

A Disaster Recovery Methodology for Protecting the Emergency Command Systems

Fei Wang, Xiaocui Zheng, and Shaobo Zhong

Abstract—An emergency command system provides indispensable support for the government to respond the emergencies rapidly, efficiently and scientifically. If the emergency command system is damaged or destroyed due to different reasons such as natural disasters, the system cannot work properly for serving the decision makers. Disaster recovery requirement is very important for the information system, and especially the emergency command system is needed at those critical moments. This paper introduces a disaster recovery methodology through establishing a cloud service center in Guangdong province, China, aiming at the protection of 21 city-level emergency command systems in Guangdong. The ongoing implementation of the cloud service center is described and several data disaster recovery approaches prototypes are briefly explained.

Index Terms—Emergency command system, information system disaster recovery, cloud service.

I. INTRODUCTION

Guangdong is a developed province with a large population in south China coastal area, which suffers many different kinds of disasters such as typhoon and flood. Disasters often cause large economic losses and social influences. Guangdong provincial government attaches great importance to the up to date science and technology to enhance its capability in responding to the emergencies. After years of construction, Guangdong emergency command center was put into use in November 2010, and then the intercommunication of emergency command systems on the province, cities and counties levels were implemented. Whole emergency command systems provide effective support for provincial government to respond to emergency rapidly, efficiently and scientifically.

Emergency command system, if destroyed in disaster, would delay emergency decision and rescue, and cause larger economic loss and social influence. Therefore it is important to establish disaster recovery support system for emergency command. Guangdong cloud service center for disaster recovery, which is a pilot project funded by National High Tech R&D Program of China, aiming at combing Guangdong emergency command system on different levels to set up the required infrastructure. Though linking the 21 disaster recovery points spreading over Guangdong, the center guarantees that Guangdong emergency command system can respond to the unexpected

situation such as information system damage or business interrupt caused by different disasters.

II. GUANGDONG EMERGENCY COMMAND SYSTEM

Emergency command system is a complex information system supporting the emergency response and a tool for the implementation of emergency plans. It is based on public safety science, information communication technology, and emergency management theories, and it integrates a large range of software and hardware together [1]. For a country, the construction of emergency command system is a foundational, long-term, and systemic work. China started this work form 2006, and the system network has been initially established, consisting of the State Council, province-level and department-level (including professional emergency command system), city-level and county-level emergency command systems. The needed heterogeneous information resources have been aggregated, which achieves inter-connection and information sharing, and has basic functions such as video consultation, surveillance video access, emergency communication and coordination. Fig. 1 shows the architecture of China national level emergency command system, and provincial system within a dashed box [1]. It shows that provincial emergency command system is a main unit in the architecture, which is transferring information with other command systems, and playing the important role in the regional emergency management.

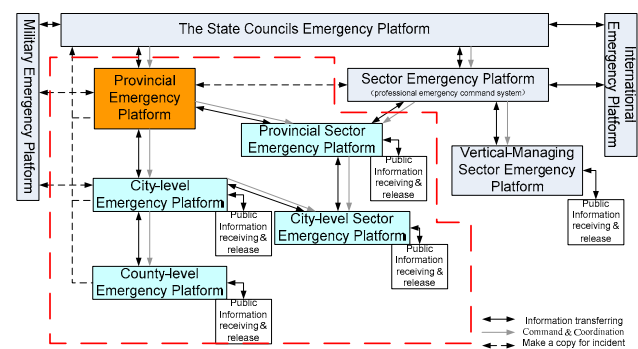


Fig. 1. The architecture of Chinese national emergency command system [1].

In July 2007, Guangdong emergency management office established ‘The Emergency Command System Construction Group’, and officially launched the construction of provincial emergency system. In March 2009, Guangdong chose 19 units as the first batch to carry out exploration and practice in emergency command system construction mode, including Zhuhai, Shantou, Foshan and other cities, as well as Department of Land & Resources,

Manuscript received August 15, 2013; revised October 29, 2013.

Fei Wang and Xiaocui Zheng are with the Graduate School at Shenzhen, Tsinghua University, China (e-mail: wang.fe@sz.tsinghua.edu.cn).

Shaobo Zhong is with the Engineering Physics Department, Tsinghua University.

Department of Agriculture, Department of Health, and Provincial Administration of Work Safety. In November 2010, Guangdong provincial emergency command system and provincial emergency command center were put into use officially. Provincial emergency command system connects the State Council emergency command system upwards, and downwards connects 21 cities and 50 departmental emergency command systems, and is going to connect Hong Kong and Macao government emergency command system, as well as other eight provincial emergency command systems in Pan-Pearl River Delta region. The whole system that implements intercommunication, information sharing, multiple departments' collaboration, is provincial government's operating center to deal with possible situations under emergencies. Provincial emergency command system regards provincial emergency command center as a decision-making platform, general duty-office as an information collecting and distribution center, and mobile emergency command system (mobile vehicle command center) as the complementary and extension of the fixed command center. With the capabilities of emergency telecommunications system, risk analysis, early warning, online consultation, resource dispatching, real time onsite information acquiring, command and coordination, emergency response evaluation, simulation and exercises and others, Guangdong emergency command center meets the needs for provincial government to fulfill the daily duty and face with two contingencies at the same time [2].

Guangdong emergency command system is constructed in accordance with the relevant national standards and a unified framework of security system. As shown in Fig. 2, it has 4 major sub-systems, including basic supporting system, database system, data exchange and sharing system, and integrated application system [3]. Basic supporting system offers basic software and hardware resources for the whole platform, such as database software, storage hardware and others. Database system defines the classification of the needed emergency datasets, such as rescue team, emergency expert, emergency resources and disaster models. Data exchange and sharing system is the foundation for managing the catalog of emergency information resources, and supports information sharing and exchange between all regions and departments. Datasets and emergency messages can be shared through this system. Integrated application system supplies powerful emergency management and intelligent decision-making capacity, such as risk evaluation and early warning functionality. Mobile emergency command system which is designed to meet the needs of on-site command and control in order to achieve unified coordination, for example video conference via satellite data channel to communicate with all levels of emergency command systems. Emergency command center is the command core site, by the means of surveillance video access, emergency communication and coordination, video conference system and intelligent solutions system, for providing comprehensive supports for decision makers or experts to deal with emergencies in the appropriate, efficient and scientific approach.

It can be seen that disaster recovery is a necessary part of emergency command system in Fig. 2. Disaster recovery

system is indispensable for guaranteeing data and all systems safety. It consists of storage, back-up and recovery components and requires hardware and software support. Back-up focuses on data safety, and disaster recovery focuses on business, service and system safety. The center should offer secure access for mobile emergency command system, and can communicate with other emergency command systems through public network. The switching time between disaster recovery center and emergency command system should be as short as possible. In emergency management, the system should work properly, and otherwise it will delay the decision making time. Therefore, it is necessary to find a good disaster recovery methodology for protecting the emergency command systems in all levels.

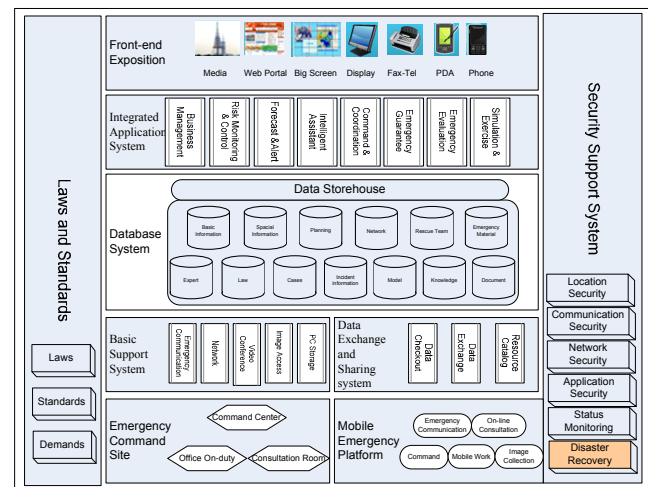


Fig. 2. The architecture of emergency command system [4].

III. PREVIEW OF DISASTER RECOVERY TECHNOLOGIES

A. Traditional Disaster Recovery Technology

Traditional disaster recovery technology mainly uses methods based on data protection to copy the persistent storage status of a protected computer system to a back-up site that is physical isolation. After disaster, back-up system would read back these data to restore to the original status. The tape back-up, remote data mirroring, snapshot and continuous data protection are commonly used the disaster recovery technologies [5].

According to methods that may be used, traditional disaster recovery technologies can be divided into two kinds: one is malfunction switching technology that is represented by data mirroring, and the other is malfunction recovery technology that is similar to traditional back-up [6]. Malfunction switching technology does not actually recover the broken-down system, but uses directly another existing facility to take over services. This method can ensure business continuity, but it needs a fully redundant hardware support, which means large costs to implement. In addition, it can only be switched to an up to date status, and cannot fit the situation that needs historical status. Malfunction recovery technology restores the hardware and software of entire system in the original location, even restores the entire service operation. This method needs not 'One-to-One redundant hardware, and the organizational structure would be more flexible. It can recover to any historical status. Its

disadvantage is taking more time for service recovery, and is difficult to guarantee business continuity.

On the other hand, the traditional disaster recovery is mainly data-level recovery. But the operational status of a computer system consists of disk storage status as well as CPU and memory status, so concerning only with disk storage status will bring some problems about the consistency between application and storage data [6]. The application inconsistency would impact on the data back-up process or data recovery process, while the method of maintaining the consistency between application status and data storage status is always based on knowledge of the application semantics, and is interrelated with specific operation environment, which results a disaster recovery solution strongly depends on application.

Traditional disaster recovery strategies include unidirectional or mutual disaster recovery between emergency command center and disaster recovery center, 'One-to-Multi' disaster recovery for key business, centralized disaster recovery for multiple emergency command centers, and outsourcing disaster recovery, and etc. [7].

Under the trend of more and more information systems, larger and larger data-scale and higher and higher efficiency demand, the contradiction between disaster recovery efficiency and cost has increasingly emerged. Three key questions should be aware: How to avoid re-construction, implement resource sharing and establish a disaster recovery center that suitable for different units; How to avoid relying on special hardware devices, ensure the independence of disaster recovery technology, and adapt to various information systems; How to provide efficient back-up and recovery service by limited resources. To solve these problems, we have to study disaster recovery cloud technologies based on resource sharing, and explore new cloud technologies which are independent of application environment, suitable for resource sharing, and have high efficiency and good expansibility.

B. Cloud Technology for Disaster Recovery

Cloud technology means utilizing clustered application, grid technology and distributed computing to congregate various types of IT resources in network through management software for cooperation, and providing service externally such as computing, storage and business access, etc. Cloud technology is characteristic of virtualization, distributed system and variable granularity [8]. Virtualization means providing a uniform service externally, and being compatible with devices and services from different manufacturers by shielding software and hardware differences internally. Distributed feature makes cloud system become a highly flexible system that supports cross-region, cross-system and cross-application. Variable granularity refers that the cloud service system can integrate various resources and provide different granularity computing and storage services as needed. These characteristics make cloud technology very coincident with the new challenges and demands of information amount, reliability, generality, efficiency, expansibility in disaster recovery area.

The application of Cloud technology in the field of

disaster recovery brings a new concept "DRaaS", which is Disaster Recovery as a Service [9], and allows the development of a number of new technologies. For example, in order to achieve application consistency, as well as to improve the efficiency of system recovery, there comes a series of system-wide replication technologies (such as system transfer technology based on virtualization)[10]. These technologies back up the consistency status of system memory and data, and transfer it to disaster recovery center remotely. After disaster, it does not have to re-configure the operation system, but to transfer the consistency status to the local, and restore system operation directly, which would greatly improve the service recovery speed. In addition, there are data de-duplication technology for reducing data transmitted between users and cloud service center significantly, and cloud storage security technology for improve data security, *et al.* [11], [12].

Meanwhile, the disaster recovery strategy has been changed by the application of cloud technology, and some new strategies such as distributed mutual back-up are put forward [13]. Multiple information systems simultaneously form multiple mutual back-up systems. They work independently at normal time, taking free storage resources among systems to mutually back up, and when disaster happened, they could quickly replace each other. Distributed mutual back-up strategy has the advantage of high reliability as 'Multi-to-one' and high efficiency without increasing or with only a little increase in disaster recovery resources.

Compared with traditional storage technology, cloud technology has advantages in data security, reliability, manageability, expansibility and investment.

Firstly, the cloud service provider sets up the cloud service center to face to various users. Each user obtains service and pay for it as needed in order to share storage resources and avoiding repeated construction. Meanwhile, because the maintenance and upgrade for cloud service center are completed by service provider, users don't need to employ professional technologist, and then saves manpower, technology and bankroll. With the business developing and data-scale growing, users can expand storage capability anytime, so they can obtain the most professional service by the lowest cost [14].

Secondly, the cloud service center can achieve full virtualization. Any authorized cloud users can simply access the cloud service center to manage or operate or store or back up data through a network cable, without concerning about what device model, interface definition or implementation method the cloud service provider use.

Finally, the cloud service center is able to provide better security guarantee for user's data, because of its independence of operation and maintenance, long distance with most users, as well as professionalism in mass data computing and storage areas.

IV. GUANGDONG CLOUD SERVICE CENTER FOR DISASTER RECOVERY

A. Layout and Planning

According to the suggestion about offsite disaster recovery for provincial emergency command system, the disaster recovery center for emergency command system

must rely on the existing infrastructure, and adopt a method such as cooperative constructing or backing up mutually for disaster recovery. Guangdong cloud service center for disaster recovery combines Guangdong emergency command system to set up required infrastructure. The cloud service center uses provincial emergency command system as the core, and divides 21 city-level emergency command systems into 3 regions by geographical location, as Pearl River Delta, East Guangdong and West Guangdong. Each region selects a conditional city as the regional back-up center to provide offsite data back-up and disaster recovery service for other cities in the same region.

Several key factors in choosing the regional back-up center should be considered.

Distance factor: If the emergency command center is too close to the back-up center, there is a great chance to suffer disaster at a same time or by the same kind. If too far, higher requirements in technology, communication, project implementation, service and management would be put forward, and the project cost would be change greatly. So we need to balance the relationship between system object and project cost, and choose an appropriate distance on the premise that it meet the requirements of cross-region and long-distance disaster recovery (more than 100km) [15].

Nature risks factor: Enough distance can not completely eliminate common disaster factors between emergency command center and disaster recovery center. It should also be considered whether these two places face the same type of nature risk, such as whether all the coastal cities, whether in the same earthquake active area, whether close to a volcano, etc.

Technology level factor: It should be accessed that the urban technology level, for instance, information, business and technical support, telecommunication convenience and diversity and so on, are sufficient to support the construction and operation of disaster recovery center.

Urban environment factor: It should be evaluated that the location of disaster recovery center has sufficient economic level, traffic convenience, infrastructure resource and supporting service abilities.

In a region, city-level emergency platforms use the technology route of 'Multi-to-One' to implement remote data replication into regional back-up center through network. Three regional back-up centers utilize geographic separation to ensure that system function and data can resist catastrophic events, and provide function replacement and data back-up services in special instances. If one city emergency command system is broken-down, the main function can be transferred to regional back-up center, so that the information system would run without interruption. Regional back-up centers adopt the technology roadmap of 'One-to-One' to implement remote mutual data replication, and provide maximum guarantee for all emergency command systems in Guangdong province in the case of serious emergencies.

B. Key Technology

According to the degree of protection, the disaster recovery system can be divided into 3 levels: data-level, system-level and application-level. Guangdong cloud service center integrates a variety of key disaster recovery

technologies to meet the need of 3 recovery levels for Guangdong emergency command system.

1) Data-level disaster recovery

Data is the core of an information system. Data protection is the key of disaster recovery, and also the prerequisite to implement system-level and application-level recovery.

Continuous data protection system is implemented to offer file-level data disaster recovery. Through installing a back-up system client on the emergency command system business sever, the back-up server backup files of emergency command system real-time to disk arrays in the disaster recovery center. When a node of emergency command system is damaged by disaster, the back-up could quickly recover the corresponding files by time, as shown in Fig. 3.

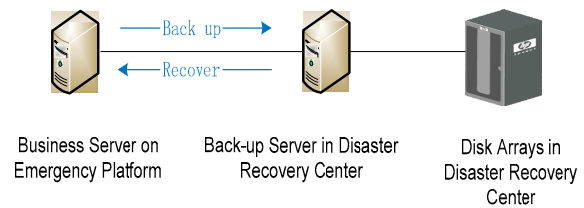


Fig. 3. Continuous data protection system.

Continuous data protection system has the characteristics of continuous data protection and rapid recovery, continuous capture, tracking and recording file-based data changes, and can provide adequately fine recovery granularity. When a disaster occurs, it can quickly recover single or multiple files or catalogs at any time point. Also, it can recover any version or any location of the files. Continuous data protection system supports flexible and efficient data protection mode, file incremental replication and cycle protection, flexible back-up space management, etc. Comparing with traditional data protection methods, continuous data protection system fits better the data protection requirement for critical business of emergency command system.

Aiming at the requirement of data basetable-level disaster recovery, Guangdong cloud server center uses large-scale distributed data management system that has self disaster recovery capability to implement back-up operations for databases on the remote business server, as shown in Fig. 4.

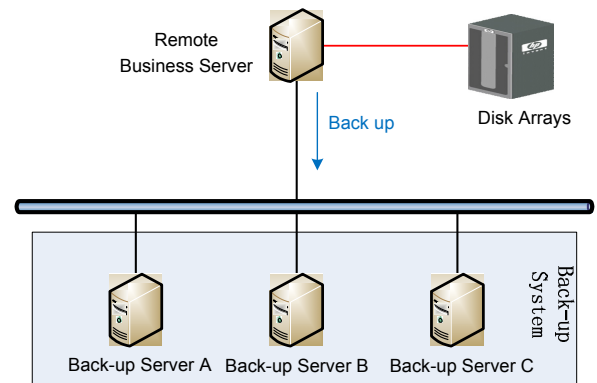


Fig. 4. Large-scale distributed data management system.

Combining NOSQL technology, large-scale distributed data management system breaks through key technologies of

mass data extraction and abstract in large-scale distributed environment, mass data organization and management, multi-duplication data consistency maintenance and others to meet the requirements of high-powered accessing and 7×24 hours availability of large-scale data for emergency command system information system.

2) System-level disaster recovery

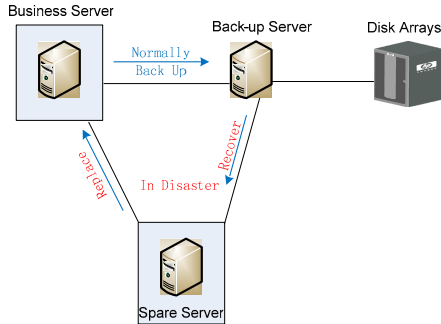


Fig. 5. Instant disaster recovery system.

In addition to data protection, system-level disaster recovery needs to back up the middleware, operating system, communication network and other operating environment as well. When a disaster occurs, the application software could be switched to run on the disaster recovery center, in order to ensure the minute-level recovery.

Guangdong cloud server center utilizes instant disaster recovery system to achieve system-level recovery. The system based on parallel disaster recovery technology, makes operation system virtualization technology as a support and full system back-up of emergency command system as a goal. It uses the remote back-up server and disaster recovery back-up operation system setting up on the production server of emergency command system to back up all data along with operating status of production server into the disaster recovery center. The center utilizes de-redundancy storage structure, and deletes redundant back-up data in real time, in order to improve storage efficiency. As shown in Fig. 5, when the production server fails, the back-up server will recover all data that has been backed up on disk arrays before to a spare server. The spare server can replace the function of the production server because it is designed to be as same as the production server. The recovery process uses pipelining mode, and could recover operating service of the production server information system automatically in 5 minutes when hardware resources are ready, even if the original information system of emergency command system is completely destroyed.

3) Application-level disaster recovery

Application-level disaster recovery cares about not only about data zero loss, but also about business continuity. It is needed to establish a back-up system that keeps consistent real-time with the production system, and ensure that business can directly transfer to the back-up system to take over another one's tasks.

Guangdong cloud server center for disaster recovery is based on infrastructures of Guangdong emergency command system. Each city level emergency command system almost has same hardware and software architectures. According to the isomorphism feature, the center can

implement offsite mutual back-up for all city-level emergency command systems in Guangdong province by using a seamless mutual back-up software system in isomorphic condition. As shown in figure 6, when a node of emergency command system fails, another node will quickly take over its work. Therefore the business could be continuous, and the external interfaces are changeless. For the front-end applications of the entire service system, background service transfer is completely transparent, which meets the need of service continuity. For the end users, it is simple to start over their ongoing emergency management work.

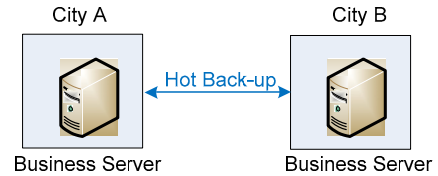


Fig. 6. Mutualback-up between isomorphic emergency command systems.

C. Expectation

Guangdong cloud service center for disaster recovery comprises one central node, several region-center-level nodes and city-level nodes. The center has been planned to provide disaster recovery service for Guangdong emergency command center and 21 city-level emergency command systems when it is fully implemented.

By the design and implementation of Guangdong cloud service center, it is possible to provide service continuously within 5 minutes by back-up server if some information nodes are broken down. The disaster recovery of Guangdong emergency command system will be upgraded to a higher protection level and will work uninterruptedly even under serious situation.

V. CONCLUSION

In summary, the disaster recovery technology has been increasingly developed from relying on a single software or equipment to being independent of specific applications or devices, from simple data-oriented disaster recovery to system-level recovery including not only data but also operating status, from focusing on data back-up and storage efficiency to focusing on service continuity and recovery speed of data accidents.

Through the proposed disaster recovery methods, Guangdong cloud service center for disaster recovery by means of the hardware and software resources of provincial emergency command system. It can avoid redundantly construction and share the whole provincial disaster recovery resources on state level. The integration of various disaster recovery technologies in the cloud environment enables the center to provide efficient disaster back-up and recovery service for all emergency command systems in Guangdong province.

Our experiences demonstrate disaster recovery technologies for large-scale information system, especially for emergency command systems. The future work will focus on testifying different applied technologies on

different emergency command system levels with maneuver and real practices.

ACKNOWLEDGMENT

This research was funded by National High Tech R&D Program of China (863), Grant No. 2012AA012608.

REFERENCES

[1] Y. Liu, W. G. Weng, and W. C. Fan, *Urban Security and Emergency Management*, Beijing, China City Press, 2012.

[2] Introduction of Guangdong Emergency Platform and Emergency Command Center. (Nov. 10, 2012). [Online]. Available: http://www.gdemo.gov.cn/yjglcgzs/08ptjs/201011/t20101110_132537.htm.

[3] J. Q. Ji, "Practices and exploration of the emergency platform system building in Guangdong Province," *China Emergency Management*, vol. 8, pp. 40-41, 2012.

[4] H. Y. Yuan, Q. Y. Huang, G. F. Su, and W. C. Fang, *Theory and Practice of Key Technologies of Emergency Platform System*, Beijing, China, Tsinghua University Press, 2013.

[5] M. H. Choy, H. V. Leong, and M. H. Wong, "Disaster recovery techniques for database systems," *Communications of the ACM*, vol. 43, no. 11, pp. 272-280, 2000.

[6] Y. D. Xu and H. L. Yu, "The future of disaster recovery: Disaster recovery cloud that orients DR resource sharing," *ZTE Technology Journal*, vol. 18, no. 4, pp. 34-37, August 2012.

[7] T. Li, X. J. Liu, J. Q. Zeng, H. Zhao, C. M. Liu, and B. Zhang, *Principles and applications of disaster recovery for information system*, Beijing, China: Posts & Telecom Press, 2007.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, and A. Konwinski *et al.*, "Above the clouds: A Berkeley view of cloud computing," UCB/EECS-2009-28. Berkeley: UC Berkeley Reliable Adaptive Distributed Systems Lab, 2009.

[9] P. Sweeney. Dell Sonic WALL. Is your disaster recovery plan ready for cloud? [Online]. Available: <http://www.networkworld.com/news/tech/2012/091212-cloud-disaster-recovery-262385.html>

[10] D. C. Guster and O. F. Lee, "Enhancing the disaster recovery plan through virtualization," *Journal of Information Technology Research*, vol. 4, no. 4, pp. 18-40, October-December 2011.

[11] D. Xiao and J. Y. Liu, "Key techniques for cloud disaster recovery," *ZTE Technology Journal*, vol. 16, no. 5, pp. 24-27, October 2010.

[12] G. Q. Bian, S. Gao, and B. L. Shao, "Security structure of cloud storage based on dispersal," *Journal of Xi'an Jiaotong University*, vol. 45, no. 4, pp. 41-45, April 2011.

[13] M. Pokharel, S. Lee, and J. S. Park, "Disaster recovery for system architecture using cloud computing," in *Proc. 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT)*, pp. 304-307, July 2010.

[14] O. H. Alhazmi and Y. K. Malaiya, "Evaluating disaster recovery plans using the cloud," *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual*, pp.1-6, January 2013.

[15] X. C. Lin, *Construction and operation management of data center*, Beijing, China: Science Press, 2010.



Fei Wang was born in Henan province, China in 1979. He holds a Dr.-Ing degree in geoinformatics from Munich Bundeswehr University, Germany. He is now a lecturer in Guangdong Branch, Institute of Public Safety Research, Shenzhen Graduate School, Tsinghua University, China. He has been involved in a number of research projects in both governmental and industrial sectors in Europe and China. His research interests lie at the geospatial technologies in disaster management, emergency management platform, GIS and cloud computing. Dr.-Ing Wang is a member of Chinese Society for Public Safety Sciences.



Xiaocui Zheng was born in Guangdong province, China in 1982. She received her bachelor and master degree in nuclear science and technology in Department of Engineering Physics, Tsinghua University in 2004 and 2006, respectively. She is now an engineer in Guangdong Branch, Institute of Public Safety Research, Shenzhen Graduate School, Tsinghua University, China. Her current research interest is Safety Science and Engineering.



Shaobo Zhong was born in Hubei Province, China in 1978. He graduated from Institute of Remote Sensing Applications, Chinese Academy of Sciences and received his Ph. D. in cartography and GIS in 2006. He is now an assistant researcher in Institute of Public Safety Research, Tsinghua University. His research interests include: emergency management information system, geo-information for disaster management, emergency decision making etc. Dr. Zhong currently is a member of Association of Public Safety, China and the secretariat of Emergency Geographic Support Service Committee, China Association for Geographic Information Service.