

FAULT-TOLERANCE : RELIABILITY'S REALITY

TOLERANCE DE PANNE : LA REALITE DE LA FIABILITE

McMENAMIN Daniel P.
Bell of Pennsylvania
Philadelphia, USA

Résumé

La fiabilité est un des grands mots d'ordre dans notre secteur d'activités. Un autre concept, l'insensibilité aux défaillances, ou la tolérance de pannes, nous offre les moyens de réaliser des réseaux totalement fiables. Dans les télécommunications, les défaillances d'alimentation électrique sont souvent la conséquence d'une mauvaise application ou d'un défaut des procédures d'entretien. En fait, l'accident énergétique le plus dévastateur enregistré dans le monde, la terrible catastrophe de la centrale ukrainienne de Chernobyl, a eu pour origine un essai qui a échappé au contrôle de l'homme.

La tolérance des pannes reconnaît la réalité, la nécessité de procéder à des opérations de maintenance. Des problèmes surgissent, des équipements cassent, et il faut réparer. La rupture d'un seul équipement ne doit pas perturber une multitude d'utilisateurs du téléphone ni affecter de larges sections du réseau. Les ingénieurs des télécommunications doivent relever ce défi malgré les coupes budgétaires et la brusque réduction des équipes techniques expérimentées. Ils doivent tirer le maximum de ce que leur permet la technologie.

Ces dernières années, plusieurs problèmes d'alimentation ont isolé de larges tronçons du réseau téléphonique. Des travaux d'étude plus prudents auraient pu atténuer ou éviter ces pannes. La présente communication examine plusieurs moyens d'introduire le concept de tolérance de pannes dans les stations d'alimentation du réseau. Elle considère également la possibilité d'équipements portables, qu'il serait facile et peu coûteux de connecter rapidement au bus d'alimentation pour que les activités puissent se poursuivre en toute sécurité dans la zone perturbée pendant les opérations de maintenance. De même, la défaillance d'un équipement en cours d'entretien risque moins de perturber le réseau.

Abstract

Reliability is an important watchword in our business. Another concept - Fault-tolerance, is an important means to achieve overall network reliability. Power related lapses in telecommunications service, often are the result of maintenance procedures which were misapplied or went awry. Indeed, the world's most devastating power glitch, the terrible failure at the Chernobyl nuclear reactor plant in the Soviet Ukraine, began with a test that got out of hand.

Fault-tolerance recognizes the reality that maintenance procedures must be performed. Problems happen, equipment breaks, and must be repaired. The breakage of a single piece of equipment should not cause problems for large numbers of telephone subscribers or affect major portions of the network. The telephone engineer's challenge is to accomplish this while flying in the face of budget cuts and a sharp decline in experienced technical support. Our coping skills must stretch with technology.

In the past few years, several power-related problems have isolated large portions of the telephone network. More prudent design work might have mitigated or eliminated these failures. This paper will explore several means of building fault-tolerance into the network power plant. Also included will be ideas for portable equipment which can be connected to the power bus quickly and cheaply to provide a safe work-around while maintenance activities are performed. Accordingly, a fault in the equipment being serviced is less likely to affect the network.

Failure Causes & Effect

Service lapses often are attributed to the broad category of interruption called "power-related." These varied problems include equipment malfunction or human error-caused anomalies from myriad areas such as: the commercial grid, standby engine plant, problems in the mains or switchgear, the telephone power plant, overcurrent protection devices in the power plant or switching system, embedded-converter problems in the switching system, lightning strike, ElectroStatic Discharge (ESD), grounding (earthing) problems, cable faults, and virtual every problem of unknown origin.

Telephone engineers will be confronted with all of these problems and he or she can't change that. If anything, the likelihood of failure is increased by the expanding variety and complexity of telecommunications equipment, and workforce downsizing, a global trend. Explaining system failures to telephone executives is an uncomfortable experience.

Redundancy

Redundant systems are a watchword for fault-tolerance. Where possible, carefully planned redundancy can achieve high levels of fault tolerance. Switching system manufacturers build it into their processing schemes. Power engineers do too, but perhaps another look is needed. Typically, power engineers provide redundancy for chargers, ringing generators and dc to dc converters. Increasingly, there is a need for other elements of the power plant to be more tolerant of failure.

Single-string batteries invite disaster. Two smaller ampere hour capacity strings are much more reliable than one large string. This is especially true of Uninterruptible Power Systems (UPS) where there is a very high discharge rate. Consideration should be given to a second string. In existing telephone dc power plants smaller capacity strings can be paralleled with the battery in place. Since most flooded telephone batteries are of the "low gravity" type, it's prudent to use similar cells so the number of cells in series are the same. Some manufacturers offer low-gravity valve regulated cells which can be floated at 2.20 volts per cell. This allows them to behave nicely in parallel with their flooded companions.

Increasing candor in the battery business has revealed numerous problems with valve-regulated batteries. Yet, because of distributed systems, loop electronics and Fiber-In-The-Loop (FITL) systems telephone engineers are still clamoring for high density batteries for vaults, huts and other equipment enclosures. Thermal runaway, cell dryout, grid corrosion, seal failure, cable and intercell connector failure, all contribute to the body of horror stories telephone people swap at social gatherings.

There's an uncomfortable feeling among maintenance people that they maintain batteries while purchasing organizations buy cut-sheets. A twenty-year cut sheet doesn't necessarily mean the battery will last that long. It probably won't. Engineers pointedly argue culpability, citing factors of: manufacturing processes, shelf time, transportation, handling, installation error, over/under charging, maintenance, cycling, thermal or vibration environment, and others. Regardless, the telephone power community has suffered sufficient failures to justify an N+1 redundancy scheme for valve-regulated batteries at critical locations.

UPS systems are increasingly important as computer data bases comprise a large part of the operational network. They aren't just support systems anymore. UPS failures are common. Inverter-leg failures are very common in thyristor systems. Many consider the UPS

the weakest link in the chain. Accordingly, parallel-redundant operation is the system of choice for critical equipment sites. Parallel UPS modules sourced on separate distribution cabinets increase reliability dramatically. Added reliability is obtained when the battery strings are tied to a common bus. Then all UPS modules can draw from all batteries, reducing the risk of a system failure.

A bypass source tied directly to the UPS paralleling cabinet increases fault-tolerance. Any or all UPS systems can fail or be taken from service for maintenance with no effect on the load. Bypass panels feeding telephone plant inverters serve the same function in the power room.

Standby engine systems are candidates for redundancy, especially at large facilities. Automatic paralleling systems with isochronous governors are common and lend themselves to telephone plant operation.

Systems

Mechanical end-cell switches are maintenance intensive and difficult to obtain parts for. While they permit more efficient use of battery capacity, they experience too many failures to be considered part of a fault-tolerant system. Solid-state switching devices and MOSFET regulators could be employed to develop a reliable, transient-free, end cell switch. For the moment, though, they do not exist, and mechanical end cell switches should be removed.

Self-supervising alarms are more fault-tolerant than non-supervised systems. With this feature, power plants report alarms with a loop-open rather than a loop closure. This eliminates the likelihood of a failure left to disaster because the alarm circuit was broken. It's very inexpensive reliability.

Switching systems which use unusual voltages aren't fault-tolerant. Spare parts, training and other support infrastructure may be difficult to obtain. Furthermore, engineers can obtain 48 volt and 24 volt telephone power equipment very quickly if a fire, flood or catastrophic equipment failure damages a telecommunications switching facility. Switching equipment using 140 volts or other unusual source potentials are very vulnerable to catastrophic failure. System planners would do well to consider phasing out such systems.

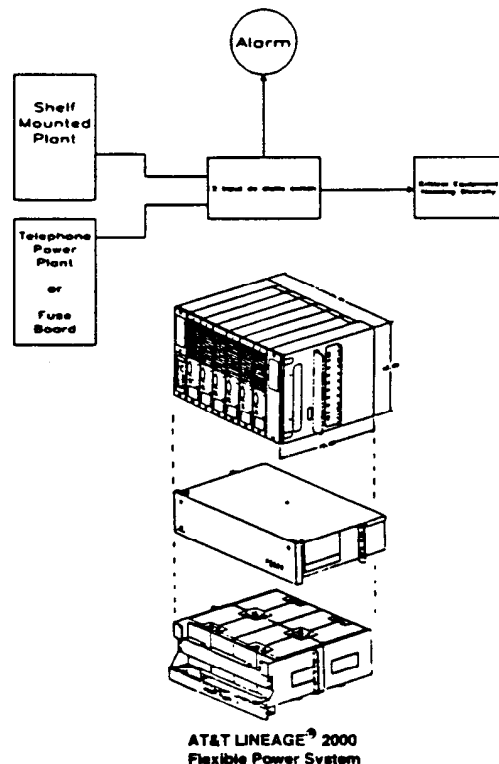
Automatic engine start systems are more fault tolerant than manual ones. Additional benefit is obtained when those engines are arranged for remote starting, and monitoring. Furthermore, they cost less to operate and maintain. A single technician could "cluster-test" a group of engines at one time via a personal computer or other interface. The computer would start and monitor the engines via monitor/control subsystems. Serious trouble would cause the engine to shut down with all important information available via the interface link.

This has several advantages. Technicians can start their systems at the onset a major storm and use commercial utility power as a backup. If an engine fails to start, there's time to deploy repairs before the highways are blocked by traffic or fallen trees. Companies could negotiate substantially lower electrical rates by being able to "curtail" large blocks of power very quickly.

A relative newcomer is closed-transitioning. In closed transition systems there is no interruption of ac power during routine engine runs or when returning to commercial power following an outage. Under automatic control, the standby engine generator is brought into sync with utility power. The engine circuit breaker is closed and the engine and utility are in parallel operation for a narrow (approximately 50 millisecond) "window" of time before the utility breaker is opened. In this mode, there is no interruption of ac power to communications equipment. This feature can be included in many automatic transfer switch designs or electrically-operated circuit breakers in switchgear systems. If the central office battery is deeply discharged, a closed transition return to commercial power is preferable because the load isn't imposed on an already stressed battery.

Large dc power plants in the 5,000 to 10,000 ampere class are phasing out, replaced by smaller systems. Perhaps 85% of dc power plants, today, carry fewer than 1,500 amperes. Central offices with multiple switching systems are arranged for distributed power plants. Such facilities are more tolerant of equipment faults. As an added advantage, separate power plants offer opportunities for power diversity for support critical transmission systems. Separate plants offer an opportunity for disaster recovery. A significant equipment failure, such as two or three failed rectifiers, could be cabled around fairly quickly to "borrow" power from one power plant to support another.

Critical multiplexers, repeaters or other equipment might be supplied a diverse-plant source by using a small shelf-mounted plant such as AT&T Corporation's new FPS - TMAT&T flexible power system. Such small power plants offer inexpensive diversity. A companion item, a two-input dc static transfer switch would complete the package.



Modern power plant designs incorporating plug-in rectifiers are inherently more fault tolerant than hard-wired plants because repair is a simple matter of plugging in a new one. The dc bus isn't exposed to risk during the rectifier repair effort.

Many engineers prefer to feed rectifiers or charger units from two circuit breaker cabinets. This ensures that a circuit breaker operation or failure on the switchgear distribution board will not disable all charging units. Additionally, the feature permits routine testing and maintenance on the source circuit breakers with less impact on the switching system and associated battery.

In the atmosphere of excitement which often accompanies central office power trouble, it is very easy for technicians and installers to accidentally bump or turn off circuit breakers on many dc distribution board designs.

Protective covers often prevent accidental bumps with little added cost. Even more forgiving are switch and fuse units, which are far less likely to be operated in error than circuit breakers. In 27 years with Bell of Pennsylvania, this author has never seen a case where a technician inadvertently caused the failure of a telecommunications facility by operating a switch and fuse unit in error or improperly. I have investigated many such failures where circuit breakers are used. Accordingly, I believe that engineers would do well to specify them, where board space permits, for switching machines or other critical circuits.

Human error remains the causal element of large numbers of failures. Painters, construction workers, housekeeping persons and others work in telephone power rooms, often with no idea of their potential for injury or to cause major trouble. And, even experienced people still drop things.

The simple act of replacing a fluorescent light tube has resulted in switching service interruptions when workers drop or even place the diffuser across open busbars.

It seems prudent to enclose all busbars and splice plates, leaving no "live" bars in the room. This helps ensure that a dropped tool or piece of material won't disrupt vital communications facilities. Insulating covers placed over battery post interconnections also protect from the obvious at very little cost.

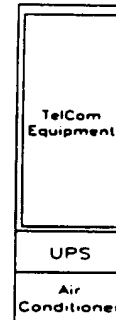
Cable often falls during installation. Armored cable, and flexible metal conduit can cause short-circuits if it falls across live circuitry. Jacketed metal-clad cable or jacketed liquid-tight flexible conduit reduces such failures with very little added cost. Such cables should be run using dedicated cable trays or other means to provide support and isolation from communications or dc power cables.

Environmental

Experience has shown that digital switching machines and some multiplexer systems perform very poorly when air conditioning is unavailable due to trouble or the loss of commercial power. Where possible, standby engine sets should be sized to carry air conditioning for digital offices. Certainly new systems should be sized to this criteria. Switch replacements would require more creativity. Very few central offices were sized to accommodate large chiller systems. Perhaps a digital switch could be compartmentalized and smaller stand-alone HVAC systems deployed, which would fit within the capacity of the existing engine set. Maintaining a constant temperature and humidity ensures the reliability of the switching system, better tolerating the loss of commercial power.

Liebert Corporation, an American manufacturer, offers equipment cabinets with air conditioning units built into the base. They call their unit a "Glass house," apparently because of the smoked glass front access door. These may be ordered with refrigerant-based systems, or with heat exchangers for connection to building chilled water cooling systems. Also, they can be provided with UPS units up to approximately 2.5 KVA. Such cabinets offer an extremely cost effective solution when small pieces of equipment such as multiplexers, etc are located in isolated spaces. Candidate locations might include a hut, vault, customer premise, or even some corner of a central office, to house critical pieces of equipment needing generator-protected air conditioning.

Air Conditioning equipped equipment cabinet



Compartmentization might also facilitate the degree of air particulate filtration needed for sensitive switches. Reliable filtration ensures the long-term viability of the switching system and circuit packs. Modern printed circuits use tiny components with lead connections or "lands" which are very close together. High power density systems compel manufacturers to forced-air cool their frames. Since fans move large volumes of air across the circuit pack surface, airborne dust can accumulate very quickly. Coatings or piles of dust reduce the life and effectiveness of a circuit pack by preventing effective cooling. Further, some dusts contain metal particles and are electrically conductive, others begin conducting during episodes of air conditioning loss due to increasing humidity. Still other particulate materials, such as concrete dust contain carbonates which become corrosive at elevated humidity levels, damaging components, conductor foils or contacts.

Deposits of smoke and soot particles can contaminate and destroy electronic circuits. Compartmentization of switching systems makes nearby equipment tolerant of the failure. Intumescent (thermally-activated) expansion-type firestop materials also help contain smoke at wall or floor penetrations, protecting nearby equipment from smoke damage. These are preferable to mineral wool bags and other "stuffing" methods. Non-halogen cable insulation has excellent fire retardancy properties, while releasing significantly lower levels of smoke and toxicity when burned. Such cabling could help avoid damage to critical central office equipment.

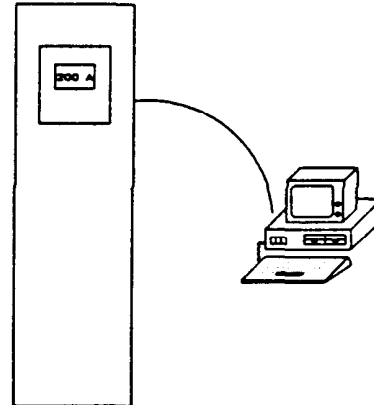
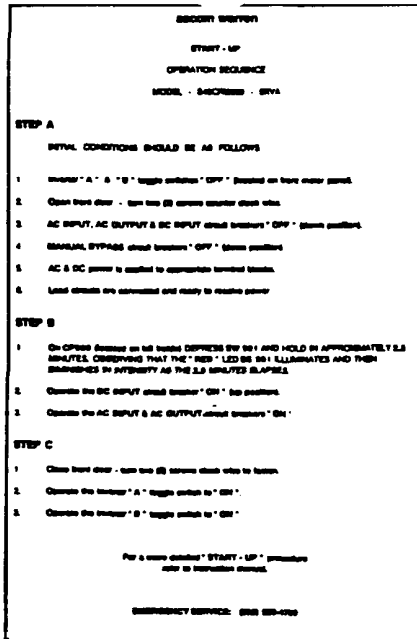
Operational Job-Aids

Many telecommunications failures are the result of human error. In another industry, few professionals are more experienced, better trained, or highly motivated than the pilots of large airliners. Yet, they make mistakes. An effective prevention tool is their various checklists.

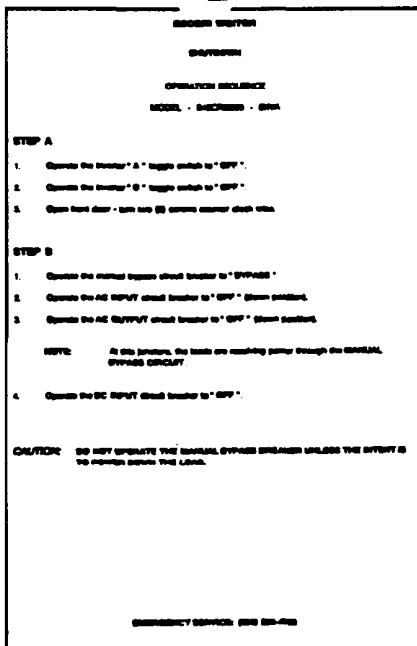
Checklists are a useful tool to achieve fault tolerance in telephone power equipment. Equipment start-up checklists serve as a reminder to those familiar enough with the equipment that they avoid the product manual. By following a simple checklist, equipment can be restarted following a malfunction or repair without errors which might cause a communications facility to fail.

Monitoring systems will help achieve fault-tolerance although they need to evolve towards an "Expert-systems" approach. This will help to compete in a world where a declining base of technical employees confront an increasingly complex mix of technologies, both in the central office and the distributed network.

There is a need for diagnostic software and interfaces which allow common laptop or notebook computers to serve as sophisticated test systems for rectifiers, controllers and other power plant subsystems. Vendors should be encouraged to produce diagnostic software for their rectifiers, controllers and other systems. These programs would drive DOS-based computers equipped with IEEE-488, VME or other suitable bus interfaces, plug-connected to the equipment under test. This would improve the troubleshooting of hard-wired equipment, reducing error, repair time and wasted parts.



Diagnostic software and computer interface for power plant equipment.



Icon-based large-area monitor interface systems working in multitasking environments such as Microsoft Corporation's Windows T.M. operating system, offer a "big-picture" macro view of a territorial map, while allowing the technician to "zoom-in" on particular sites, systems or subsystems. Hopefully, such monitor/control/display systems will meet the standards to be set forth very soon by the T1E1 standardization committee. As such, systems should be interactive with other network support systems over a packet-switched digital network using similar protocols.

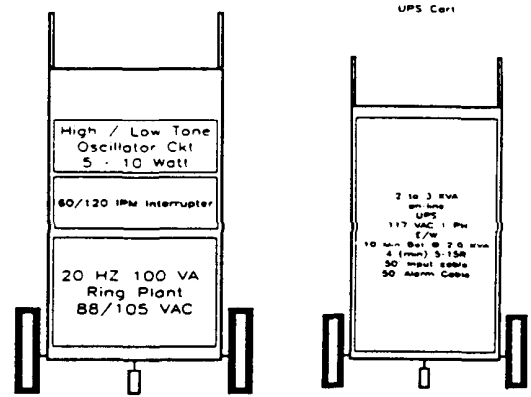
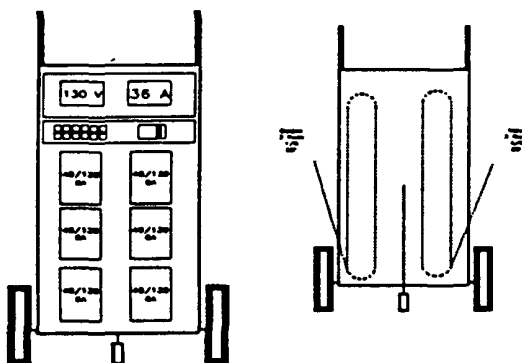
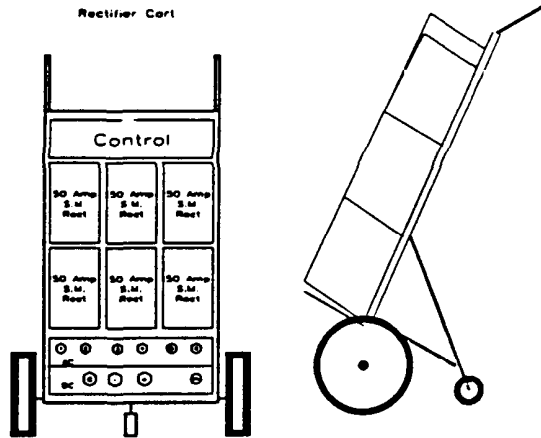
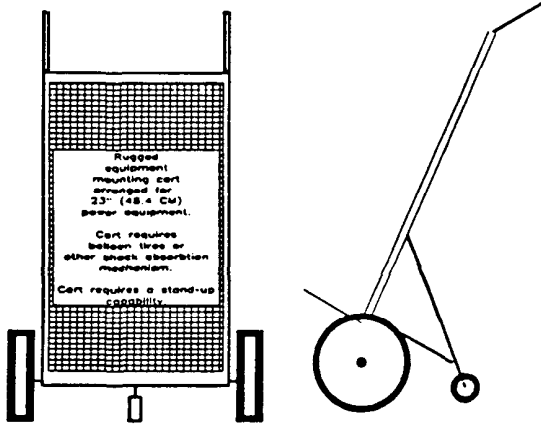
Documentation

Many engineers and maintenance technicians would like to see technical support literature on floppy disks or CD ROM. These could be carried in a laptop computer or loaded in a centralized computer base. A technician with his or her laptop, could keep a copy of often used literature and dial into their home office for drawings when the site drawings are missing or dated. Using this approach, problems are not exacerbated by a lack of drawings - they'd be available and offer the latest revisions.

Exhibit Courtesy of Ascorm Warren Corporation

Portable Equipment

Portable equipment could be connected to the bus to augment or substitute for rectifiers, inverters, converters, ringing current sources, etc. during repair efforts. This provides increased fault-tolerance. Switchmode equipment makes such a possibility very easy to achieve because of its' small size and weight. Portable equipment could also be used transitionally, to augment a viable power plant while a new switching machine is put into service.



Conclusion

Telecommunications executives operating in today's distressed global economy face many threats. The economy has depleted their customer base, the downsizing of large telephone companies has depleted their talent pool. They face stiffer competition than ever before because there are many more players in this game, and they hire from a broad pool of available talent.

Retired doesn't mean tired anymore. In recent years, many telephone professionals leave their jobs, voluntarily or otherwise, in their forties and fifties. Many have twenty or more productive years to sell. Companies can hire these employees for lower wages because their incomes are virtually subsidized by pensions. It's tough competing against people you've trained to be the best.

Equally daunting is a looming potential for regulatory restraint as government agencies become increasingly intolerant of a brittle telephone network.

These challenges can only be met by making decisions which squeeze returns from micron-thin profit margins, yet provide unparalleled reliability in an environment which is anything but stable or reliable.

Fault tolerant approaches to equipment, procedures and training serve to eliminate or minimize the impact of inevitable equipment problems to the telephone customer. With creativity, such approaches often cost less than present methods of operation. Fault tolerance is a win/win scenario. There is always room in this business for a win/win scenario.