http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 15 to 16, 2015
Lima – PERU

D2-02_01

Disaster Recovery in the modern EPU

By

Lhoussain Lhassani(*) & **Herwig Klima**
Stedin **Verbund**
The Netherlands **Austria**

SUMMARY

The occurrence and impact of natural or human caused disasters in recent years has proven that even the most prepared electrical power utilities experience unexpected difficulties in facing these extraordinary situations. The power system operation and in particular its recovery from disastrous failure relies extensively on communications and information systems. It is therefore essential for power utilities to have robust and resilient telecommunication and information systems infrastructures, fast deployment communication facilities, and adequate work processes for dealing with emergency situations.

The work of Cigré WG D2.34 aims to provide a background for Business Continuity Management for Electric Power Utilities (EPUs) from the perspective of information systems and telecommunications as well as a comparison of experiences and procedures among utilities in order to set guidelines and best practices for the power community. This paper provides an overview of the work accomplished by the members' contributions.

KEYWORDS

Business Continuity, Disaster/Disaster recovery, Risk Assessment, BIA.

Stedin Netbeheer B.V. Postbus 49, 3000 BN Rotterdam – The Netherlands
E-mail: Lhoussain.Lhassani@Stedin.net

1. Introduction

An extraordinary situation (disaster) occurs when the nature of an incident is such that it actually interference or poses a significant risk to an EPU's critical business objectives. Telecommunication and the related information systems are one of the key topics within EPU's. There is a considerable degree of automation as well as this degree is still increasing.

2. Supported services & possible disasters

Different application-oriented service categories can be identified. Some of them can be identified as critical, other less critical.

- Operational Services: SCADA, Teleprotection.
- Operation Support Services: Maintenance and support of the Power System infrastructure.
- Security, Safety and Environmental Services
- Corporate Communication Services: Administration and corporate needs of the Utility organization and its employees.
- Business and Market Communication Services
- Commercial Communication Services

3. Planning for Business Continuity in EPUs

3.1 Establishing the context

Major incidents and disasters have various origins and can be initiated by various events such as:

- Climatic (e.g. cyclone/hurricane, snow storm, lightning).
- Earthquake/tsunami,
- Bushfire
- Fire (Building, Office)
- Flood
- Cyber related (targeted or accidental)
- Sabotage
- Human error

Communication and other systems are essential for the re-establishment of the power system after any major disruption; it must be particularly robust, geographically redundant, and tolerant to many anomalies in its constitution. As a "National Critical Infrastructure", the Utility is subject to state-specified obligations assuring rapid recovery of the electrical power in case of major disasters.

The Business Continuity Planning (BCP) is based on:

- Maintaining, resuming, minimizing the impact of a disaster and recovering the business. It is more than a recovery of the technology.
- A Business Impact Analysis (BIA) and a Risk Assessment.
- Regular real testing.

3.2 The process of Business Continuity Management

The BCM process has to be defined on different levels within the organization:

Stedin Netbeheer B.V. Postbus 49, 3000 BN Rotterdam – The Netherlands
E-mail: Lhoussain.Lhassani@Stedin.net

- Strategic level: Policies, scope and preconditions are defined here. The process is formalized and its organization is agreed. Responsibility and ownership of BCM is part of this level.
- Tactical Level: The decisions taken at Strategic Leven are the framework of structure of BCM. Parts of this responsibilities are:
    - Requirements and guidelines
    - Risk assessments
- Operational Level: Predefined process at Tactical Level is realized here:
    - Preparation and implementation of the needed measures.
    - Assuring the agreed service levels

Figure 1: Business Continuity Management - Overview
[Source: Business Continuity Institute]

Steps in the process of a disaster recovery

1. Protect: Protecting the ICT environment from environmental problems, hardware failures, operations errors, malicious attack and natural disasters is critical to maintain the desired levels of system availability for an organization.
2. Detect: Detecting incidents at the earliest opportunity minimizes the impact to services and reduces the recovery efforts.
3. React: Reacting to an incident in the most appropriate manner leads to a more efficient recovery and minimizes any downtime.
4. Recover: Implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first.
5. Improvement: Lessons learned from large and small incidents should be documented, analyzed and reviewed. Understanding these lessons allow the organization to be better prepared to control and prevent incidents and interruptions.

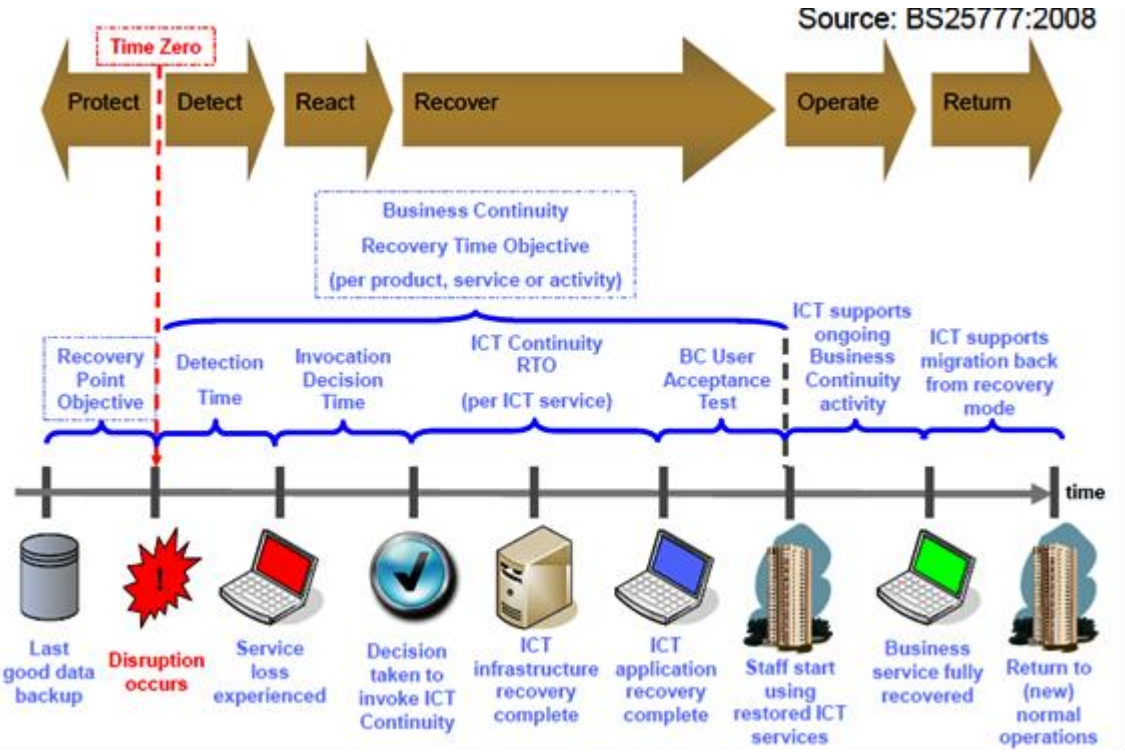

Figure 5: processes regarding critical ict infrastructure

3.3 Establishing a Risk and Vulnerability Analysis Framework

EPUs must understand their critical objectives in order to deal with a disaster. Hence a risk rating methodology that quantitatively aligns its critical business objectives is indispensable.

The Minimum Business Continuity Objective (MBCO) has to be defined. MBCO is the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster. It is set by the executive management of the organization and can be influenced, dictated and/or changed by current regulatory requirements or industry practices. (*Source: Singapore Standard 540 - SS 540:2008*)

The goal of BCM is to keep operation above the MBCO level, even facing a major incident:

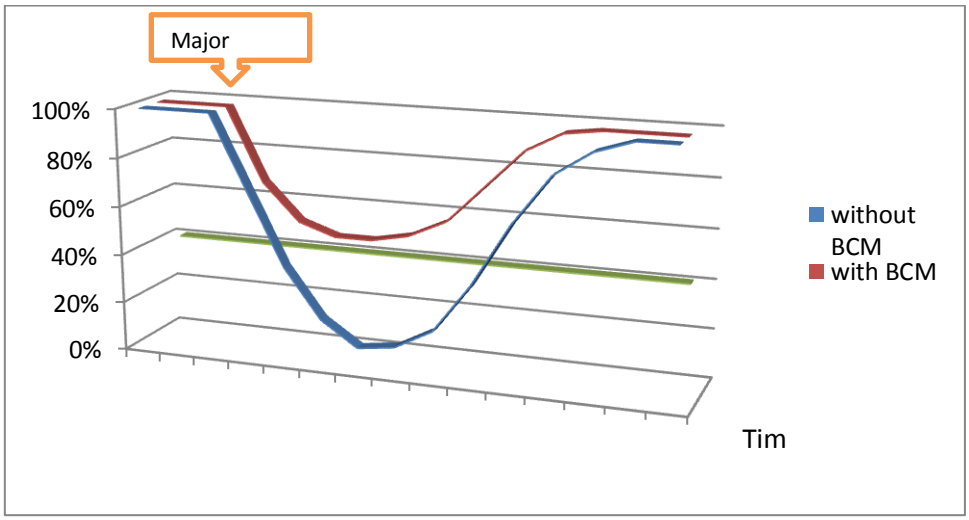

Figure 3: Each critical activity has its own MBCO.

Stedin Netbeheer B.V. Postbus 49, 3000 BN Rotterdam – The Netherlands
E-mail: Lhoussain.Lhassani@Stedin.net

Having a Business Continuity Plan and a Disaster Recovery Plan is vital for the organizations activities. In simple terms, the BCP/DRP are developed to help the organizations keeping their business running, completely or partially, in case of disaster, defining roles and action plans in the recovering process, so it can be made more rapidly and efficiently.

As a part of the BCP, a good DRP for telecommunications is needed to ensure an effective response to a disaster that affects telecommunications services and minimize the effect on the business. The major goals of the DRP are:

- Minimize interruptions to the normal operations.
- Limit the extent of disruption and damage.
- Minimize the economic impact of the interruption.
- Establish alternative means of operation in advance.
- Train personnel with emergency procedures.
- Provide for smooth and rapid restoration of service.

To achieve these goals, the most important factors that it shall take into account are:

- Communication: Notify all key players for a certain problem and assign them a task toward the recovery plan.
- Customers - Notifying clients about problems minimizes possible panic.
- Tools: Be sure that the plan includes the identification and access to all the tools needed for the recovery, such as manuals, procedures, applications, devices, privileges, etc.
- Backups: Backups should be stored in separate locations. If backup resources are taken offsite, these need to be recalled. If you are using remote backup services, a network connection to the remote backup location (or the Internet) will be required;
- Facilities: Having backup sites (hot or cold) and mobile recovery facilities are also good options;

Testing the plan: provisions, directions, frequency for testing the plan should be stipulated

After identifying the potential impacts of disaster and to understand the risks and construct the BCP plan itself, in order to realize business continuity, the BCP must be not only established but also continually updated and maintained in a "Plan", "Do", "Check" and "Act" basis, to ensure that it remains appropriate to the needs of the EPU in terms of covering the measures and action plans to meet the Recovery Time Objective.

3.4 Conducting Business Impact Analysis for credible disasters

The key methodology to apply in order to decide appropriate business continuity processes and plans is the conducting of a risk based business impact analysis:

- Recovery Time Objective (RTO), Recovery Point Objective (RPO), analysis templates
- Results used in technical design and in the performance requirements of the ICT business continuity plans.
- Implementation of the results mentioned above
- Testing and going into operation state

As a result of a business impact analysis (BIA) and risk assessment, the organization must identify measures to:

- Reduce the chance of an interruption
- Shorten the interruption period
- Limit the impact of a disruption in the organization's key products and services

4. Building Disaster Preparedness into ICT

For the telecommunication and information technology must be considered three aspects. First the ICT is a basic service for normal and high secure operation of EPU's. Second the ICT is very necessary to recover from an disaster. And third a disaster in the ICT normally causes a disaster in the EPU's core business as well.

A viable continuity operations plan needs to include:

- a succession plan and delegation of authority
- alternative facilities
- safekeeping of vital records
- security
- interoperable communications
- a regular continuity of operations plan training, testing and exercise plan

Enhancing the emergency response capacity

Considering the measures for strengthening emergency response management of power communication network will enable to provide a more efficient and fast recovery process. Some of the most important measures are listed as follows:

- Improve contingency plan under various organizational entities and at various levels
- Prioritize the critical services
- Strengthen the integration, storage and sharing of emergency response resources
- Emergency response maintenance systems and talent team for fast response
- Adjust planning and improve communication network structure
- Adopt network deployment method for improving availability
- Adopt technologies with less risk of failure (radio, satellite …)
- Invest on disaster recovery support systems to improve time response

5. Conclusion

Business continuity management and disaster recovery is essential for companies, especially for EPU's. A disaster can mean the end of a company, when there is no appropriate preparation. The recovery procedures will need good preparation and trained staff.
The final Technical Brochure can be a good guideline where the user can get a benchmark of several approaches to this theme as well as inputs in technical and hints for rules in an international context.

Stedin Netbeheer B.V. Postbus 49, 3000 BN Rotterdam – The Netherlands
E-mail: Lhoussain.Lhassani@Stedin.net