Power On AUSTRALIA

Product Bulletin

Are we next for a BLACKOUT ?

New York, Toronto, London, Copenhagen, Stockholm, Geneva, Rome… Are you next for a blackout?

Jean-Francois Christin, EMEA Sales Promotion Manager, MGE UPS SYSTEMS
– October 2003 –

2003 was the year of the blackout, those giant power cuts that deprive towns and even entire countries of electricity. Although those occurring in New York and Italy were impressive, it should be pointed out that twenty or so lesser power cuts have affected around 550 million people over the last 30 years. Such figures can get you thinking. The increasing likelihood of such power cuts occurring and their sheer scale will have increasingly serious economic consequences.

The causes of such power failures can be grouped into two families, each one without the slightest sign of improvement for the moment: electricity production and transmission that are finding it hard to keep up with demand on the one hand, and climatic phenomena on the other. To these can be added other electrical failures occurring inside a building and which are the cause of most power cuts.

Electricity consumption is rising and infrastructures are finding it hard to keep up

Where production is concerned, we learn something from the case of Italy: the peninsula only meets 83% of its needs[1]. Similarly, the wave of power cuts affecting the American West in 2000 and 2001brought the lack of investment in electricity production sharply into focus. Last June, Japan feared a shortage of 5 million kilowatts in the middle of the summer[2].
The heterogeneity of political and economic situations concerning energy is not favourable to the reliability of electricity production and transmission. In 1987, Italy said goodbye to nuclear energy production in a referendum. Then Germany recently decided to shut down its nuclear power plants. In France, on the other hand, EDF[3] intends to extend the service life of its nuclear plants, which, along with equipment ageing and safety requirements, will undermine their availability. Furthermore, a European directive sets a target of "22.1% of electricity produced from renewable energy sources, to be implemented by 2010"[4].

With respect to transmission and distribution, the same thing has been observed in most countries throughout the world. Countries offering the choice of electricity supplier have yet to make the necessary provisions to ensure proper maintenance of the electricity network. The obsolescence of the North-American network was, in addition to insufficient production, one of the causes pointed out during the famous electricity shortages in California. In Europe, large consumers can choose their supplier. And their distributors can buy electricity according to a daily rate, just like on the stock exchange. The national networks are therefore interconnected and there are more switching operations, which generate sharp spikes. European standard EN50160, which sets the level of energy quality, still represents an everyday challenge for energy distributors. All the more so as there is no regulating organisation to guide overall technical and economic homogenization.

Consequently, when safety margins have not been set up, this means that an entire network can by cut, as in Denmark and Sweden on 23 September last.
It's a well-known scenario. If one of the power plants or one of the lines is cut, the current it was carrying is automatically transferred to other network lines. The circuit-breakers protecting the lines open, the automatic switching systems send the current to other lines, and so on.

When climate is involved

Climatic phenomena have also to be taken into account. Some are quite spectacular: the storms in France in December 1999 deprived some 4 million homes of electricity. In April 1990, cities in the North of Egypt were subjected to power cuts due to sand storms. We might also mention the famous ice rains in Canada in January 1998.
More generally, climatic disturbances, in the form of global warming measured in recent decades, place stress on equipment and imply more energy consumption. The Swedish case showed up a water deficit in electricity dams.

And as if that wasn't enough, most power failures occur inside buildings. In one of its technical booklets, Schneider Electric lists the many types of interference that can affect a low voltage network, to make electricians and designers aware that protection means must be put in place[5]. MGE UPS SYSTEMS estimates that 20% of power failures are due to the untimely tripping of circuit-breakers, 20% to various pieces of equipment breaking down and 15% to human error during maintenance operations.

Caught in a stranglehold between high productivity and dependence on energy: economic players make sure they have protection against power failures.

For companies, power failures put financial factors at stake.
With the constant increase in productivity, the cost of each electricity failure is increasingly high. Such losses cost industry and commerce in the United States 10 billion Euros per year [6]! For example, if the financial trading system stops for an hour, the cost is over six million Euros! [7]

In industry, the way production is organised involves new energy requirements. Production based on demand and continuous processes cannot afford a breakdown at any point on the production line. In the glass-making industry the whole production line has to be properly stopped if any machinery stops working. And if the glass solidifies the plant can be immobilised for several days, the time it takes to clean everything up.

In the semi-conductor industry, the highly technical manufacturing processes and exceptionally expensive materials used leave no room for mistakes. If a power failure occurs and dust gets into the clean room the whole plant has to be shut down. The same applies to many industries with highly automated and computerised production.

There are of course sectors where the stakes are not financial but human. It is not therefore surprising to see that these sectors are the most up-to-date in terms of protected installation design. Air control, for example, shows us the type of measures that can be taken by setting up "resilient" electrical architectures.

High Availability Power Solutions, the key part of the resilient electrical installation[8]

Such installations are seen to be very high-tech. Upstream of the installation we normally find the famous back-up generator. However, there are very few business activities able to withstand switching to this sort of generator. This is why Uninterruptible Power Supplies have become widely used over the last twenty years or so. It is estimated that the world market in UPS was worth 5.2 billion Euros in 2002.

Uninterruptible power supplies render the network insensitive to disturbances by guaranteeing two things: autonomy, thanks to a battery; and voltage quality.
There are several varieties of UPS, outlined in standard IEC62040. This standard distinguishes between three types. With the first type, the voltage and frequency delivered to the application are those of the networks (Voltage and Frequency dependent, VFD); with the second type, the voltage delivered by the UPS is independent of the network voltage (Voltage Independent, VI); the third type, which must be used for sensitive applications, provides total independence with respect to frequency and voltage (VFI)[9]. The use of electronic power components and information technology enables the UPS to act within several milliseconds. The applications are thus completely unaffected.

To guarantee voltage quality another type of innovation is now regularly implemented: the harmonics conditioner. Its role is to meet the widespread use of electronic equipment which tends to deform the voltage. The conditioner acts like a buffer between the polluting applications and the voltage supply.

Another feature of resilience is the double power supply and Source-Transfer System (STS). Here the idea is to have two sources of electricity. Final distribution to the applications is via the STS. Equipped with a genuine mini computer, it continually scans the voltage of the two sources and chooses the best one according to criteria sent to it.
Its advantage is its capacity to switch from one supply to the other without the application detecting a brown-out. This is made possible by thyristors, semi-conductors acting as instantaneous switching devices.
It also isolates applications and keeps them protected while the rest of the installation is under maintenance.

However, to configure these solutions, experts must be called on mastering the complexity of industrial and tertiary electrical installations.

Maintenance and supervision are essential to achieve reliability

Here the idea is to act in two areas: reduce the likelihood of a breakdown and cut down on troubleshooting times when an electrical fault occurs.

Acting on the first involves a certain number of operations: periodically checking equipment, changing components before they reach the end of their service life (just like in the aeronautical industry), and taking regular measurements in order to check how well the installation reacts to problems and monitor its ageing.
Much progress has been made in this area leading to better and quicker measuring productivity and, above all, better identification of invisible faults, just waiting to spread.

The capacity of switchgear to connect up to the computer network makes it possible to supervise and monitor both UPS and STS. There are also switch cabinets able to recover the circuit load in real time. These do away with the need for laborious measurement sheets, which can now be downloaded in a matter of seconds. Even more importantly, an alarm is triggered before the load exceeds the value able to be withstood by the circuit-breakers. Another simple tool is thermographic analysis, which quickly and very efficiently locates faults arising from current unbalance, installation wear or harmonics pollution.

The second area concerns maintenance times. If a failure occurs, a resilient installation enables the application to continue to be supplied. However, it does not necessarily continue to be protected. It is therefore vital to act quickly and prevent the application from working in degraded mode as this would have a knock-on effect, so well known in the world of electricity. Thanks to the IT communication capacities already mentioned, it is possible to receive alarms on a PC or mobile phone. A technician can then be alerted in a matter of seconds and have a preliminary diagnosis of the problem to make his intervention even more efficient.

Blackouts have undoubtedly become more frequent. But the range of solutions available shows that there are means of preventing the risks inherent in a failed electricity supply. Investing in such solutions is just like investing in insurance: the investment must be tailored to the financial risks. The tools used to estimate these risks are available. For large structures, this job involves the finance department, the operations manager (production manager or IT manager) and the site manager.

---

[1] Le Figaro, 29 September 2003

[2] Source: Missions Economiques – Centre Francais du Commerce Extérieur, Lettre de veille internationale « Electricité » (Economic Missions, French centre for international trade, international watchkeeping letter on electricity), June 2003

[3] EDF: Electricité de France

[4] Directive 2001/EC of the European Parliament and Council of 27 September 2001

5 Schneider Electric "Cahier Technique" (technical booklet) no. 141, « Electrical disturbances in LV » , Roland Calvas, May 2001

[6] Power Quality Application Guide – Cooper Development Association Nov 2001.

[7] Ibid.

[8] Resilience n. Phys. Number characterising the impact resistance of a material (Larousse). The Anglo-Saxons refer to a "resilient power supply", i.e. an electrical supply which is impact-resistant and that has resilience. (Harraps). Leonardo Power Quality Initiative, application note 4.1: "A resilient system is a system able to withstand a certain number of sub-system and component failures while continuing to operate normally. »

[9] These topologies are better known as, respectively: off-line or passive-stand-by, line-interactive and on-line double conversion.