WHITE PAPER

‘Insuring’ Operational Resiliency

ROGER FRANKLIN
PRESIDENT AND CEO
CRYSTAL

CRYSTAL™
Wherever Content Flows...™

www.crystalcc.com

Why do businesses purchase disaster insurance?

Because they need to mitigate the impact that disasters might have on their operations. Businesses can generally weather sales cycles, personnel issues, etc., but anything that directly impacts its revenue stream must immediately be addressed. In short, they need to maintain business continuity.

Satellite transmission and video distribution businesses are no different. They must spend capital to avoid or decrease the impact of problems that are beyond their control. This is typically done via ‘self-insurance’ and can pay for itself many times over by purchasing excess equipment or emergency capacity. For many commercially supported networks, the lost revenue from even a single missed commercial segment can approach the capital needed to avoid the loss in the first place.

But how does your company most intelligently apply this capital?
In order to answer this question, one must examine what types of operational interruptions a satellite-oriented business might face. Generally, these interruptions fall into two broad categories: *Equipment Malfunction and Facilities Issues.*

Running ‘Hot’ and ‘Cold’

Equipment malfunction is straightforward, although the best response to it may not be. The typical strategy for handling equipment issues is to have backup equipment on hand to replace failed units. This takes the form of a ‘hot’ standby, where a replacement piece is already powered up and configured for quick insertion as a substitute, or a ‘cold’ standby where it is not.

In many cases cold standbys are not acceptable. Too much time is lost to connect and configure the replacement equipment to match the failed piece of equipment. Hot standbys allow for rapid response to problems, but require operators or technicians to perform dual configuration when changing a setup. Also, when the equipment in question is a computer system, operators must keep the backup ‘hot’. This is a lot more involved and requires continuous synchronization of databases.

One for One, or One for Many?

It is not economically feasible for facilities to provision a redundant spare for every piece of equipment and this type of configuration may not be required. This is because one piece of equipment (e.g. a Modulator) can serve as a backup for several like pieces of equipment. At an installation with 5 uplink transmission ‘chains’, it is unlikely that the modulator in 2 or more of these chains will fail during the same reasonable span of time. A single modulator can serve as the backup for all 5. This type of redundancy strategy is referred to as ‘1 for N’ (or sometimes as ‘N for M’ if more than one total backup is to be used).

Of course, in 1 for N redundancy, the backup equipment cannot be pre-configured and ‘hot’ for insertion into a chain. For rapid insertion one would employ switches of the appropriate type to quickly switch the backup unit into service and the primary unit out of the chain, rather than manually connecting cables. This leads to:

Automated Solutions

For very simple installations, backup units are preconfigured and wired to be placed into service when another unit fails, without manual intervention by personnel. Once a threshold of network and system complexity is crossed, a Network Management and Control System is required.

A Network Management and Control System monitors most or all units of equipment at a facility, detects failures, and rapidly switches backup units or chains of equipment into service for the failed unit(s). The system automatically configures the backup equipment, which is necessary for any 1 for N type of redundancy. This type of implementation is referred to as Redundancy Protection Switching.

A Network Management and Control system (such as Crystal Control, Crystal’s NMS) has a number of advantages:

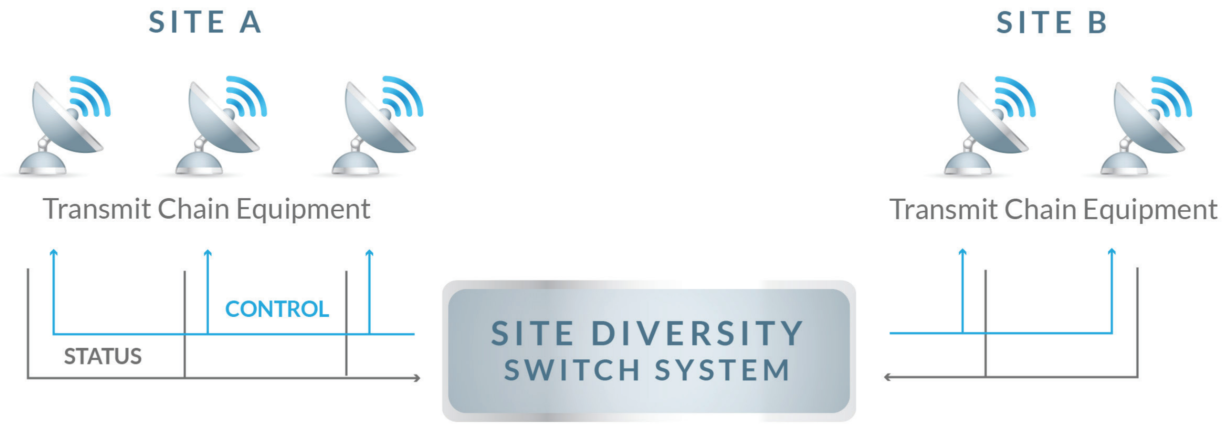
- Performs automatic switch out upon failures, configures and switches equipment into service, even in 1 for N topologies - often with sub-second responsiveness.
- Alerts personnel via audible and visual alarms, or using email or SMS messages. This prevents failed equipment from going unnoticed, which happens with automatic redundancy switching that happens without the aid of a Network Management and Control System.
- Logs all failures for future analysis and provides a 3rd party record of failures.
- Automatically switch upon failure events, or switch with as much or as little operator interaction and decision making as desired.
- Respond following a script of pre-thought out, complex decision trees (e.g. ‘switch in chain k, except if ‘blackout’ is currently in effect, then follow switch Plan B’).

Besides responding to ‘hard failures’ of equipment, sophisticated Network Management and Control Systems, such as Crystal Control, spot long range trends in equipment performance, and alert operators to a imminent failure, before it occurs. This allows for the timely swap out or recalibration of equipment.

Facilities Issues

Facilities can be subject to several types of temporary ‘outages’, that range from loss of power, exceeding backup power capacity, floods, earthquakes, failures in basic HVAC or plumbing, backhoes, etc. Particular facilities may be temporarily disadvantaged by extreme weather, and an outgoing or incoming transmission may be impaired.

In many of cases, facilities enlist backup equipment located at a geographically separate facility. Such a strategy is referred to as Site Diversity Switching. Entire transmit chains will serve as the 'unit' that is switched in or out as a whole. A master Network Management and Control System must be employed in such a case, with domain over all of the facilities involved.



A beneficial byproduct results when facilities use Site Diversity Switching in a sizable way: Less redundant equipment is required to yield the same safety margins against failure. This is because the redundancy burdens are shared across multiple facilities. A recent analysis of one transmission entity revealed a potential savings in excess of $100K.

If weather conditions are only moderately severe, a different mechanism may be employed by uplinkers at a facility without involving redundant equipment. A system of Automatic Uplink Power Control (AUPC) adjusts HPA power to the transmit dish in real time, based upon the sensed attenuation due to weather conditions. Sophisticated AUPC systems make sub-second adjustments to power, based on the strength of the returned downlink signal. For multiple transmissions concurrently, the AUPC system ensures that total power to any single feed does not exceed limits.

True Disasters

Disaster conditions involve the permanent or long-term loss of significant portions of transmission or reception infrastructure. An example of this is the complete loss of a transmission/reception facility due to explosion, catastrophic geologic or weather event (hurricane, volcano, earthquake, etc.), political instability or terrorism, or the unexpected loss of a satellite.

These events call for a different response strategy that is ‘global’ in nature. Why? Because the best response is not simply switching in backup equipment. The demands of a large disaster will overwhelm the previously laid plans for backup equipment and capacity. In these cases channel capacity needs to be prioritized, where the operation of certain low value channels are sacrificed to maintain that of high value channels. Transmissions must be moved to entirely new modes for conveyance, such as fiber or Internet or satellite.

Response to large-scale impacts to operations are best handled via a sophisticated Network Management and Control System. The chief advantage is that optimal responses to disaster scenarios are mapped out ahead of time. Clear thinking reigns over than of an emergency and the response actions are ‘codified’ into the Network Management and Control System.

Layered Response

A competent Network Management and Control System is the best bet to insure Operational Resiliency. And the best of such systems will support:

- Redundancy protection switching
- 1 for N style redundancy
- Rapid, automatic or operator assisted response
- Degrading equipment notification and trend graphing
- Automated uplink power control
- Elevated response for disaster recovery