Contingency planning evolution

By Shri Karve

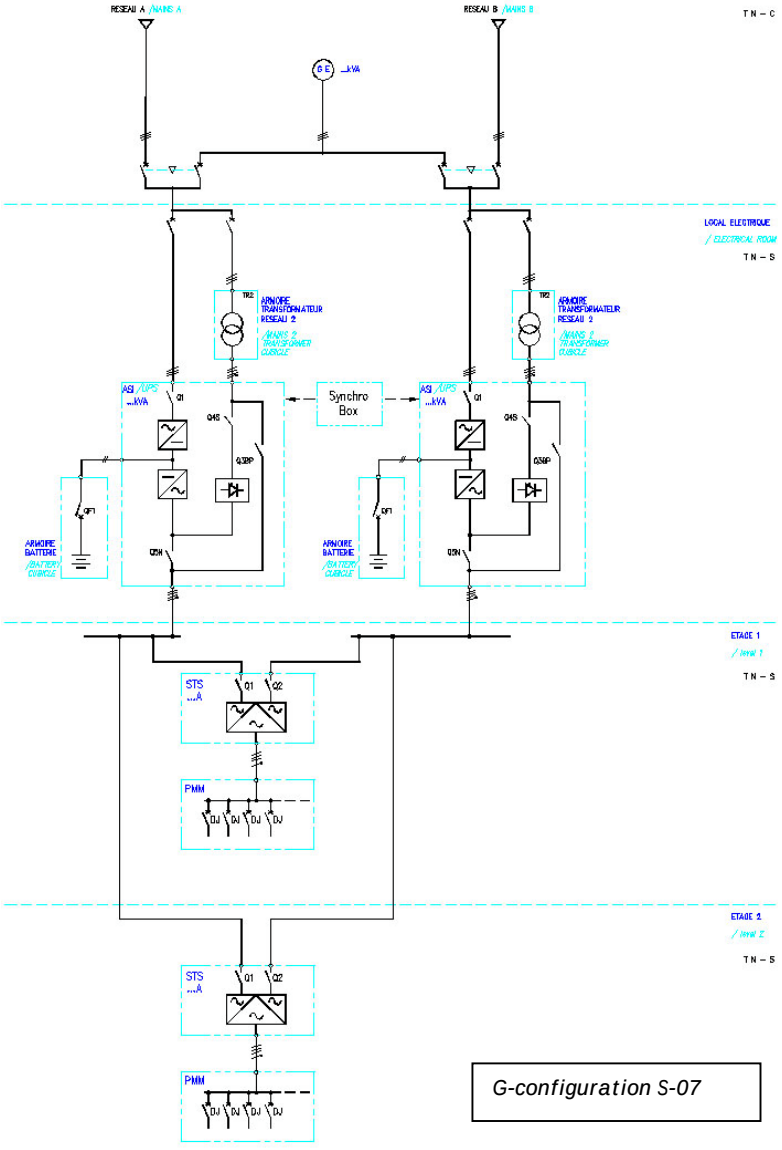
The key to disaster recovery and business continuity today is operational resilience. As the relentless application of technology continues we must attempt to create an arena in which we can protect these technological advancements. Our reliance on 24/7/365 IT availability means that the success of any Disaster Recovery Centre is measured in milliseconds.

Many Disaster Recovery Centre customers come from financial sectors who rely on backup centres for their IT business continuity backbone. Events of 9/11 have focused the minds of the financial services regulators to ensure that all major institutions have suitable contingency plans in operation. In some major countries, especially the USA, CEOs are legally responsible for protecting their organisation's data. Companies that lose their data, for whatever reason, go into liquidation within 14 months of the loss, so the ability to recover data is vital.

However, the key to disaster recovery is not just redundancy; the resilience of the system or the networks is critical. Resilience must be applied to technology at the design stage to ensure continuity even during a cataclysmic event, which may be natural disasters, software problems, cyber terrorism or latent design defects in the electrical and mechanical support systems of the data centre.

Fault tolerance

Most of new multiple data recovery centres are now being built far away from main financial hubs. According to the SwissRE study, over 50% of disasters are weather-related but terrorism is getting expensive too. In view of this, infrastructure and electrical system design needs to be fault-tolerant. For example, a short circuit should not stop the functionality of the whole building. A malfunction such as that should clear itself because of its fault tolerant design which is part of the operational resilience. Since UPSs are at heart of any data centre, a high degree of attention must be paid to resilience in UPS system design.



G-configuration S-07

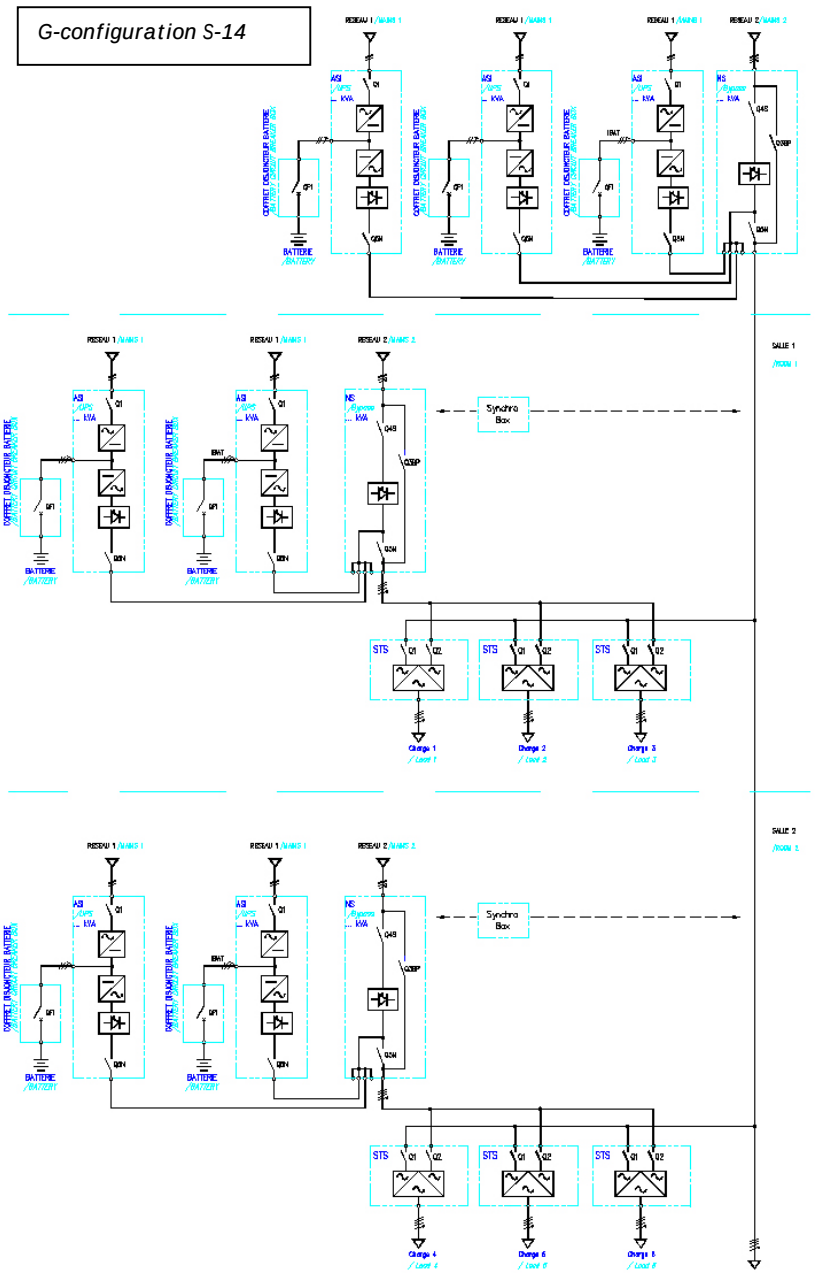
Contingency planning evolution

By Shri Karve

(MTTR) and Meantime Between Failure (MTBF), i.e. Availability = (1- MTTR/MTBF) x 100. MTBF can be increased by means of enhanced equipment reliability and using products that are independently certified by recognised bodies e.g. TUV, KEMA and Veritas. It is important to make sure that both the equipment and the installation as a whole shall be fault tolerant. In view of this, following factory witness tests it is imperative to carry out system integrity (SI) testing that includes all the key components of the Data Centre prior to hand over to client. During the SI testing one needs to simulate faults at various levels within the electrical circuits and the mechanical items within the Data Centre. This type of simulated testing can prove the robustness of the system design, equipment and the installation. SI testing would bring to the fore any issues related to non-compatibility between different packages or equipment.

Protection

MTTR can be reduced by use of remote on-line diagnostics and use of skilled experts carrying out repairs within short space of time. Correct range of spares need to be available on 24/7 basis. Normal utility availability of 99.9 % can result in 9 hours of blackout or several short blackouts and some brown outs. As the utility companies are not required to guarantee continuity, organisations also have to protect themselves against these power losses. Certainly, no financial institution can accept this poor level of availability, so it is essential, therefore, to have data centres backed up with UPS systems and standby generation to protect their core IT infrastructure. It is known that the cost of financial trading system failure for one hour is 6 million euros (Source: IBID).



In order to achieve a high level of resilience with a UPS system, units which comply with dual conversion design as per IEC 62040 must be used. In other words, critical IT load is protected against any power quality issues at the input of the UPS whether it is voltage or frequency related. It is important to note that some of the rotary UPSs, and a small percentage of static UPS may not be of dual conversion design.

Contingency planning evolution

By Shri Karve

Static type UPS

Static type UPSs utilise battery banks to provide adequate back up time to provide cover during Mains loss or poor quality from the utility supply. This allows enough time for the stand-by generators to fire up and support the UPSs. For the large Data Centres it is worth using ten year design life batteries in accordance with BS6290 Part 4 1997 standard. It is also necessary to install a battery monitoring system that is based on Impedance-check technology. However it is very likely that in few years time the battery banks will be replaced with Fuel Cell technology.
Battery autonomy can be based on requirements set by the client, but 10-15 minutes is the common figure used in this type of industry. Standby generation is also essential to cover for long outages and also to support non-essential loads, for example, air conditioning, lighting, and so on.

It is good practice to have n+1 redundancy even at the standby generation level, whereas it is critical for UPSs to go with n+n redundant design. (If n is the minimum requirement to support the critical load, for example, 2 x 500 kva UPSs, then n+1 redundancy would mean 3 x 500kva UPSs and n+n would mean 4 x 500kva UPS.) It is important to utilise an external centralised static by-pass (CSB) per each parallel redundant UPS system. CSB provides a very high degree of resilience when compared to simple modular parallel UPS systems. The reason being that CSB static switch is rated for the system load whilst the modular type UPS system depends on static switch that is rated only for the individual module rating i.e typically only 20 % of the load !

Blade servers

Since the growth of Blade servers it is good to have generator sets that have excellent compatibility with leading power factor imposed by Blade servers. This will provide added resilience in the event of the entire UPS system going into bypass mode during a mains loss situation. Since most of the IT loads generate harmonics it is good practice to limit propagation of such pollution by using Active Harmonic Filters. This helps to reduce the size of the neutral conductor, i.e., saves copper cost and eliminates fire risk and nuisance tripping of circuit breakers. UPSs need to be provided with suitable active harmonic filters to ensure that the current distortion **(**THDI**)** level is held at 5% or lower, regardless of loading on the UPS system. This would help to meet the anti-pollution recommendation G5/4.

In order to limit the damage caused due to a faulty source the static load transfer switches (STS) need to be used at power distribution unit (PDU) level so that any fault is limited to that part of the circuit and system resilience is not affected. These STS units are very fast acting (2-10 millisecond switching time) hence they can switch the critical load from one source to the other without jeopardising functionality of the servers.

In-built design

Each UPS system needs to have built-in redundancy and resilience at the design stage. Once the design is checked for any dormant or hidden points of failure, it is good practice to carry out factory witness tests for each individual item, i.e., UPS systems, switch gear, standby generator sets and so on. Even during factory witness testing it is good practice to simulate short circuit on the load side to help measure the fault tolerance level of the UPS system and its components. Also evaluate100% load step performance of the UPS system and standby generators. It is recommended that suitable critical component monitoring systems such as UPS battery banks monitoring are deployed, as this type of monitoring would help the Facilities Management team to take proactive steps necessary to avoid an internal disaster in a Data Recovery centre.

Before closing, there is no substitute for planned and regular maintenance which should also include thermal imaging of critical components, for example, UPS**,** batteries during discharge, PDUs and switch gear.