

Equipment Protection

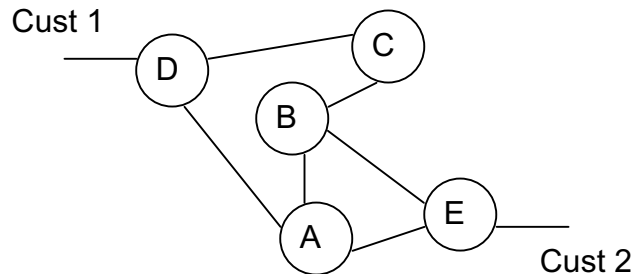
Introduction

Telecommunications networks have a long tradition of reliability. When other infrastructures fail due to natural or man-made disasters, the telephone is used to summon rescue efforts. Where loss of telecommunications service means loss of revenue, businesses have come to depend on this reliability for their operations.

The reliability of the network is achieved through two design concepts: (a) redundant paths through the network, and (b) redundant components in each network element. Redundant paths mean that, in case switch A becomes incapacitated, a signal normally dependent on switch A can be routed through switch B. Redundant components mean that if one component of a network element fails, another component will take its place. This paper will detail the redundant component concept.

Protection Scopes

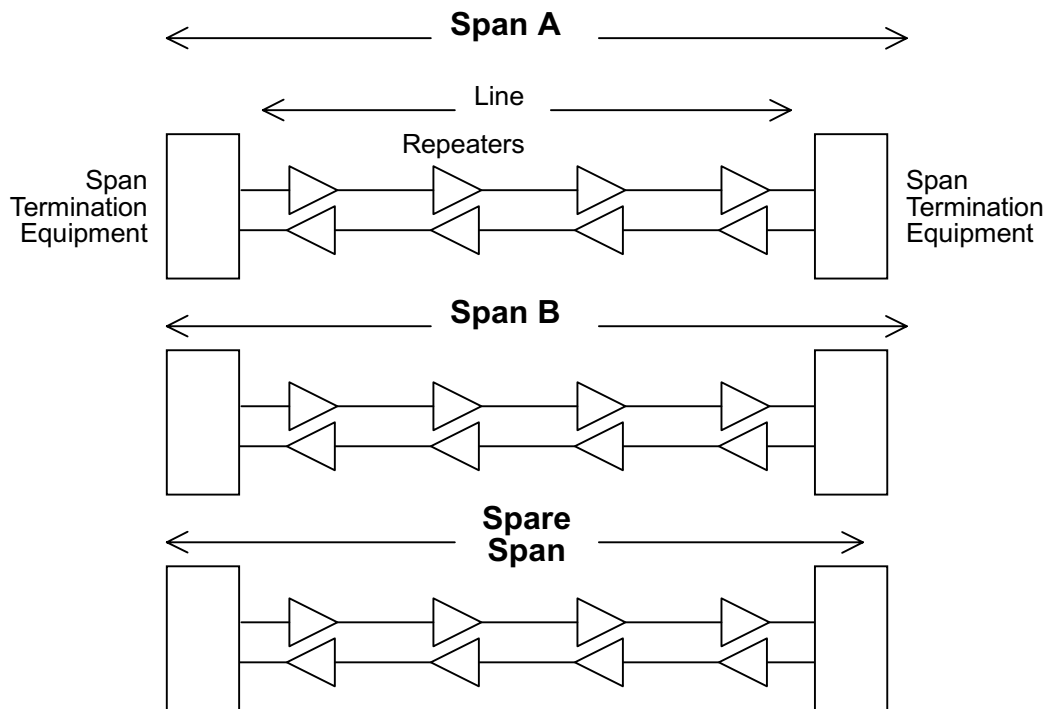
Depending on the viewpoint, the birds eye view, or the worms eye view, protection takes different strategies. Network architects are responsible for the long view by designing alternate routes. Thus if an entire switching center is incapacitated, the signals would travel a different route to the destination. Naturally, signals to or from the downed node would cease.



In the network map above, the shortest route from D to E is D-A-E. However, if node A is incapacitated, the alternate route D-C-B-E, albeit longer, could be used. Alternate routing provides protection against major disasters.

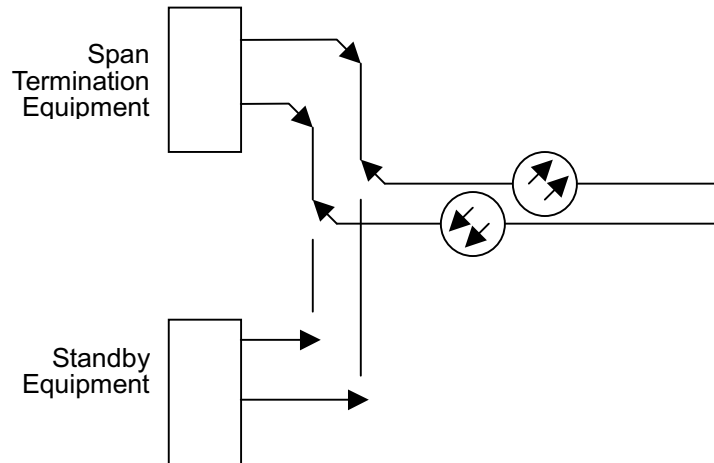
Span Protection

Transmission engineers take the local view by providing redundant equipment and redundant transmission spans to protect against failures. In the diagram below, one or more spans, each a two-way transmission system, provide transmission facilities between two nodes. Failures can occur in any of the repeaters of the line, or within the terminal equipment at the two ends. The span protection strategy is to substitute the entire span that has a failure in either a repeater or a terminal. For E1 or T1 lines, because of the numerous repeaters in outdoor environment result in frequent line failures, span protection strategy is used.



Equipment Protection

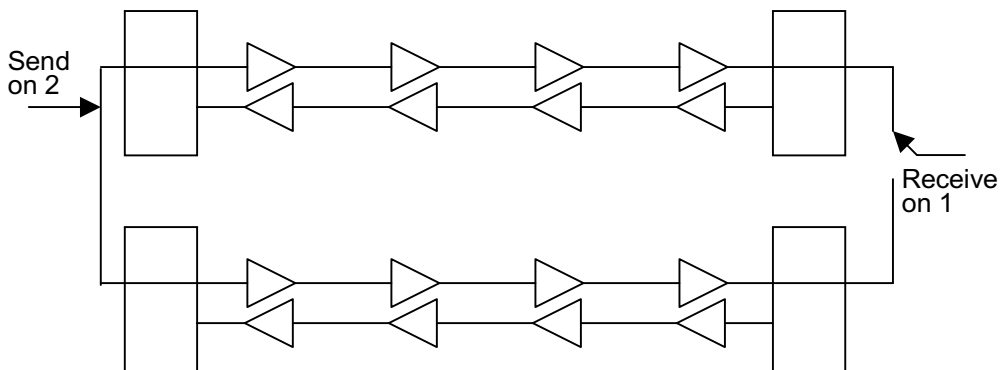
Because of its low loss, optical fiber can traverse metropolitan spans without repeaters. This lowers the installation cost, and also increases reliability. Failures of optical fiber would be a result of a far less likely physical breakage, rather than failure of electronics. Because of this difference, the protection strategy shifts from span protection to equipment protection, where electronics reside.



Protection Coordination

In most cases of protection design, both the near end and the far end must coordinate the switching to the spare. The exception is the "send on two, receive on one" span protection strategy. In all other cases, because the location of the fault is uncertain, the protection strategy must cover all possible locations of a fault.

Where one-for-one span protection is employed, no coordination is necessary for the "send on two, receive on one" strategy. Signals are sent on both spans, each end selects one span to receive the signal. At the receiver, when the signal fails, due to any number of reasons, that end switches to the other span to receive. No notification to the other end is needed.

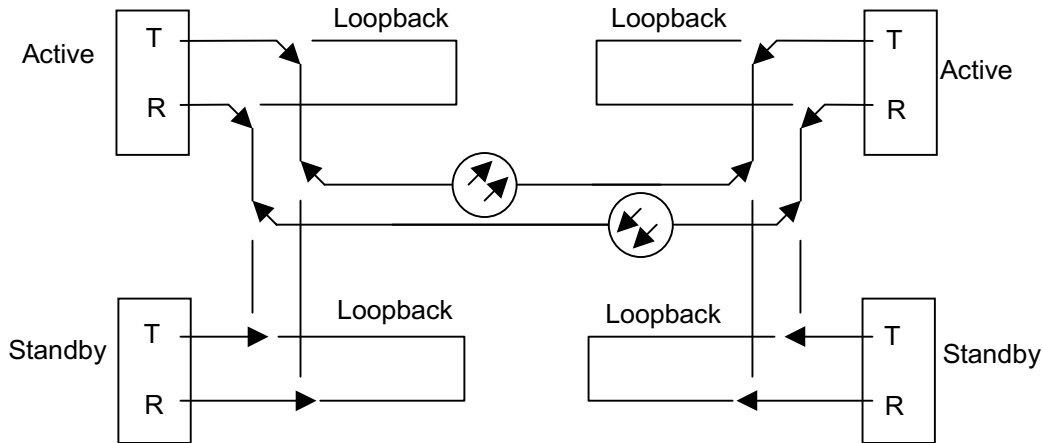


Another exception to coordination is protection of peripheral equipment, such as the power supply. Protection of peripherals is beyond the interest of this paper.

For all other cases, such as one-for-many span protection, and for all equipment protection, coordination between two ends is necessary. In what follows, coordination for equipment protection is discussed.

One-for-One Protection

Switching for one-for-one protection is schematically illustrated below.



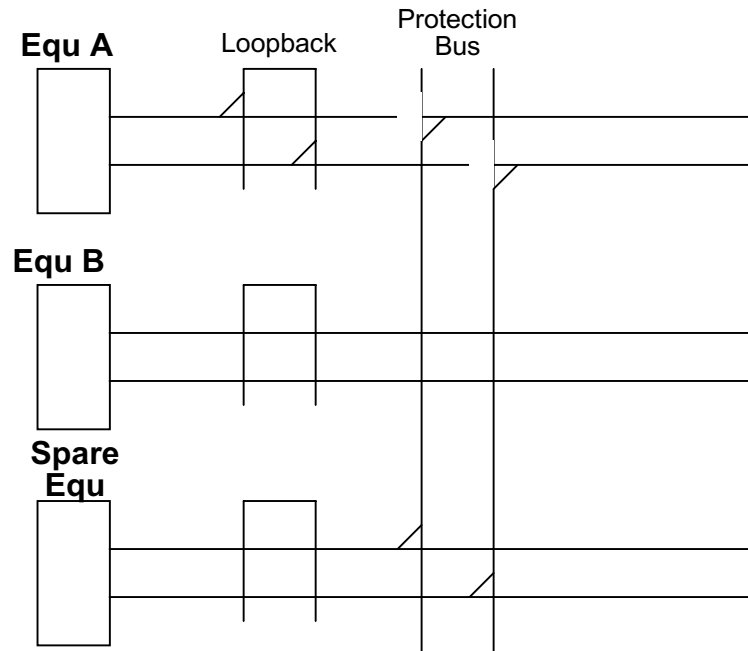
At both ends of the span, each piece of equipment has a duplicate for protection. Switches at both ends allow either equipment, the top in the drawing, to handle signals under normal conditions. In the standby position, the spare has switches for signal loop-back, so that the proper operation of the standby equipment can be assured whenever needed. Telecommunication veterans like to remind novices that standby equipment not constantly tested results in a failed standby when needed.

Faults can occur either at the transmitting end, the transmission media, or at the receiving end. In any of these situations, only the receiving end would detect the fault. The receiving end would then switch to the standby. At the same time, the receiving end would interrupt the return signal, so that the transmitting end would also switch to the standby. This is necessary because the fault can be at either end. Of course, if the unprotected transmission media, the fiber, would fail, service would not be restored. Saving an extra fiber is balanced against this risk when using equipment protection strategy.

After switching to standby, normal equipment on both sides would be looped back on itself. This would allow the determination of the location of the fault.

One-for-Many Protection

Switching for one-for-many protection is schematically illustrated below.



At both ends of the span, standby equipment is provided for protection of several similar equipments. A protection bus allows switches at both ends to substitute the standby for any one of the several protected equipments. As in the one-for-one case, the switches provide for signal loop-back of the standby equipment. For this strategy to meet the rapid-response requirement of protection switching, every group of equipment protected by the single spare must be configured in the same way.

Again, as in the one-for-one case, when a fault along a transmission path occurs, the receiving end would detect the fault and switch to standby. At the other end, signal interruption forces the switch. Thus the entire span would be switched to the standby. This strategy applies to both span protection and to terminal equipment protection.

Like the one-for-one case, after switching, equipment on both sides would be looped back on itself. This would allow the determination of the location of the fault. Because optical fiber technology cannot use bus architecture, the design for one-for-many fiber protection is more complex.

Single-Fault Assumption

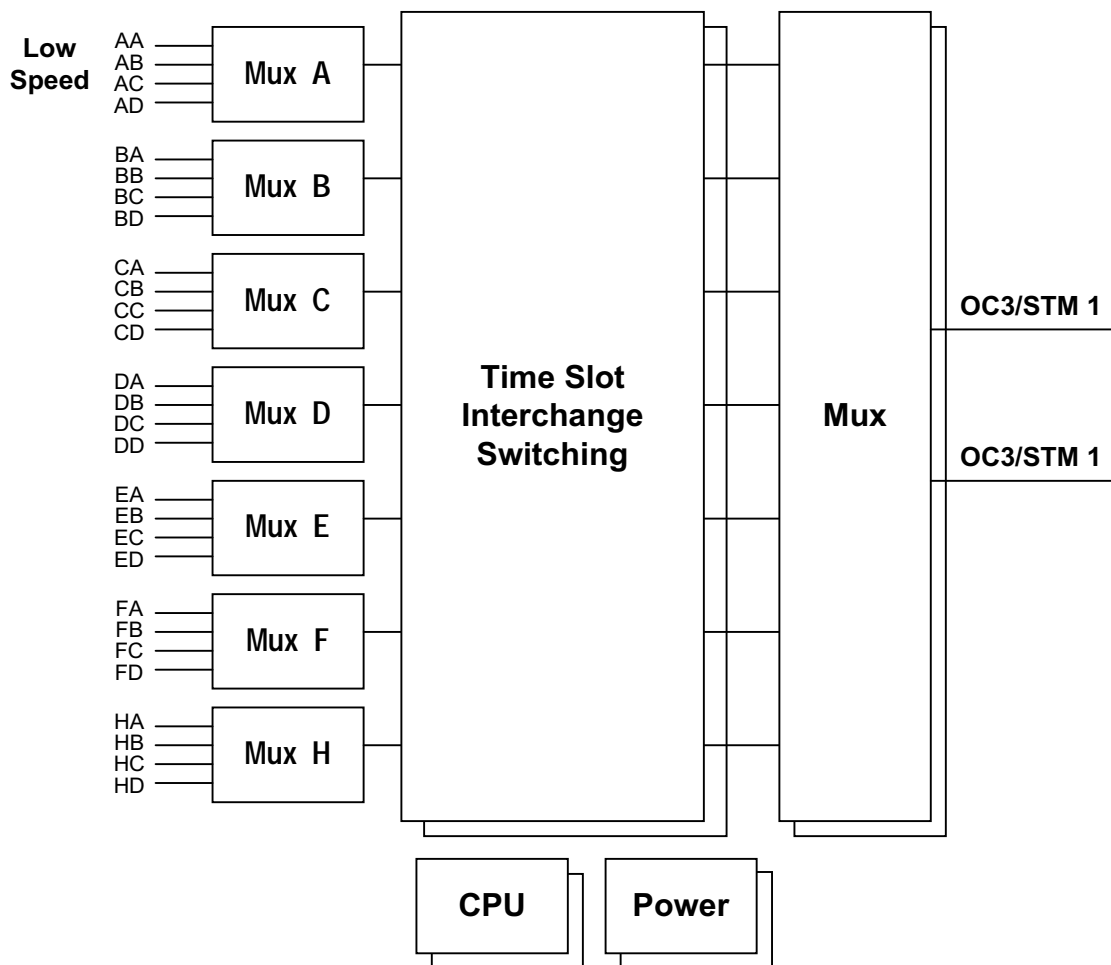
Single-fault assumption simplifies the protection software and eases human understanding of network condition. For example, one can manage a list of all possible places where a single fault might occur. But to manage a list of all possible double-fault would be daunting. The single-fault assumption has validity only if the single fault can be detected quickly and repair made before the occurrence of another fault. Using the two parameters in network design, mean time to repair divided by the mean time to failure yields the probability of a double fault.

The single fault assumption also applies when a group of equipment is assigned to protect a larger set of equipment. When one element of the group has been invoked for protection duty, the other elements of the group, although theoretically available, will not be assigned protection duty until repair is made of the original fault. Again, the rationale is in simpler protection software and easier human understanding.

Protection Example

In the Loop-V 4200-28, optional 1 for 6 protection is provided. As shown in the block diagram below, the 28 low-speed inputs are grouped into 7 groups of 4 inputs each, labeled A to H. Within each group, the inputs are labeled A to D. Thus the first group has inputs AA, AB, AC, and AD. The second group has inputs BA, BB, BC, and BD. The last group, H, can be used as normal inputs, or as protection for the other 6 groups. When used as protection, the equipment for HA can be used to protect one or more of the 6 inputs AA, BA, CA, DA, EA, and FA, and similarly for HB, HC, and HD. The inputs that HA protect must be of the same type and configured the same. If not, then HA will not provide protection for that input.

The single fault assumption will result in the following restriction. If protection is invoked for any one of the four equipments of H group, HA, HB, HC, and HD, then the other 3 will not be available for protection.



NOTE: Mux H & Ports can also be used for protection for other.