail to come on-line or fail in service. The load shed system controls 47 floor distribution cubicles supplying tenants' power to different areas, with one of four priority levels set for a given circuit. With just one generator left, only emergency systems and the computers would continue to run.

"The cabling was the only expensive part of the job, and that was because it was a complicated retrofit and we had to use wiring capable of some tight bends and run-throughs," says Rodbard. "Despite the triple redundancy you are not looking at a big outlay. And anyway, what's a few pounds on some extra circuitry compared with the massive losses that can hit these companies if their system is down for even a few minutes? At Chase Manhattan the requirement was quite simple, the power must not go off."

Mark Faithful BSc Hons is a freelance technical journalist.

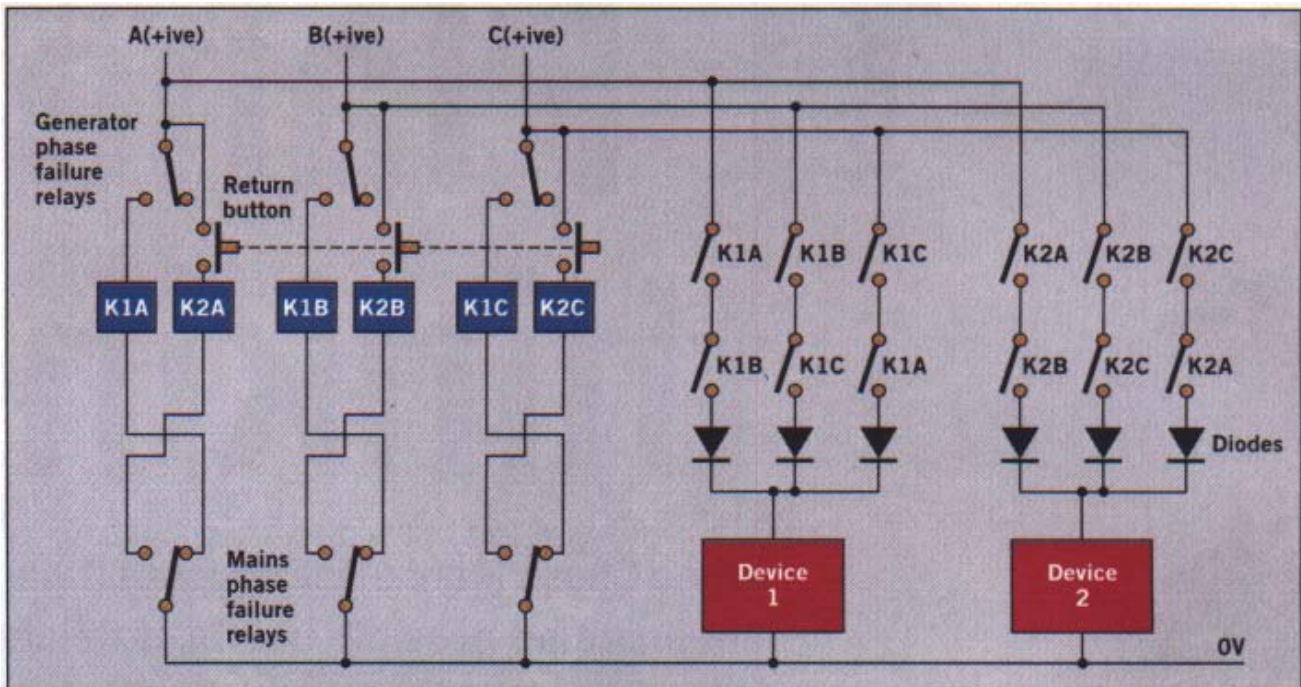


FIGURE 1: A triple redundancy control circuit. The elements that control the main circuit are arranged in a triplex configuration, to ensure normal operation even in the event of a failure of one component or supply.

Taking one circuit:

- If the upper phase failure relay is powered but not the lower relay, then K1A operates;
- if the lower phase failure relay is powered and the return button is operated, K2A operates;
- if upper and lower phase failure relays are both operated or both relaxed, neither relay operates (switching in both poles of the supply is not a problem for a 24 V supply, and reduces lengths of wiring loops);
- a fault in any component will produce incorrect operation of the relay contacts.

In the circuit shown in figure 1, device 1 will operate when the K1 contacts close, ie the top phase-failure relays are energised and the lower relays are not. Normally this would occur because the contacts of all the K1 contacts close, but if K1A failed to close then only two of the feeds to device 1 would fail, but the centre of the three circuits would still operate it via K1B and K1C.

Alternatively, if a relay stuck closed when all three should release, then no feed would be received by device 1. So failure of one phase-failure relay or power supply does not affect the correct operation of device 1.

The diodes mean that:

- No connection is made between the three dc supplies, even though they are operating the device;
- a wiring fault to earth in one circuit, or collapse of one dc supply, cannot affect the other dc supplies;
- a wiring fault after the diodes (ie in the single wire feeding the device) will still cause failure.

Therefore diodes must be as physically close as possible and preferably adjacent to the final device. At Chase Manhattan they are mounted on terminals in the original Klockner Moeller panels at the far end of the interwiring.