From business continuity to design of critical infrastructures: ensuring the proper resilience level to datacentres.

Andrea Giacchero[1#], Francesco Giordano[2*], Massimiliano M. Schiraldi[3*]

[#] Risk Management, Cassa Depositi e Prestiti S.p.A
Via Goito, 4-00185, Roma, Italy
[1] andrea.giacchero@uniroma2.it
[*] Department of Enterprise Engineering
Tor Vergata University of Rome
Operations Management Research Group
Via del Politecnico 1, 00133, Roma, Italy
[2] giordano@ing.uniroma2.it
[3] schiraldi@uniroma2.it

***Abstract* – Since a few years, companies that runs business critical applications are increasing their focus on their support infrastructures. Indeed, it is clearly useless to pursue higher systems reliability, when the infrastructure is vulnerable. Aim of this paper is to explore the value of business continuity within the scope of the design of resilient system. The publication of the fifth revision of ANSI/TIA/EIA 942 standard provides operation managers and risk managers with a framework to plan and design resilient infrastructures. It will be shown how to use the aforementioned standard to analyse the gap between the current and the desired resilience level of a system, and suggest the proper steps to reach it, accordingly to the business continuity requirements. This approach was adopted on the case of the power system infrastructure of a primary Italian Application Service Provider, granting 24/7 mission critical services to its customers.**

***Keywords* – Electrical Infrastructure; System Resilience; System Reliability; Business Continuity; Operational Risk; Risk Management; Risk Assessment; Critical Infrastructures; Information Technology support system; Reliability Analysis; Datacentre resilience**

I. Business Continuity and Resilience Strategies

With the ever-changing landscapes of nowadays business environments, organizations face difficult and variable situations, which threaten their profitability and existence. Business is exposed to risks from all directions and in many scenarios: regional power outages, natural disasters, acts of war or even economic downturns can seriously damage enterprise operations. In the last fifteen years, terrorism in New York, London, Istanbul and elsewhere, and natural disasters such as earthquake in Japan or Asian South East Tsunami, heightened the priority of a conscious protection from major business operational disruptions. The worst result in lacking of a shield could be a business disruption or a downtime, whose financial impact can ruin enterprise as a whole. Other important consequences can be market share loss, productivity fall, regulatory non-compliance and reputation damage.

Continuity of operations can be defined as an effort within organizations, aimed to ensure that critical functions keep their operational status, during a wide range of emergencies, including localized acts of nature, accidents, technological or attack-related emergencies. It is the good business practice of conscientiousness of public and private entities responsible to their stakeholders (Federal Emergency Management Agency, 2009). Business continuity management is an actual approach to keep on business service and operations during the occurrence of a disruptive event, IT related, business related, or a natural disaster. It is an on-going priority for all enterprises, and its goals are:

- to quickly respond to any threat;
- to seize each opportunity;
- to avoid expensive downtimes;
- to avert security attacks;
- to lessen impact of other catastrophic events.

Accidents occur from a combination of active failures and latent conditions (Reason, 2008). The damage can be so serious that one or more infrastructure component can break out or be unavailable for a long time, with potential information losses. Furthermore, it is important also to consider the long-term effects of such unexpected events. Business disruptive events still affect operations long after the event itself was solved. This

case is represented by market share loss, share price drop, loss of brand value, damage to company credibility. When disasters occur, the very short run determines whether - and how - an organization will go past it: in 1999 Stead & Smallman already stated that, in order to achieve a long-term businesses survival after a disaster, a short-term continuity of operations is essential**.**

In spite of the impact and negative consequences of disasters on businesses, surveys show that only about two-thirds of large organizations have developed business continuity plans (Williamson, 2007). Probably the main reason of this behaviour could be the trend of top management not to allocate resources on low-probability events, which are often underestimated, regardless of potential impact (Angeletti, *et al.*, 2014). In addition, complexity of the business continuity templates presented by government agencies and consulting firms can be considered a cause of this behaviour (Duncan, *et al.*, 2011). Probably, the lack of an operations continuity culture pushes enterprises to consider their continuity plans as emergency projects and not just a part of a holistic strategy.

Business continuity management hence supports preventing, responding to, managing and recovering from fallouts of an incident or a disruptive event. It assists in maintaining uninterrupted availability of all resources required for essential business operations. Business continuity planning is therefore that part of operational risk management that establishes which are the correct reactions and the best cost-effective measures to be taken when a disruptive event occurs, in order to avoid business interruptions. It aids organizations in staying in business under extreme circumstances and it is a good business practice for public and private entities responsible to their stakeholders (Federal Emergency Management Agency, 2009). Knight and Pretty (2000) showed how the lack of confidence in managers and directors' ability to act promptly and effectively during adversities can drive share values down. Thus, business continuity management represents one of the key responsibilities for the company top management.

The increased attention on this topic led government and regulatory agencies to define requirements and legislative measures to face critical events. In 2003, the British Standards Institution published the Publicly Available Specification n. 56 "Guide to Business Continuity Management", which recommends a holistic approach to draw up a program to increase organisation operational resilience level. In 2010, the US National Fire Protection Association provided the Standard n. 1600, the foundation for disaster/emergency management planning and business continuity programs, both in private and public sectors, suggesting common program elements, techniques, and processes.

A Business Continuity strategy is not simply limited to dealing with disruptive events when they occur: it creates a culture within the organization, which aims to increase resilience level, to ensure stability in products and service delivery. These practices should be carried on even if accidents are considered "normal", due to the increasing complexity and tight bound between people and technology (Perrow, 1994; Cacciabue, 2004). Moreover, business continuity management should not chose likelihood as the main criterion in approaching risks, but it should use business impact instead. Hence, potential loss event types can be classified as follows (Vancoppenolle, 2007):

- failure of an isolated infrastructure element, including single points of failure;
- longer-term interruption of a critical information flow;
- longer-term interruption of a critical business activity chain or business process;
- local longer-term business interruption;
- complete business interruption.

This classification becomes more interesting and reliable thinking that fallouts of an unexpected event usually involve larger impact levels. Again, this underlines why business continuity management should be driven by potential impact, in order to be effective in managing the events. In fact, the immediate consequence of a disruptive event is business damage. The business continuity management should hence address the effect of those events on operations (*e.g.* buildings, computers, networks, machinery, etc.) and solve the issues caused by the events themselves, in order to keep business running. A business continuity management program should be integrated into the company culture and be owned by everyone within an organization, in order to be successful.

While a simple business continuity planning concerns protection of business operations and processes, a resilient strategy extends the boundaries of protection beyond unexpected events and disasters to include any changes from normal business activities, resulting from events, such as mergers, downsizing, market changes or any other circumstance or business request. A resilience program enables a business to protect itself from untoward events and capitalizes opportunities, being resilience the capability to quickly adapt and respond to disruptions and to maintain continuous business operations. This is a prerequisite to minimise operational, financial, legal and reputational risks that arise from a disruption. The goal is to empower enterprises with the capability to promptly adjust and transform business in response to any change in order to manage hazards and opportunities, create competitive position and improve shareholder value. A resilience program contributes to develop effective long-term strategies, ensuring actions perfectly aligned to enterprise's risk aversion.

Resilience is a property intimately related to the organizations ability to avoid, contain and mitigate accidents. Viewed as the "inner capacity of a system, predisposed to a shock or stress to adapt and survive by changing its non-essential attributes and rebuilding itself" (Manyena, 2006) - has three main dimensions (Westrum, 2006):

a) the capability to prevent an accident from occurring;
b) the capability to prevent that an occurred accident spreads its impacts;
c) the capability to recover to the normal state, after an occurred accident.

A resilience strategy plan helps reducing the actual impact of disruptive events to business, through the identification of potential weaknesses. According to the principle of awareness, a resilient system must know what to look for (how to monitor performance) and what to expect (means how to anticipate threats into the future) (Hollnagel, 2009). Thus, first it is necessary to understand which exactly the business requirements are, to survive to an unexpected event and then to plan for overcome challenges that could come at any time. The ability in disaster recovering can also be improved by both pre-event and post-event activities (McDaniels et al., 2008), in order to mitigate and being prepared to the initial impact of a disaster. Thus, the concept of resilience has to be used for strategic decision-making, since it offers a means to consider the relative risk of alternative scenarios. For example, while planning a new hospital in an earthquake zone or expanding a supply chain into a politically unstable area, it becomes important measuring the resilience associated to different strategies - initial resistance or recovery from a possible disaster - in order to choose accordingly between them. Enterprise success relies upon its ability to be resilient, which allows it to take full advantage of changes in its business environment and to anticipate unexpected events and risks, increasing shareholder values and gaining competitive advantage. This approach to resilience can proactively help facing loss event, in order to minimize damages and to maximize return on investment from assets, technology and people right when enterprise needs them the most.

Resilience engineering is the research field that tries to understand complexity associated to socio-technical systems, through studying methods, techniques and tools to raise organizations aptitude to maintain their operations while facing accidents (Hollnagel, Woods, & Levenson, 2006). If a major incident occurs, the organization should be able to maintain the continuity of its operations and protect the stakeholders' interests. Indeed, the main goal of a business resilience program is to protect critical operations, services and resources and to maintain business continuity. A firm should carry out this goal according to a wider vision, which should be systematic and proactive in order to anticipate future business changes and discontinuities. Same vision should lead to implement preventive actions to achieve the firm's resilience targets. A strong business resilience strategy can reduce waste of time and money, since it is a ready-right-from-the-start strategy, not just a routine to recover from unwanted event.

An effective business resilience program, requiring strong efforts in business continuity and disaster recovery activities in order to get the proper resilience level for critical operations, should not forget to focus on ICT infrastructure. Events such as the 9/11 attacks, the Katrina hurricane or other long blackout events, stressed the link between normal business operations and critical infrastructures like power sources and telecommunications. Complex challenges push companies to deal with advanced security technologies, and organizations rely deeply on automation and on those elements of the physical infrastructure that support automation, such as telecommunications, information systems, and electrical systems availability. It is well known that there are several critical systems, such as banks, healthcare systems, communications services, etc. which deeply rely on IT systems. In the financial services industry, a 24/7 uptime is required for computer and network equipment related to trading and banking activities. It is also clear that an Emergency Room cannot tolerate a minimum failure of its technological infrastructure. Protecting a company with investment in information systems is costly but indispensable to survive and stay competitive; thus, the growing reliance on information systems increases the risk of ICT system outage.

Hence, organizations are actively engaged in improving their resilience against major operational IT disruptions. Managing and mitigating risk requires an agile network architecture that can guarantee low latency and high availability for real-time applications, maintaining security in access control at the same time. A company should question which risk represents the greatest threat to continuity of its own business operations, whether it is able to accommodate a major growth in computational workload or how current recovery capacity match peak business processing volumes. It is very important to ensure reliable and timely delivery of critical applications and data and to respond - with flexibility - to changing business requirements.

In 2006 the Basel Committee on Banking Supervision defined the "business resilience" as the skill to absorb the impact of a major disruption while maintaining operational each critical activity or service. It also classified the IT risk as an operational risk, defined as "the risk of loss resulting from business disruption and system failures, related to hardware, software, telecommunications and utility outage / disruptions" (Basel Committee on Banking Supervision, 2006). This underlined a strong correlation between IT and Operational risks: banks, as well as many other organizations, have increasingly linked their business performance to information systems.

The result is that IT has taken a very important and critical role in the operational processes continuity, becoming one of the major sources of Operational risk.

II. IT AND OPERATIONAL RISKS

Nowadays, risk management in Information Technology (IT) operations became critical for day-by-day life in almost any organization; risk exposure within the scope of IT function can have significant fallouts on the balance sheet. IT risk is linked with many aspects of business operations: business environment, quality control processes and information flows. In fact, if operational blackouts, such as computer malfunctions, power failures and transportation disruptions become frequent, customers will reasonably choose to do business with competitors that can promise a higher resilience level. Organizations totally rely on IT infrastructures to protect business from a wide range of security threats, more than just technology failures or disruptions. It is mandatory that organizations be able to provide continuous availability of IT services in case of a disruptive event or outage. Potential reputational damage associated with IT failures may reflect upon the competence of the Risk Management, imposing to organize a suitable plan for business continuity and a disaster recovery program.

From an IT perspective, risk management goal is to analyse potential injuries and threats; in particular, risk management has to:

- assess and determine potential losses due to accidents or disasters in electrical infrastructure;
- implement plans and strategies to deal with the issue of contingency planning, deciding whether a contingency plan or business continuity plan is appropriate for the enterprises;
- develop hardware and software strategies to achieve the best recovery arrangement for IT systems;
- provide off-site storage facilities to ensure that critical data are properly protected.

It is always a balance of costs versus risk: it must decide which the right solution is and how much prevention is affordable or sensible. The alternatives are to allow services interruptions or plan for the recovery time objective and recovery point objective or to create such resilience that there will always be a service. Defining and developing IT resilience planning has undoubted benefits to an enterprise, such as a perfect Business-to-IT alignment and improvements to IT architecture. Another benefit is to help operations managers in their need to design resilient solutions, although disaster recovery managers own the budget for disaster recovery and IT development.

IT is not limited to services supply anymore. An example is given Enterprise Resource Planning software implementations, which currently manage all the aspect of companies' life: human resources, accountability, operations and customer relationship management, etc. These tools, used within most of the medium and large enterprises, need large datacentres and computer communication networks, which need in turn their proper power supply. To increase resilience and redundancy into business processes and systems is the main advice given by legislative bodies and regulatory institutes. IBM approached this topic as well, defining business resilience as "the ability to rapidly adapt and respond to business disruptions and to maintain continuous business operations" (IBM, 2009).

Unexpected events occur quite often because of any organization intrinsic weaknesses: vulnerable IT systems that are "worked around", lack of operator training, process variations, incorrectly followed routines, and so on. While analysing the causes of most major disasters, it was found that there are several factors that, combined together, lead to the damage. IT departments spent a long time putting in place contingency and disaster recovery plans for their systems, such as:

- backing up data files;
- creating off-site storage of critical company records;
- duplicating and making redundancy in critical processing elements;
- establishing system security practices;
- using system/network diagnostic and troubleshooting procedures;
- using operation sites with emergency computer during emergencies.

However, these solutions may not be sufficient: it is clearly useless to pursue higher systems reliability, when the support infrastructure is vulnerable. Availability of IT infrastructure must become the starting point of any IT disaster recovery planning. In 2005, the US Telecommunication Industry Association, one of the leading trade associations of ICT industry, defined the TIA/EIA 942 "Telecommunications Infrastructure Standard for Data Centers" guideline (subsequently acknowledged by the American National Standard Institute, ANSI). This is one of the most renown and followed standard in technical services design. Its use is limited to IT service systems (thermal, electrical, security, etc.). The ANSI/TIA/EIA 942 standard was conceived to support the design a new power infrastructure, not for the resilience assessment of an existing one. Indeed, methodologies and techniques successfully used in reliability engineering to assess the reliability level of an infrastructure, like Fault Tree Analysis (Vesely W. E., 1969) or Failure Mode and Effect Analysis (U.S. Department of Defense, 1949), cannot properly explain failure events triggered by human-infrastructure interaction (Kontogiannis et al.,

2000). For power systems, for example, about 70% of failures seem to be caused by operators' errors (Uptime Institute, 2008) and not by machinery breakouts.

Power systems obviously play a fundamental role in our lives: we depend on electrical systems; just think of air traffic control, traffic light grids, rail networks, intensive care units, patient monitoring, stock exchanges, etc. An unexpected blackout takes out data and communications capabilities and electrical system is inherently vulnerable. It is basic for an organization to understand, assess and manage risks associated to power disruptions to enhance its reliability and guarantee uninterrupted operational services. The risks associated with disruptions of one's own power system pressed directors and managers to increase reliability of technologies. It is indeed very challenging to design and build the most reliable system. In the past it was common to intend the continuity subsystem as a static, standalone Uninterruptible Power System (UPS), which could supply the operational structure only for a limited time; on the contrary, today enterprises are asking for an actual, permanent and unconstrained uninterruptible power source. To ensure such continuity requirement, a holistic approach is required, since all the parties involved should be acknowledged about power system design, about its maintenance plan and about its features.

III. Business Continuity and Design of Electrical system

An electrical structure is a complex system, exposed to many hazards, which can be found in a wide variety of places (e.g. in rural/urban setting, during night-time shifts, under inclement weather, etc.). In order to implement a complete business continuity planning on an electrical system, specific evaluations and a deep analysis should be realized, to install or upgrade critical power facility infrastructure. The analysis concerns power generation, transformers, emergency generators and controls, transient voltage protection, batteries, branch circuits, fire alarm systems, grounding systems, conduit and static transfer switches in response to interrupted power.

The requirement of business continuity under every foreseeable failure requires particular techniques, such as standby power generation, independent battery power sources and automatic transfer switches (*make-before-break* switches). Thus, organizations require sophisticated power systems, generators and other electrical and mechanical systems to ensure business operation: the system designer must define the appropriate system availability level, to evaluate the potential impact of an outage lasting one day, one hour, or just few seconds. An effective business continuity planning should not only consider *short breaks* (less than 5 seconds blackouts), but also *long breaks*, even many-days breaks. The highest criticality of the whole operations determines the reliability of the entire system. The current design approach requires that first, the intended use should be defined, and then the systems should be designed accordingly to the required reliability specifications. Indeed, the critical factors required to ensure a greater resilience to the system should be identified since the design phase.

An ICT-supplying power system suffers from specific issues, different from the industrial machinery world, for several reasons. For example, an electro-mechanic user will experience a downtime period only after a significant power disruption, while an electronic component can be disturbed also from a few voltage quality issues (Dugan, McGranaghan, Santoso, & Beaty, 1996). Moreover, downtime experienced by electronic devices will be probably longer than blackout. Finally, there are higher chances that a single event could influence all the subsystems in an ICT environment. These reasons increase criticality while designing high availability electrical infrastructures. For the ANSI 942 standard, "infrastructure" refers to each technological system related to ICT, from the raised floor up to the thermal systems. The same standard provides useful design criteria to assure a pre-defined resilience level, giving operative suggestions in designing system features, like component redundancy for concurrently maintainability.

To increase the reliability of a power system, the easiest solution is to use redundant parts in proper locations. To evaluate their application result, two techniques of reliability analysis can be used, the Fault Tree Analysis (FTA) and the Failure Mode and Effect Analysis (FMEA). The former is applied since 60's to evaluate safety and reliability while developing projects in which errors are intolerable (Haumptmanns, 1988). It aims to identify every relevant fault cause and the interaction between them. It uses a Boolean logic scheme to describe the failure modes, reporting the relationship between symptoms and components and calculating the main system failure chance (this specific approach is called Probabilistic FTA). A significant advantage of FTA is the availability of a great number of tools that can implement it. The typical use of this methodology is pre-hoc, to analyse design errors (Vesely et al., 1981), despite recently it was also used, post-hoc, to analyse accidents and understand which approach, between a component or a system review, would be more effective in increasing the system resilience rate.

The second approach is used to show potential failures and their overall effects on the system. If it is used for quantitative analysis (FMECA, in which C stands for Criticality), it also helps assessing the criticality of these effects evaluating occurrence probability, detection opportunities and damage severity, through estimation of a Risk Priority Number (RPN) per each subsystem or component (Sheng-Hsien & Shin-Yann, 1996). According

to the cited Military Standard, "FMEA is a method of reliability analysis intended to identify failures, which have consequences affecting the functioning of a system within the limits of a given application, thus enabling priorities for action to be set".

These two methodologies, extensively used for maintenance operations in manufacturing industry, are not easily usable for the evaluation of IT infrastructure resilience. Kontogianis et al. (2000) evidenced that with the FTA time factor is not properly considered. For example, a short blackout might not affect business applications, thanks to the UPS systems; a longer one might not as well as, if using auxiliary power generators. Hence, the occurrence of these events should be computed independently, since the same failure has different fallouts. On the other hand, the well-known flaw of FMEA/FMECA is the qualitative attribution of scores used for RPN calculation, which can lead to radically different results. Indeed, some standards oriented to give uniform scores have been studied and improved along the years, for automotive and industrial automation fields (Society of Automotive Engineering, 2009), but nothing similar has been addressed to auxiliary systems. Moreover, traditional maintenance indexes can significantly vary if dealing with ICT users or plant infrastructure: the mean time to restore a datacentre to its operational status is usually significantly longer than to restore a machinery to its working status (in 2008, the Uptime Institute calculated that the ICT breakdown lasts 4 hours as an average).

IV. ENHANCING ELECTRICAL SYSTEM RESILIENCE: FROM THEORY TO PRACTICE

The ANSI 942 standard classifies four different types of system architectures, or "tiers", each one with specific performance levels. This approach is closer to system engineering vision than to traditional technical approach, therefore being compliant with the holistic view prescribed for operational risk management. The following paragraphs will shortly describe the prescription that a system must have to reach each tier specification. The values of availability performance per each architecture is an "end-user perceived unavailability" and has been statistically computed from the Uptime Institute, based on the log files of 16 primary datacentres along 10 years of analysis.

- *Tier 1 (basic architecture)*: "Tier 1" architecture is only capable to supply its users, without redundancy within or between its subsystems. Every planned maintenance operation must be completed during power off, and every power system failure will cause an operational disruption. Perceived availability statistically results to be 99.67%, correspondent to 28 hours/year of downtime for a 24/7 system. Approximately 24 hours out of 28 are maintenance related downtimes.
- *Tier 2 (redundant capacity components architecture)*: Tier 2 configurations require at least N+1 redundant active components (UPS, power generators, etc.), with a single distribution path. Tier 2 topology does not allow scheduled online maintenance. Moreover, in this configuration some kind of active components failure may however disrupt business continuity. Perceived availability is 99.75%, correspondent to 22 hours/year of downtime. 36 hours every two years are due to scheduled maintenance operations.
- *Tier 3 (concurrently maintainable architecture):* tier 3 architectures, in addition to tier 2 specification, require at least a N+1 redundant configuration for each subsystem. Moreover, two different distribution paths and two different power sources should be designed, with only one active at time. Thus, it is possible to disconnect each component without influencing operational continuity. In order to obtain a concurrently maintainability standard, every user should be connected properly to both distribution lines. Perceived availability is 99.98%, correspondent to 4 hours of down time every 2.5 years, and it is not necessary to disconnect the IT load during the scheduled maintenance.
- *Tier 4 (fault tolerant architecture):* a Tier 4 architecture is designed to have a completely redundant configuration, which ensure that every failure of each component will not be critical for the IT load. Each path must be compartmentalized, therefore a single failure event cannot affect the distribution subsystem. Using this architecture, the operational continuity is granted against each failure and most of voluntary unwanted operations (maintenance errors, sabotages, etc.). Perceived availability is 99.99%, correspondent to less than 4 hours failure every 2.5 years.

This classification can help operations managers in optimizing the total costs of a business continuity plan: if scheduled maintenance downtimes are allowed, according to the plan, a Tier 2 design can be the proper design choice, while, if the criticality requires a full 24/7 operational service, probably a Tier 4 system is needed.

The following paragraphs will show one application of ANSI 942 standard in defining the operational continuity plan within a primary Italian Application Service Provider who was pursuing a business continuity company-wide project, with specific focus on its datacentre operations. The main goal was to check the continuity status ex-ante and to plan how to reach the desired resilience level.

The first step for the continuity plan was to define the system requirements: the site should be operational 24/7 without a single interruption; each downtime, regardless of its duration, lead to high penalties, due to its critical importance in the customers' business. This leads to get "*five nine"* availability level (i.e. 99.999%) for

its IT system, so its infrastructure should grant greater availability. This target is almost unreachable, since it would mean not a single failure within 45 years; hence, the firm goal is to maximize the availability rate, starting from its infrastructure.

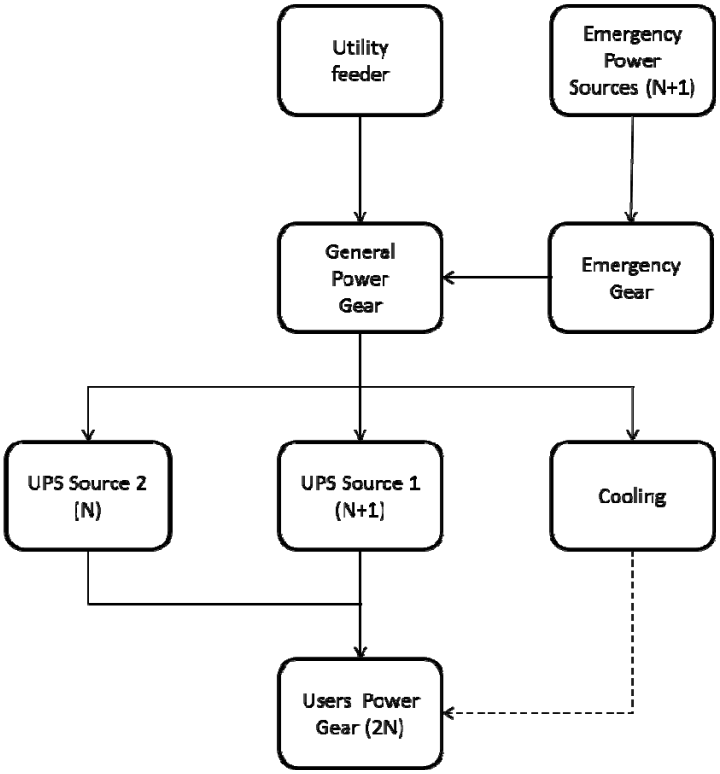

Figure 1. The system in its original configuration

Such operational continuity level should rely on a Tier 4 infrastructure, according to the ANSI 942 standard. Originally, the company infrastructure reached the Tier 2 only, as evidenced during the initial assessment: it has a single line distribution and no redundancy in power sources or utility feeders. Moreover, capacity of one UPS power system was close to be saturated by the IT system: without that UPS system, the architecture would have resulted to be analogous to Tier 1 scheme. This resilience level was considered not adequate from the company's management. Thus, to improve the system resilience, the company developed a plan to enhance the structure up to a Tier 4 (so-called "fault tolerant site" – less than 1 failure in 4 years, according to the Uptime Institute statistics). The technical infrastructure included the 2,000-ampere-consuming datacentre (one of the largest datacentre in Italy), a 6,000-BTU-dedicated cooling tower system, two UPS sources, one set of 4.4 MVA power generators and a Medium Voltage feeder.

Clearly, given the size of the analysed electrical system, the company's management perfectly knew that moving from a Tier 2 to a Tier 4 architecture would have demanded a huge economical effort. However, the main issues found while trying to implement the operational continuity plan was given by another, obvious, requirement: neither the IT service continuity nor its resilience should have been negatively affected during the performance of works. The project plan for the improvement works reported a two years schedule. This issue represents an example of the typical difficulty that companies need to face, when practically trying to implement the theoretical recommendation included in third party's guidelines. The ANSI 942 standard can help in supporting the architectural design of a system, letting the ISO/IEC/IEEE standards define the technical features. However, while this approach is handy in the design phase, its use while the system is already alive can be actually challenging.

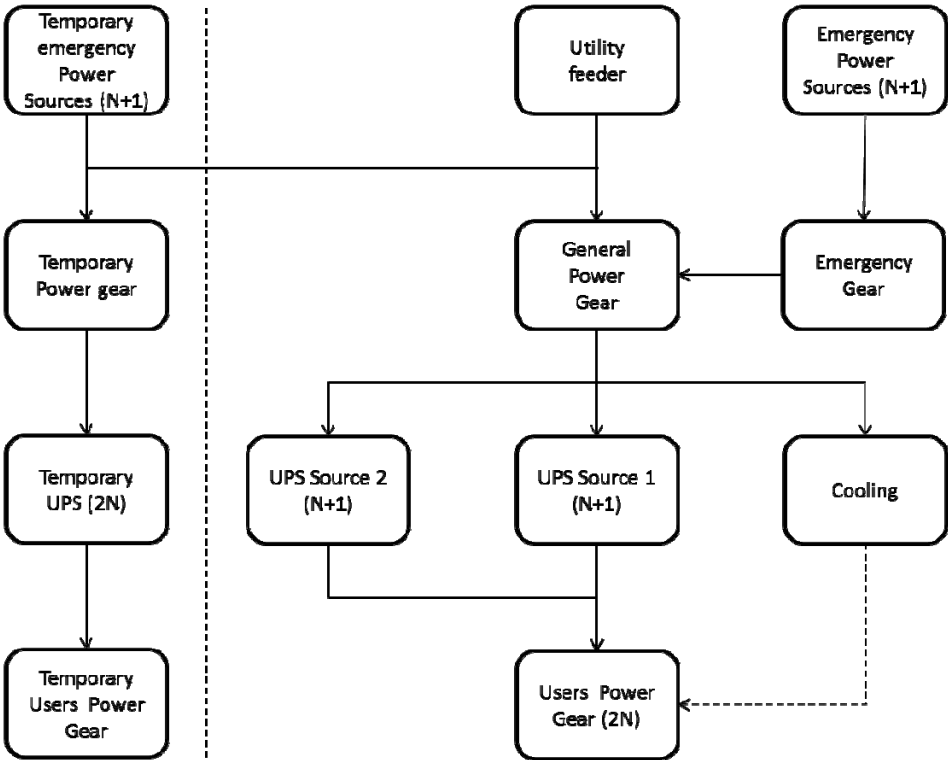

Figure 2. Evidence of the temporary solution

The company had to plan carefully the project for improving the resilience level of its electrical infrastructure, adopting a temporary solution to ensure a secondary redundant power source to some critical IT systems during the enhancement works. This temporary solution included the purchasing of dedicated equipment, including an extra set of 400 kVA power generators, a physically isolated UPS source and extra electric gears connected by an independent supply line.

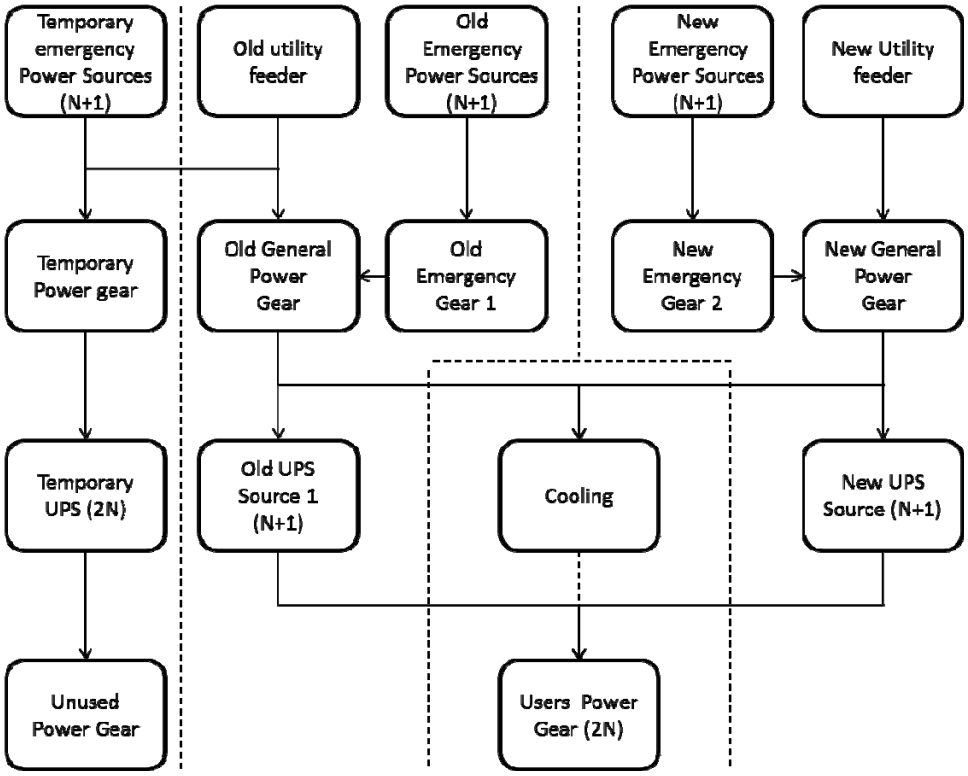

Figure 3. The system in Tier-4 configuration, along with the temporary solution

The works were divided in the following main steps:

1) analyse each electrical load in the main datacentre and, for each one, compare its criticality level with the requirement of a Tier 4 infrastructure;
2) separate each non-critical IT system from the main datacentre, identifying a Tier 2 sub-system; after this step, the load requiring Tier 4 infrastructure was reduced by 30%;
3) deploy the temporary solution and connect it to the critical IT system as a redundant power source;
4) realize a whole new line, with new utility feeders and auxiliary power generators, as the second distribution path required by the Tier 4 scheme;
5) revamp the old line, adapting it to serve as the first distribution path of the Tier 4 scheme.

The temporary solution was scheduled to remain operative for more than one year. The cost of the adoption of the temporary solution accounted for about 20% of the budget for total improvement works.

The temporary solution, not compliant to a Tier-3-grade system, was kept for future expansions of the datacentre capacity, but is currently unused.

V. CONCLUSIONS

In this paper, we highlighted the importance of the business continuity in the IT world. An adequate operational risk management strategy is the key point to reach the highest continuity levels, as required by customers' service level agreements and by regulatory organization such as, for example, the Basel Committee.

It was underlined how the technical infrastructures are currently the main weaknesses of the complex IT environment. A lot of concern is given to protecting IT services from viruses, worms, denial-of-service attacks and every kind of malware software. However, it is often much easier to sabotage the electrical infrastructure of a company than to penetrate its information system with any sophisticated application-layer intrusions. On top of this, power systems are exposed to blackouts and other natural disruptive events, so a great attention should be given to them.

Many companies are still not prepared to face these challenges while keeping their own business operational. The ANSI/TIA/EIA 942 standard is clearly a good starting point, since it does not give engineers the state-of-art regarding the technical problem, as in the classical ISO/IEC/IEEE recommendations and standards; instead, it gives a systemic and holistic view of the system, focusing its attention on the resilience aspects of system design.

This approach was proven to reach its goal not only in "green field" cases, but also if some systems are already operational on site. On the other side, it was also proven that the first implementation of an operational risk management strategy is a challenge for the company and requires a strong commitment by top management. In fact, the transient state can take quite long and it can drain many resources, although at the end of the path, its results can lead to grant real continuous service.

VI. REFERENCES

[1] Angeletti, C., Giacchero, A. & Schiraldi, Massimiliano M. (2014). Managing rare and undetectable events in risk assessment: the case of a satellite system launch project, *International Journal of Project Organization and Management*, 6 (1/2), to appear.
[2] ANSI/EIA/TIA-942. (2008). Telecommunications Infrastructure Standard For Data Centers – Rev. 5.
[3] Basel Committee on Banking Supervision (2006). *High-level principles for business continuity*, The Joint Forum, August.
[4] Basel Committee on Banking Supervision (2006). *International Convergence of Capital Measurement and Capital Standards. A Revised Framework*, June.
[5] British Standards Institution, Publicly Available Specification n. 56 (2003). *Guide to Business Continuity Management*. London
[6] Cacciabue, P. (2004). *Guide to applying human factors methods*, London: Springer.
[7] Dugan, R. C., McGranaghan, M. F., Santoso, S., & Beaty, H. W. (1996). *Electrical Power Systems Quality*. New York: McGraw Hill.
[8] Duncan, W. J., Yeager, V. A., Rucks, A. C. and Ginter, P. M. (2011). *Surviving organizational disasters*, Business Horizons, 54, pp. 135-142.
[9] Federal Emergency Management Agency (FEMA), 2009. *Continuity of operations division*. Retrieved from http://www.fema.gov/about/org/ncp/coop/index.shtm.
[10] Haumptmanns, U. (1988). Fault tree analysis for process industries engineering risk and hazard assessment. *Engineering Risk and Hazard Assessment , 1*, 21-59.
[11] Hollnagel, E. (2009). *The four cornerstones of resilience engineering*, in Nemeth C., Hollnagel E., Dekker S. (Eds.), Resilience Engineering Perspectives: Preparation and Restoration, vol. 2. Ashgate, Burlington, pp. 117-133.
[12] Hollnagel, E., Woods, D., and Levenson, N. (2006). *Resilience engineering: Concepts and precepts*. Hampshire, England: Hashgate.
[13] IBM (2009). *Business resilience: The best defense is a good offense. Develop a best practices strategy using a tiered approach*, IBM Business Continuity and Resiliency Services, January.
[14] Institute of Electrical and Electronical Engineers (2007). IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. IEEE Standard 493-2007.
[15] Knight, R. F. and Pretty, D. J. (2000). *The I1npact of Catastrophes on Shareholder Value.* The Oxford Executive Research Briefings. Oxford: Templeton College, University of Oxford.
[16] Kontogiannis, T., Leopoulos, V., & Marmas, N. (2000). A comparison of accident analysis techniques for safety-critical man-machine systems. *International Journal of Industrial ergonomics* (25), 327-347.
[17] Manyena, S.B. (2006). *The concept of resilience revisited*, Disasters, 30, pp.434-50.

[18] McDaniels, T., Chang, S.E., Cole, D., Mikawoz, J. and Longstaff, H. (2008). *Fostering resilience to extreme events within infrastructure systems: characterizing decision contexts for mitigation and adaptation*, Global Environmental Change 18 (2), pp. 310-318.
[19] National Fire Protection Association (2010), 1600: Standard on disaster/emergency management and business continuity programs. Quincy, Massachussets, US.
[20] Perrow, C. (1994). *The limits of safety: The enhancement of a theory of accidents*, Journal of Contingencies and Crisis Management, 2(4), 212.
[21] Reason, J. (2008). *The human contribution: Unsafe acts, accidents and heroic recoveries*, Surrey, England: Ashgate.
[22] Sheng-Hsien, T., & Shin-Yann, H. (1996). Failure mode and effects analysis - an integrated approach for product design and process control. *International Journal of Quality & Reliability Management , 5* (13), 8-26.
[23] Society of Automotive Engineering. (2009). *J1739.* SAE.
[24] Stead, E. and Smallman, C. (1999). *Understanding business failure: Learning and un-learning lessons from industrial crises*. Journal of Contingencies and Crisis Management, 7(1), pp. 1-18.
[25] Uptime Institute: Turner, W. P., Seader, J. H., Renaud, V., & Brill, K. G. (2008). *Tier Classification Define Site Infrastructure Performance.* Santa Fé: The Uptime Institute.
[26] U.S. Department of Defense. (1949). *Procedure for performing a failure mode effect and criticality analysis.* United States Military Procedure, MIL-P-1629.
[27] Vancoppenolle, G. (2007). *What are we planning for?*, in Andrew Hiles (edited by), "The Definitive Handbook of Business Continuity Management", Second Edition, John Wiley & Sons, Ltd.
[28] Vesely, W. E. (1969). *Fault tree handbook.* Idaho Falls, IN-1330: Idaho Nuclear Corp.
[29] Vesely, W., Goldberg, F., Roberts, N., & Haasl, D. (1981). *Fault Tree Handbook.* US Nuclear Regulatory Commission, System and Reliability Research Office of Nuclear Regulatory Research. US Nuclear Regulatory Commission.
[30] Westrum, R. (2006). *Resilience typology*, in Hollnagel E., Woods D., Leveson N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, London.
[31] Williamson, B. (2007). *Trends in business continuity planning*, Bank Accounting and Finance, 20(5), pp. 50-52.