Electronics, Communications and Networks
A.J. Tallón-Ballesteros et al. (Eds.)

doi:10.3233/FAIA231235

Research on Business Continuity of Electric Power Information System

Ji MA[1], Li ZHAO and Chongchao ZHANG
State Grid Si Ji Wang An Technology (Beijing) Co., Ltd

Abstract. This article introduces the classification of disaster recovery levels for power information systems and a framework for business continuity construction. Through comprehensive risk analysis and evaluation of the impact on business continuity, recovery capability assessment and disaster recovery strategies were formulated, followed by planning and designing disaster recovery plans and developing business continuity plans. In order to improve the disaster recovery capability of information systems and ensure production safety and stability, the post-disaster recovery effect of power information systems was studied in depth. The power information system disaster recovery plan can effectively ensure production continuity and stability. By using appropriate disaster recovery plans and technical means, highly reliable and continuous information systems can be achieved to ensure smooth operation of enterprises and provide important support for enterprise production.

Keywords. Electric power information system, disaster recovery, Business continuity

1. Introduction

With the continuous deepening of the information construction of the power industry and the gradual expansion of the scope of power grid services, the operation of the power grid in production and operation increasingly relies on various business application systems. The occurrence of regional disasters in the power industry often leads to a large amount of power data damage or loss, resulting in complete interruption of business systems and inability to recover quickly in a short time. It is precisely because of this dependence and the unpredictability of disasters that how to ensure that the power grid can quickly and timely recover information systems and their supported businesses after a disaster event occurs in the information system, and ensure the stable operation of information systems and uninterrupted business[1]. When the system stops working due to accidents (such as fires, earthquakes, etc.), disaster recovery provides the power grid with application switching capabilities, realizes the rapid takeover of the fault system by the disaster recovery-side business system, allows the system functions to continue to function normally, and minimizes the system Stop time, strengthen the robustness of the information system, realize uninterrupted, highly reliable service demands, and ensure the continuity of the operation of core business systems.

[1] Corresponding author: Ji MA, Marketing Business Department, State Grid Si Ji Wang An Technology (Beijing) Co., Ltd., Room 539, 5th Floor, Building C, State Grid Park, Future Science and Technology City, Changping District, Beijing, China; E-mail: 767416854@qq.com.

2. Disaster Recovery Level

Disaster recovery (DR) refers to the establishment of backup systems and data synchronization through technological means such as remote backup centers in the event of natural disasters, cyber-attacks, equipment failures, or other emergencies, to ensure the normal operation of critical business systems and minimize losses caused by disasters[2]. The comparison of levels of disaster recovery is shown in Table 1.

Table 1. Comparison of disaster recovery levels

DR Level	Feature	Advantage	Disadvantage
Data-level	Establish a remote backup or disaster recovery system, such as for databases or files.	Low cost and simple to implement.	Longer data disaster recovery time
Application-level	Deploy application programs in a dual-center primary-backup or active-active mode, with the primary center as the production environment and the disaster recovery center as the backup environment.	Provide complete, reliable, and secure services to ensure business continuity.	The cost is high and more software support is required.
Business-level	Business-level disaster recovery requires full infrastructure capabilities (such as telephone, office location) in addition to the necessary information systems-related technologies.	Guarantees business continuity.	Difficult and expensive to implement, also requires investment in premises costs.

(1) Data-level disaster recovery is a fundamental method that primarily involves establishing remote backup centers to back up data, ensuring no data loss or damage occurs in the event of a disaster. However, if only data-level disaster recovery is adopted, business applications will be interrupted in the event of a disaster.

(2) Application-level disaster recovery is built on the basis of data-level disaster recovery. It establishes identical application systems in backup sites and uses synchronous or asynchronous replication technologies to ensure critical applications are recovered and operational within a permissible time frame, minimizing the impact of a disaster and allowing users to remain largely unaware of its occurrence.

(3) Business-level disaster recovery refers to enterprise-wide disaster recovery that goes beyond necessary IT-related technologies and provides backup for other non-business aspects, such as alternative workplace and office staff. Business-level disaster recovery should not only ensure the normal operation of critical businesses but also provide corresponding emergency measures, such as backup workplaces and temporary office staff, to swiftly transfer operations in emergency situations.

Disaster recovery technology should be guided by business requirements. While establishing backup systems and technological means, specific enterprise needs and emergency measures must be considered to ensure the rapid recovery of critical businesses and minimize the losses caused by disasters.

3. Business continuity of power information system

When facing various disasters or risk events, business continuity refers to the ability of an enterprise to respond and adjust quickly and effectively to ensure normal operations are not affected[3]. The main indicators for measuring the continuity of a highly reliable electric power information system include the Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which respectively refer to the acceptable time for IT system downtime or the recovery time required after a disaster, and the maximum duration of data loss that the business can tolerate.

The methodology for achieving business continuity includes three main stages[4]: analysis, design, and implementation. These three stages consist of seven corresponding steps: risk analysis, business impact analysis, recoverability assessment, recovery strategy design, recovery solution design, business continuity planning, business continuity plan testing and maintenance. The whole process of power information system business continuity is shown in Figure 1.

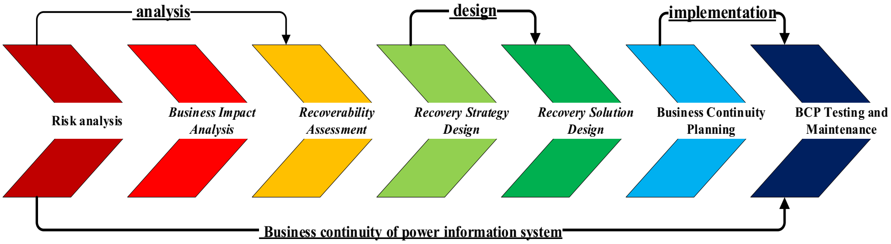
analysis
design
implementation
Risk analysis
Business Impact Analysis
Recoverability Assessment
Recovery Strategy Design
Recovery Solution Design
Business Continuity Planning
BCP Testing and Maintenance
Business continuity of power information system

Figure 1. The whole process of power information system business continuity.

3.1. Risk Analysis

When developing a Business Continuity Plan (BCP), Risk Analysis (RA) is a primary task. RA entails evaluating the major potential threats that a company may face in order to determine the risk level faced by business processes, management systems, and information systems. This includes analyzing various risk factors and proposing corresponding countermeasures and improvement plans, as well as defining preventive measures for risks.

The risk analysis of electric information system is shown in Table 2. Based on the extent of risk damage, these risks can be classified into disaster, malfunction, and security threat risks. To ensure the continuity of the power information system, it must have the capability of automatic adjustment and rapid response to risk. Meanwhile, potential disaster risk events and any unacceptable physical threats that may arise in the current operating environment of the power information system also need to be identified[5].

Table 2. Risk Analysis of Electric Power Information System

Classification	Description	Risk	Risk Disposal
Disaster	Fire, Flood, Earthquake, Landslide, etc.	High	Force majeure, difficult to predict, large impact.
	Severe cold, Bad weather, Lightning strike, Collapse, Tsunami, etc.	Medium	Force majeure, risk response measures can be taken in advance according to the situation.
malfunction	Hardware equipment failure, Application system failure, Technical defect, etc.	High	The risk is relatively large and the scale of impact is relatively small, so prevention schemes need to be established for different systems.
	Fire fighting facilities damage, Site facilities failure, Intentional damage, etc.	High	Large risk and impact scale.
Security threat	Hacker attacks, Viruses, worms, Trojans, etc.	High	Prevention plans need to be established for different systems.

When performing risk analysis, it is crucial to fully consider the business characteristics of the company and the basic features of the information system, as this is the most important part of the entire BCP process. Risk analysis can prevent network failures when unexpected events (e.g. natural disasters, political events, technical malfunctions, etc.) occur, thereby ensuring business continuity of the company. Additionally, risk analysis can also promote improvement of the company's management system and information system, addressing shortcomings arising from upgrades that did not fully meet current needs.

3.2. Business Impact Analysis

Business Impact Analysis (BIA) is a method for assessing the losses caused by interruptions to business operations. It is primarily used to identify the impact on critical business functions and the interdependencies among them. BIA analysis can determine crucial business functionalities, provide a foundation for establishing business recovery priorities and choosing appropriate disaster recovery strategies[6].

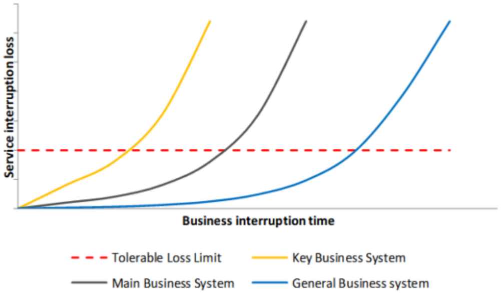

Figure 2. Business Impact Analysis Curve.

The business impact analysis curve is shown in Figure 2. BIA development is mainly assessed by business departments and considers characteristics such as service time, service cycle, and other relevant factors. When establishing the Recovery Point Objective (RPO), the business type and data sensitivity should be considered. If the business is highly sensitive to data, a higher RPO should be implemented; conversely, if the business is not highly sensitive to data, the RPO can be appropriately lowered.

The business impact analysis is shown in Table 3, the analysis results of BIA are crucial for an enterprise's disaster recovery plan. By analyzing critical business functions and their dependencies, it ensures that the enterprise has the ability to quickly restore operations during disasters, thus protecting its productivity and profitability.

Table 3. Business Impact Analysis

Information System Category	Service Description	Maximum Recovery Time
Key Business System	High criticality, high recovery urgency, and significant impact and loss caused by functional business interruption.	4 hours
Main Business System	Medium criticality, medium recovery urgency, and impact and loss caused by functional business interruption are relatively heavy.	24 hours
General Business System	Low criticality, low recovery urgency, and general impact and loss caused by functional business interruption.	1 week

3.3. Recoverability Assessment

Recoverability Assessment (RA) is the process of assessing an enterprise's current recovery capabilities. This process evaluates the technical architecture, backup and recovery processes, and management structure of the information systems that support the enterprise's critical business processes. The recoverability assessment primarily utilizes the results of a business impact analysis as input to assess the current information systems and disaster recovery management status within the enterprise, and to identify gaps between current recovery capabilities and objectives[7].

The analysis of information system resilience is shown in Figure 3. The assessment content mainly includes evaluating the resources required to ensure the normal operation of critical business processes, such as human resources, technical architecture, technical management processes, and network environment. Through this process, the resources associated with each critical business process within the enterprise can be identified. Conclusions can then be drawn to determine whether the current critical business environment can meet the needs of disaster recovery management·

Accurately assessing the recovery capabilities of critical business processes is essential to the survival and development of the enterprise during the recoverability assessment process. To achieve this goal, it is necessary to have a thorough understanding of disaster recovery management knowledge and to review the enterprise's existing management system, identify any deficiencies or weaknesses, and provide specific and effective recommendations.

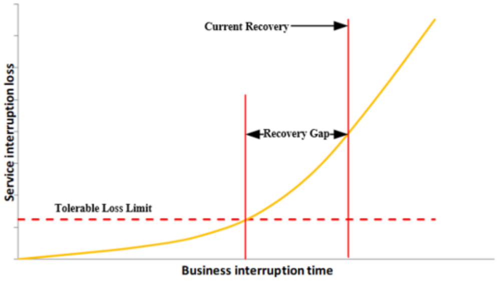

Figure 3. Resiliency Recovery.

3.4. Recovery Strategy Design

Recovery Strategy Design (RSD) involves determining the approach to obtaining disaster recovery resources based on the evaluation results from the previous analysis stage. It also entails analyzing the requirements for the recovery resources and implementing measures and action plans to reduce the gap between current business recovery capabilities and planned objectives[8].

Level 1: Conduct data backup at least once a week, and store backup media offsite. The requirements for backup data processing systems and backup network systems are not specifically defined.

Level 2: Meet the requirements of Level 1, and equipped with partial data processing equipment available for disaster recovery. The backup site needs to be equipped with some communication lines and corresponding network equipment, or to be deployed within a predetermined time.

Level 3: Conduct full data backup at least once a day and store backup media offsite. Key data should be sent to the backup site in a timed batch manner through the communication network. The backup site needs to be equipped with partial data processing equipment, communication lines and corresponding network equipment available for disaster recovery.

Level 4: In addition to Level 3 requirements, it is necessary to equip all data processing equipment, communication lines and corresponding network equipment required for disaster recovery, which are in a ready or running state.

Level 5: In addition to the requirements of Level 3, remote data replication technology should be employed to continuously replicate key data to the backup site in real-time through the communication network.

Level 6: It is necessary to implement remote real-time backup to ensure zero data loss. The backup data processing system should have the same processing capability as the production data processing system, and use "cluster" software to enable real-time switching.

Table 4. Relationship between disaster recovery capability level and RTO/RPO

Disaster Recovery Capability Level	Disaster Recovery Capability	RTO	RPO
1	Basic Support	>2 days	1-7 days
2	Standby Site Support	>24 hours	1-7 days
3	Electronic transfer and partial equipment support	> 12 hours	Hours to 1 day
4	Electronic transfer and complete equipment support	Hours to 2 days	Hours to 1 day
5	Real-time data transfer and complete equipment support	Hours to 2 days	0-30 minutes
6	Zero data loss and remote cluster support	Minutes	0

The recovery characteristics of the disaster recovery capability levels are shown in Table 4. Given the significant differences in requirements for different levels, companies should evaluate their backup and disaster recovery equipment reasonably and select the appropriate level according to their own needs. At the same time, factors such as storage of backup media offsite, selection and construction of backup sites, and reliability of communication networks and equipment are all key elements of disaster recovery equipment. Companies should develop appropriate measures to ensure high reliability, high success rate, and low risk rate of backup and recovery operations.

3.5. Recovery Solution Design

The Recovery Solution Design (RSD) selects appropriate solutions for various information systems based on disaster recovery strategies. The design of disaster recovery solutions requires consideration of many factors including infrastructure architecture, level of digitization, application systems, network configuration, organizational structure, and technical recovery processes[9].

1. Data-level disaster recovery plan

Generally, applications are deployed in the primary data center and data backups are locally implemented. The data to be backed up is transported manually at fixed intervals or saved asynchronously in a remote location using data replication tools. When a fault occurs at the primary center, the data-level disaster recovery plan utilizes backup data in the disaster recovery center to complete data recovery, and once user requests are switched to the disaster recovery center, business operations can be resumed.

2. Application-level disaster recovery plan

The application-level disaster recovery plan primarily uses dual-center primary-backup or active-active deployment modes, with the application being produced in the primary center and served as backup in the disaster recovery center. Only one data center can simultaneously provide read-write access to the same business system, with the other data center serving as a hot backup. Request distribution is achieved through load balancing equipment, and application databases are locally implemented for high availability, while data is unidirectionally synchronized with the backup environment. Any data replication technology may be used. When a fault occurs at the primary center, the application-level disaster recovery plan distributes requests to the disaster recovery center through load balancing. The disaster recovery center database becomes the primary database, synchronizes data with the primary database, and takes over the application at the disaster recovery center to improve business continuity.

3. Business-level disaster recovery plan

In addition to the necessary information system-related technology, the business-level disaster recovery plan must also possess all infrastructure capabilities. This includes backing up non-information technology systems such as phones and offices. In the event of a disaster, the business-level disaster recovery plan can not only recover data and applications in the disaster recovery center but also conduct normal business operations at backup work locations, ensuring that the services provided by the information system are complete, reliable, and secure.

Based on investigations of critical electric power information systems, disaster recovery plans for relevant systems were compiled from the perspectives of system disaster recovery response level, PTO, and RPO for three application scenarios: comprehensive office system, business management system, and production operation system[10]. The power information system disaster recovery plan is shown in Table 5.

Table 5. Power Information System Disaster Recovery Plan

System Name	**Describe**	**Level**	**RTO （/h）**	**RPO （/h）**	**DR Plan**
Integrated Office Application System	Integrate multiple office software and peripherals to improve company collaboration and management efficiency.	Low	24-72	24-36	Data-level
Business Management Application System	Organize resources such as personnel, equipment, funds, materials and information in a rational way and maximize their effectiveness to achieve specific business objectives of an enterprise system.	Medium	12-48	8-24	Data-level or Application-level
Production Operation Application System	The system engaged in production and operation activities in the enterprise, including research and development, production and operation and their supply, guarantee, planning, control and other subsystems.	High	4-12	2-8	Application-level or Business-level

For production and operation application systems, such as production management systems, marketing management systems, asset management systems, financial management systems, human resource management systems, PKI/CA systems, and domain management systems, disaster recovery solutions above the application layer should be adopted. During the recovery process, according to the recovery plan, production and operation application systems should be prioritized, followed by business management application systems, and finally, comprehensive office application systems. Comprehensive office application systems should be periodically backed up in the office environment and archived in paper form, and it may not be necessary to adopt application layer and off-site data disaster recovery solutions.

3.6. Business Continuity Planning

Business Continuity Planning (BCP) is a process and institutional framework derived from the regular operation rules of the enterprise. Its purpose is to help companies effectively respond to disasters, ensure uninterrupted operation of critical business, and maintain the same business processes and organizational structure before, during, and after the disaster to ensure the continuous operation of important critical business[11]. The business continuity planning disaster recovery techniques are shown in Table 6.

Table 6. Business Continuity Planning disaster recovery technology

Key technology	Recovery guarantee	Technical method
Equipment redundancy technology	Automatically switch to backup system for operation in case of hardware failure.	Dual controllers for disk arrays, dual power supplies for servers, disk RAID, dual engines for network devices, etc.
Network communication line redundancy technology	In case of a network fault, services can be quickly switched to the standby network environment.	Multi-route communication line access to the equipment room, link aggregation, Ethernet network technologies (such as RPR, EAPS, ERPS, and RRPP), and network switching technologies (such as manual IP address switching, DNS redirection switching, and load balancing switching).
Node device redundancy technology	The dual-system hot backup or dual-system cold backup technology is used on nodes such as servers, switches, firewalls, and routers.	Dual-system parallel redundancy and dual-system hot backup of the UPS, and server clusters (such as load balancing cluster LBC and high availability cluster HAC).
Data continuity support technology	Adopt data sharing, replication, backup, and recovery technologies to ensure rapid recovery when data is lost or damaged.	Network storage architecture, snapshot, copy, mirroring, replication, deduplication, multipathing software, continuous data protection (CDP) and other technologies.
Application continuity technology	Use technologies such as the "geo-three-center" active-active system (data Active-active network active-active, application active-active) to improve application availability and continuity.	Application server cluster, heartbeat monitoring, drifting IP addresses, cluster software, virtual machine drifting, database clustering and other technologies.
Equipment room facility redundancy technology	Ensure redundancy of key equipment in the equipment room	Power supply and multiple UPS power supply, multiple ground points, N+1 precision air conditioners in the equipment room, and common emergency standby air conditioners in the equipment room

BCP is a systematic engineering project that requires the integration of various technical means mentioned above to ensure that enterprises can effectively respond to disasters. In practical applications, BCP needs to be tested and rehearsed multiple times before it can truly guarantee the continuity and stability of enterprise business in the face of disasters.

3.7. Business Continuity Plan Testing and Maintenance

To ensure the currency and effectiveness of the Business Continuity Plan, it is necessary to conduct tabletop exercises, actual testing, and ongoing maintenance. This includes maintaining daily plans, maintaining results from exercises, maintaining changes made to the plan, and regularly maintaining switch/restore plans. It is important to follow standardized processes and operations based on best practices to ensure the practicality and effectiveness of the BCP[12].

1. Asset Management

Managing the basic information of disaster recovery resource files and disaster recovery relationship files is a prerequisite for achieving data synchronization, exercise contingency plans, and one-click switching.

2. Status Monitoring

Real-time monitoring of the operation status and switch process in the data center and multi-dimensional statistical analysis and visualization of the operation status.

3. Contingency Plan Management

To conduct disaster exercises and timely response to real disasters, disaster recovery relationships are freely arranged, providing a usable sequence for one-click switching when a disaster occurs, improving switching efficiency.

4. Exercise Management

Real-time DR exercises are conducted according to the plan to ensure that the data center environment is truly available. It includes three modules: "Exercise Plan", "Exercise Task", and "Approval Management".

5. Switch Management

Maintaining synchronization tasks, flow configuration, certificate configuration, and other features that support one-click switching to ensure quick response to disasters and timely one-click switching. It includes four modules: "One-Click Switching", "Synchronization Task", "Flow Configuration", and "Certificate Configuration".

6. Backup Management

Developing backup tasks for all data and critical data and achieving data recovery in the event of data loss. The data recovery capability can be verified according to business needs. It includes three modules: "Backup Task Development", "Recovery Verification", and "Recovery Execution".

4. Conclusion

This article explores how to improve the stability and availability of power information systems through disaster recovery mechanisms and business continuity. To ensure the secure production of power information systems, factors such as scale, resource utilization, and operation and maintenance mode should be fully considered. When considering disaster recovery schemes, the complexity of business and actual operation and maintenance conditions should be taken into account in order to maximize the benefits of physical and application disaster recovery. For power businesses with high backup and business continuity requirements, advanced backup technology and disaster recovery solutions should be adopted to quickly and effectively restore data. In terms of physical disaster recovery, more advanced data backup and recovery technologies are conducive to improving disaster recovery efficiency; in terms of application disaster recovery, critical business modules and nodes should be selected for appropriate restoration. In the future, we will continue to research the technology and implementation of power information system disaster recovery to improve the disaster recovery system and better respond to business risks.

References

[1] GB/T 42581-2023, Information technology services Data center business continuity level evaluation guidelines [S].

[2] Liu Wei. Research and Discussion on Disaster Recovery Construction of Information Systems [J]. Digital Communication, 2011 (6): 3. DOI: 10.3969/j.issn.1001-3824.2011.06.016.

[3] Qi Ke, Zhao Hongwei, Pang Songtao. Research on Disaster Recovery Technology System [J]. Digital Communication World, 2023 (2): 185-187.

[4] Du Yu. Research on the design of business continuity evaluation index of electric power information system[J]. Light Source and Lighting, 2022(006):000.

[5] Fan, Huaiwei. Analysis of Information System Business Continuity[J]. Network Security and Informatization.2020(5): 4.

[6] Rubin HBracing for Zero Day[J].IT Professional,1999,1(3):73-79.

[7] Yang Y X , Yao W B , Chen Z .Review of disaster backup and recovery technology of information system[J].Journal of Beijing University of Posts and Telecommunications, 2010.

[8] Feng Y , Hua-Feng Z .Research and Application of Disaster Recovery Technology to Grid Enterprises Information Systems[J].Electric Power Information Technology, 2012.

[9] Fang Lin, Zhang Yuqing, Ma Yuxiang: Business Continuity Security Management Model and Implementation Process for Information Systems [J]. Computer Engineering, 2005,24:180-182.

[10] Yan Longchuan, Zhang Bing, Yuan Xiaoyu, et al. Design and Application of an Automatic Test and Verification System for Power Information System Business [J]. Power Informatization, 2022 (002): 020.

[11] Yang Jun Analysis and Scheme Design of Information System Disaster Recovery Technology [J]. Railway Computer Application, 2022, 31 (8): 5.

[12] Liu Ping, Zhang Jiaju, Zhang Yinping. Research on Business Operation and Maintenance of Electric Power Information and Communication System [J]. Electric Power Information and Communication Technology, 2019, 17 (10): 6. DOI: CNKI: SUN: DXXH0.2019-10-012.